

№6

2013

ИЮНЬ

Научно-практический
журнал для специалистов

Республика Беларусь, г. Минск

Информационная безопасность

*Тема номера:
«Информационная
безопасность»*

Комплектация для систем защиты кабельной продукции в автомобильной и других отраслях промышленности



Schlemmer
CABLE PROTECTION SYSTEMS

FEK ООО «ФЭК» РБ, 220015, г. Минск, пр. Пушкина, 29 Б,
тел./факс: +375 (17) 210-21-89,
+375 (29) 370-90-92, +375 (29) 274-17-13,
e-mail: info@fek.by, www.fek.by

ПОДПИСКА В БЕЛАРУСИ: «Белпочта» – 00822
ПОДПИСКА В РОССИИ: «Роспечать» – 00822
«АРЗУ – Почта России» – 91654

ISSN 1999-7515



9 177199 917510 6 13006

KLINKMANN

www.klinkmann.by

Компоненты для автоматизации и инсталляции



RAFI



ROSE

CHINT

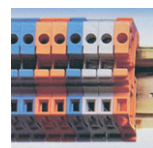
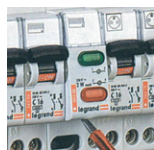
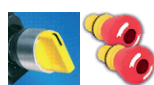


ABB
entrelec

finder



legrand

**Rockwell
Automation**

Подробная информация на нашем сайте
или по телефону 8 (017) 200 08 76

ООО «ШПАТ ЭЛЕКТРО»
СНИЖАЕТ ЦЕНЫ
НА ТОВАРЫ КАТАЛОГА

ELFA DISTRELEC 2013-2014

ДОСТАВКА КАТАЛОГОВ КУРЬЕРОМ ПО МИНСКУ
ИЛИ ПОЧТОЙ ПО РЕСПУБЛИКЕ БЕЛАРУСЬ

220070 г. Минск пр. Партизанский, 14, офис 215А

Тел. (375-17) 345-96-34 (многоканальный)

Факс: (375-17) 214-54-90

E-mail: shpat@shpat.com

**СКИДКА
до 15 %**



**ЖУРНАЛ ИЗДАЕТСЯ ПРИ ИНФОРМАЦИОННОЙ ПОДДЕРЖКЕ
ФАКУЛЬТЕТА РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ БЕЛГОСУНИВЕРСИТЕТА.
ЖУРНАЛ ВКЛЮЧЕН В СПИСОК НАУЧНО-ТЕХНИЧЕСКИХ ИЗДАНИЙ ВАК РЕСПУБЛИКИ БЕЛАРУСЬ**

электроника
инфо

**International magazine
of amateur and professional electronics
№6 (96) июнь 2013**

Зарегистрирован
Министерством информации
Республики Беларусь

Регистрационный №71
от 05 марта 2009 года

Главный редактор:
Раковец Леонид Иванович
e-mail: electronica@nsys.by

Заместитель главного редактора:
Асмоловская Ирина Михайловна
i.asmalouskaya@electronica.by

Редактор технический:
Бортник Ольга Викторовна

Редакционная коллегия:

Председатель:
Чернявский Александр Федорович
академик НАН Беларуси, д.т.н.

Секретарь:
Садов Василий Сергеевич, к.т.н.
e-mail: sadov@bsu.by

Члены редакционной коллегии:
Беляев Борис Илларионович, д.ф.-м.н.
Борздов Владимир Михайлович, д.ф.-м.н.
Голенков Владимир Васильевич, д.т.н.
Гончаров Виктор Константинович, д.ф.-м.н.
Есман Александр Константинович, д.ф.-м.н.
Ильин Виктор Николаевич, д.т.н.
Кугейко Михаил Михайлович, д.ф.-м.н.
Кучинский Петр Васильевич, д.ф.-м.н.
Мулярчик Степан Григорьевич, д.т.н.
Петровский Александр Александрович, д.т.н.
Попечиц Владимир Иванович, д.ф.-м.н.
Рудницкий Антон Сергеевич, д.ф.-м.н.

Отдел рекламы и распространения:
Антоневич Светлана Геннадьевна
тел./факс: +375 (17) 204-40-00
e-mail: asg@nsys.by

Учредитель:
ТЧУП «Белэлектрониконтракт»
220015, Республика Беларусь,
г. Минск, пр. Пушкина, 29 Б,
тел./факс: +375 (17) 210-21-89,
+ 375 (17) 204-40-00
www.electronica.by

© Перепечатка материалов, опубликованных
в журнале «Электроника инфо», допускается
с разрешения редакции

За содержание рекламных материалов редакция
ответственности не несет

Подписной индекс в РБ:
00822 (индивидуальная),
008222 (ведомственная)

Цена свободная

Подготовка, печать:
400 экз. отпечатано
тип. ООО «Полиграф»
г. Минск, ул. Кнорина, 50/4-401А
Лицензия №02330/0494199 от 03.04.2009 г.
Подписано в печать 19.06.2013 г.
Заказ №

СЛАВНЫЕ ИМЕНА

ЧЕЛОВЕК, ПРИДУМАВШИЙ БИТ.....2

**18-Я НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ».....4-163**

ПРИВЕТСТВИЯ.....4

РЕЗОЛЮЦИЯ.....6

ФОТОРЕПОРТАЖ С КОНФЕРЕНЦИИ.....7

ОТКРЫТИЕ КОНФЕРЕНЦИИ.....9

ПЛЕНАРНОЕ ЗАСЕДАНИЕ В БРЕСТСКОМ ОБЛАСТНОМ КУЛЬТУРНОМ ЦЕНТРЕ.....13

СИСТЕМЫ И СРЕДСТВА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.....20

МАТЕМАТИКА И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....43

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....54

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ.....68

СОЗДАНИЕ КРУПНОМАСШТАБНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ.....83

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....84

ЗАКРЫТИЕ КОНФЕРЕНЦИИ.....92

ЗАОЧНОЕ УЧАСТИЕ.....97

РЕЦЕНЗИРУЕМЫЕ СТАТЬИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ.....164

ПРАЙС-ЛИСТ.....228

СПИСОК РЕКЛАМОДАТЕЛЕЙ

«Алнар».....228
«Альфалидер групп».....228
«БелПлата».....182
«Вектор технологий».....96
«ГорнТрейд».....171
«Минский часовой завод».....82
«Нанотех».....53
«Приборостроительная компания».....228
«Промтехсервиснаб».....166
«СветЛед решения».....228
«Тиком».....171
«ФЭК».....228

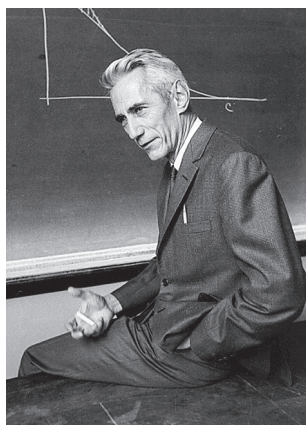
«Чип электроникс».....228

Обложки, цветные вставки

Microchip.....III вст.
«Альфасофт».....II вст.
«Клинкманн».....II обл.
«ФЭК».....I, III обл., I вст.
«ШПАТ».....II обл.
«Электроконтинент».....IV обл.
«Элтикон».....IV обл.
«Энерджи».....IV вст.

ЧЕЛОВЕК, ПРИДУМАВШИЙ БИТ

В конце 1930-х годов Шеннон был первым, кто связал булеву алгебру с переключающими цепями, являющимися составной частью современных компьютеров. Благодаря этому открытию булева алгебра могла быть использована как способ организации внутренних операций компьютера, способ организации логической структуры компьютера. Таким образом, компьютерная промышленность многим обязана этому человеку, даже несмотря на то, что его интересы подчас находились далеко от компьютеров.



Клод Элвуд Шеннон родился 30 апреля 1916 года в небольшом городе Гайлорд на озере Мичиган. Его отец был адвокатом и в течение некоторого времени судьей. Его мать преподавала иностранные языки и стала директором Гайлордской средней школы. Молодой Клод очень любил конструировать автоматические устройства. Он компоновал модели самолетов и радиоцепи, создал также радиоуправляемую лодку и телеграфную систему между своим домом и домом друга. Он исправил радиостанции для местного универмага. Томас Эдисон был одновременно его героем детства и дальним кузеном, хотя они ни разу не встречались. Позже Шеннон добавил Исаака Ньютона, Чарльза Дарвина, Альберта Эйнштейна и Джона фон Неймана в список своих героев. В 1932 году Шеннон был зачислен в Мичиганский университет.

Клод Шеннон специализировался в электротехнике. Но математика также его увлекала, и он пытался посещать столько курсов, сколько было возможно. Один из тех математических курсов, по символической логике, сыграл большую роль в его карьере. Он получил степень бакалавра по электротехнике и математике. «Вот история моей жизни, – говорит Шеннон. – Взаимодействие между математикой и электротехникой».

В 1936 году Клод Шеннон стал аспирантом Массачусетского технологического института (MIT). Его руководитель Ванневар Буш, создатель дифференциального анализатора (аналогового компьютера), в качестве темы диссертации предложил описать логическую организацию анализатора.

Работая над диссертацией, Шеннон пришел к выводу, что булева алгебра может с успехом использоваться для анализа и синтеза переключателей и реле в электрических схемах. Шеннон писал: «Сложные математические операции возможно выполнить посредством релейных цепей. Числа могут быть представлены позициями реле и шаговыми переключателями. Соединив определенным образом наборы реле, можно производить различные математические операции». Таким образом, объяснял Шеннон, можно собрать релейную схему, выполняющую логические операции И, ИЛИ и НЕ. Также можно реализовать сравнения. С помощью таких цепей легко осуществить конструкцию «If... then...».

В 1937 году Шенноном написана диссертация под названием «Символический анализ релейных и переключательных цепей». Это была необычная диссертация,

она расценивалась как одна из наиболее значимых во всей науке того времени: то, что сделал Шеннон, проложило путь к разработке цифровых компьютеров.

Работа Шеннона имела очень важное значение: теперь инженеры в своей повседневной практике, создавая аппаратуру и программы для компьютеров, сети телефонной связи и другие системы, постоянно пользуются булевой алгеброй. Шеннон преуменьшал свою заслугу в этом открытии. «Просто случилось так, что никто другой не был знаком с этими обеими областями одновременно,» – говорил он. И после заявлял: «Мне всегда нравилось это слово – булева».

Справедливости ради нужно заметить, что до Шеннона установлением связи между булевой алгеброй и переключательными цепями занимались в Америке Ч. Пирс, в России – П.С. Эренфест, В.И. Шестаков и др.

По совету Буша Шеннон решил добиваться докторской степени по математике в MIT. Идея его будущей диссертации родилась у него летом 1939 года, когда он работал в Cold Spring Harbor в Нью-Йорке. Буш был назначен президентом Carnegie Institution в округе Вашингтон и предложил Шеннону провести там немного времени: работа, которую делала Барбара Беркс по генетике, могла послужить предметом, для которого Шеннон применит свою алгебраическую теорию. Если Шеннон смог организовать переключение цепей, то почему он не сможет сделать то же в генетике? Докторская Диссертация Шеннона, получившая название «Алгебра для теоретической генетики», была завершена весной 1940 года. Шеннон получает Докторскую степень по математике и степень магистра по электротехнике.

Фрай, директор отделения математики в Bell Laboratories, был впечатлен работой Шеннона в области символической логики и его математическим мышлением. Летом 1940 года он приглашает Шеннона работать в Bell. Там Шеннон, исследуя переключающие цепи, обнаружил новый метод их организации, позволяющий уменьшить количество контактов реле, необходимых для реализации какой-либо сложной логической функции. Он опубликовал доклад, названный «Организация двухполюсных переключающих цепей». В конце 1940 года Шеннон получил Национальную научно-исследовательскую премию. Весной 1941 года он вернулся в Bell Laboratories. С началом войны Т. Фрай возглавил работу над программой для систем управления огнем для противовоздушной обороны. Шеннон присоединился к этой группе и работал над устройствами, которые засекали вражеские самолеты и нацеливали зенитные установки.

AT&T, владелец Bell Laboratories, была ведущей фирмой мира в области связи и естественно, что в лабораториях Bell также велись работы по системам связи. На этот раз Шеннон заинтересовался электронной передачей сообщений. Мало, что было понятно ему в этой области, но он верил, что математика знала ответы на большинство вопросов.

Сначала Шеннон задался простой целью: улучшить процесс передачи информации по телеграфному или

телефонному каналу, находящемуся под воздействием электрических возмущений или шума. Он пришел к выводу, что наилучшее решение заключается не в техническом усовершенствовании линий связи, а в более эффективной упаковке информации.

Что такое информация? Оставляя в стороне вопрос о содержании этого понятия, Шеннон показал, что это измеримая величина: количество информации, содержащейся в данном сообщении, есть функция вероятности, что из всех возможных сообщений будет выбрано данное. Он назвал общий потенциал информации в системе сообщений как ее «энтропию». В термодинамике это понятие означает степень случайности (или, если угодно, «перемешанности») системы (однажды Шеннон сказал, что понятием энтропии ему посоветовал воспользоваться математик Джон фон Нейман, указавший, что, т.к. никто не знает, что это такое, у Шеннона всегда будет преимущество в спорах, касающихся его теории).

Шеннон определил основную единицу количества информации, названную потом битом, как сообщение, представляющее один из двух вариантов: например, «орел» – «решка», или «да» – «нет». Бит можно представить как или 0, или как присутствие или отсутствие тока в цепи.

На этом математическом фундаменте Шеннон затем показал, что любой канал связи имеет свою максимальную пропускную способность для надежной передачи информации. В действительности он доказал, что, хотя можно приблизиться к этому максимуму за счет искусного кодирования, достичь его невозможно.

Этот максимум получил известность как предел Шеннона. Каким образом можно приблизиться к пределу Шеннона? Первый шаг заключается в том, чтобы воспользоваться избыточностью кода. Подобно тому, как влюбленный мог бы лаконично написать в своей любовной записке «я лбл в», путем эффективного кодирования можно сжать информацию, представив ее в наиболее компактной форме. С помощью специальных методов кодирования, позволяющих проводить коррекцию ошибок, можно гарантировать, что сообщение не будет искажено шумом.

Идеи Шеннона были слишком провидческими, чтобы иметь немедленный практический эффект. Схемы на вакуумных электронных лампах просто не могли еще вычислять сложные коды, требовавшиеся для того, чтобы приблизиться к пределу Шеннона. На самом деле только в начале 70-х годов с появлением быстродействующих интегральных микросхем инженеры начали в полной мере пользоваться теорией информации.

Все свои мысли и идеи, связанные с новой наукой – теорией информации, Клод Шеннон изложил в монографии «Математическая теория связи», опубликованной в 1948 году.

Теория информации, помимо связи, проникла также и в другие области, в том числе в лингвистику, психологию, экономику, биологию и даже в искусство. В подтверждение приведем, например, факт: в начале 70-х годов в журнале «IEEE Transactions on Information Theory» была опубликована редакционная статья под названием «Теория информации, фотосинтез и религия». С точки зрения самого Шеннона применение информационной теории к биологическим системам вовсе не является таким уж неуместным, поскольку, по его мнению, в основе механических и живых

систем лежат общие принципы. Когда его спрашивают, может ли машина мыслить, он отвечает: «Конечно, да. Я машина и вы машина, и мы оба мыслим, не так ли?».

В действительности Шеннон был одним из первых инженеров, высказавших мысль о том, что машины можно запрограммировать так, чтобы они могли играть в карты и решать другие сложные задачи.

В 1948 году он публикует работу «Программирование компьютера для игры в шахматы». Ранее подобных публикаций на эту тему не было, причем созданная Шенноном шахматная программа явилась основой для последующих разработок и первым достижением в области искусственного интеллекта. В 1950 году он изобрел механическую мышь Тесей, которая, будучи управляема магнитом и сложной электрической схемой, скрытой под полом, могла найти выход из лабиринта.

Он построил машину, «читающую мысли» и играющую в «монетку» – игру, в которой один из играющих пытается угадать, что выбрал другой играющий, «орел» или «решку». Коллега Шеннона, также работавший в Bell Laboratories, Дэвид У. Хейджелбарджер построил опытный образец; машина запоминала и анализировала последовательность прошлых выборов оппонента, пытаясь отыскать в них закономерность и на ее основе предсказать следующий выбор.

Клод Шеннон был одним из организаторов первой конференции по искусственному интеллекту, состоявшейся в 1956 году в Дартмуте. В 1965 году он побывал по приглашению в Советском Союзе, где прочитал ряд лекций по искусственному интеллекту.

В 1958 году Шеннон покинул Bell Laboratories, став профессором в Массачусетском технологическом институте. После того, как в 1978 году он официально ушел на пенсию, его величайшим увлечением стало жонглирование. Он построил несколько жонглирующих машин и разработал то, что можно было бы назвать объединенной теорией поля для жонглирования.

С конца 50-х годов Шеннон опубликовал очень мало работ по теории информации. Некоторые из его бывших коллег поговаривали, что Шеннон «перегорел» и ему надоела созданная им самим теория, но Шеннон отрицал это. «Большинство великих математиков писали свои лучшие работы, когда были еще молодыми», – говорил он.

В 1985 году Шеннон и его жена внезапно решили посетить Международный симпозиум по теории информации, состоявшийся в английском городе Брайтоне. В течение многих лет он не принимал участия в конференциях, и сначала его никто не заметил. Затем участники симпозиума стали перешептываться: скромный седоволосый джентльмен, который то приходил, то уходил из залов, где слушались доклады, это – Клод Шеннон. На банкете Шеннон сказал несколько слов, немножко пожонглировал тремя мячами и подписал множество автографов инженерам, выстроившимся в длинную очередь. Как вспоминал один из участников, «это воспринималось так, как будто Ньютон появился на конференции, посвященной проблемам физики».

В начале марта 2001 года, в возрасте 84 лет, после продолжительной болезни Клод Шеннон скончался. Как писали вездесущие журналисты — скончался человек, который придумал бит.

18-Я НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

Уважаемые участники конференции!

Постоянный Комитет Союзного государства уделяет большое внимание вопросам совершенствования информационной безопасности Союзного государства и национальных систем защиты информации России и Беларуси.

Достаточно отметить, что в целях решения этих вопросов уже завершены две союзные программы и реализуется третья программа «Совершенствование системы защиты общих информационных ресурсов России и Беларуси на основе высоких технологий».

Ежегодный статус этой конференции и широкий круг ее участников позволяет своевременно и на высоком техническом уровне отслеживать и реализовывать все

передовые достижения в области информационной безопасности.

Выражаю уверенность, что данная конференция послужит дальнейшему динамичному развитию информационных технологий в наших странах, а ее поочередное проведение в различных регионах Беларуси и России – популяризации ее результатов на всем информационном пространстве Союзного государства.

Желаю участникам конференции успешной и результативной работы на благо государств-участников Союзного государства.

Г. Рапота,

Государственный секретарь Союзного государства

Уважаемые участники конференции!

Примите наши искренние поздравления по поводу открытия 18-й научно-практической конференции «Комплексная защита информации», которая является ежегодным значимым мероприятием Союзного государства. С момента проведения первой конференции в 1997 году данный форум является одним из ведущих международных мероприятий, на котором обсуждаются проблемы обеспечения информационной безопасности, защиты информационных ресурсов, создание эффективных технических и программных средств защиты информации.

Интенсивное внедрение информационных технологий во все сферы жизни и деятельности общества привело к тому, что информационный ресурс сегодня является таким же богатством, как производственный и человеческий потенциал каждой страны. При этом обеспечение информационной безопасности личности, общества и государства, является одним из важнейших фактором и необходимым условием, положительно влияющим на стабильное социально-политическое, экономическое и международное развитие Беларуси, России и Союзного государства в целом.

Правительство Республики Беларусь рассматривает конференцию как общепризнанное международное ме-

роприятие, на котором осуществляются обмен мнениями и выработка конструктивных предложений по решению теоретических, организационных, правовых и технических проблем обеспечения защиты информации. Выражаю уверенность, что запланированные к обсуждению вопросы связанные с организационно-правовым обеспечением безопасности субъектов информационных отношений, современными методами и средствами защиты информации в информационных системах, защитой критически важных объектов информационно-коммуникационной инфраструктуры, позволят выработать предложения по решению насущных проблем информационной безопасности. Реализация принимаемых на конференции решений при формировании приоритетов развития информационных технологий позволит значительно повысить эффективность защиты информационного пространства Союзного государства Беларуси и России в современных условиях.

Желаю участникам конференции плодотворной работы и дальнейших успехов в решении задач информационной безопасности на благо наших стран и народов.

А.Н. Калинин,

Заместитель Премьер-министра Республики Беларусь

Уважаемые участники конференции!

Интенсивное развитие информационно-коммуникационных технологий несет не только очевидные преимущества, но и требует создания механизмов эффективного противодействия угрозам в информационной сфере.

Решение данной задачи возможно только на основе консолидации усилий органов государственной власти, бизнеса, научных организаций и гражданского общества, а также применения наилучшего опыта в данной области.

Национальные интересы Республики Беларусь и Российской Федерации в области обеспечения безопасности требуют объединения усилий по защите информационного пространства Союзного государства.

Ежегодное проведение конференции дает возможность в формате открытого обмена мнениями и идеями искать пути внедрения передовых технологий и создания принципиально новых продуктов в области защиты информации.

Предметный подход к выбору тем для обсуждения сделал конференцию авторитетной площадкой для обсуждения наиболее важных задач в области обеспечения информационной безопасности Союзного государства.

Желаю всем участникам конференции конструктивной работы и плодотворного сотрудничества.

Н. Климашин,

Заместитель Секретаря Совета Безопасности
Российской Федерации

Уважаемые организаторы,
участники и гости конференции!

Примите искренние поздравления по поводу открытия 18-й научно-практической конференции «Комплексная защита информации». Данный форум является одним из ведущих международных мероприятий, на котором обсуждаются проблемы обеспечения информационной безопасности, защиты информационных ресурсов, создания эффективных технических и криптографических средств защиты информации.

В современных условиях значение защиты информации в обеспечении безопасности Союзного государства и успешного социально-экономического развития Беларуси и России непрерывно возрастает. Функционирование и совершенствование системы защиты информации как одной из базовых составляющих информационной безопасности требуют от нас эффективной координации действий.

Оперативно-аналитический центр при Президенте Республики Беларусь рассматривает настоящую конференцию как общепризнанное значимое мероприятие Союзного государства, на котором осуществляется обмен мнениями и выработка конструктивных предложений по решению теоретических, организационных, правовых и технических проблем обеспечения защиты информации. Конференция ежегодно собирает вместе ученых, представителей государ-

ственных органов, исследовательских и производственных организаций. Благодаря универсальному подходу к анализу задач защиты информации, нацеленности на рассмотрение вопросов, имеющих практическую значимость, она по праву заслужила репутацию одной из важнейших инициатив по обеспечению безопасности Союзного государства.

Представители белорусской делегации поделятся опытом деятельности по обеспечению технической защиты информации в нашей стране и предложениями относительно перспектив работы в этой сфере. Мы высоко ценим предоставляемые конференцией возможности для использования нашего потенциала на благо работы по укреплению безопасности Союзного государства, а также для ознакомления с достижениями и идеями российских коллег.

Выражаю уверенность, что результаты 18-й научно-практической конференции «Комплексная защита информации» станут важным ресурсом для государственных органов Республики Беларусь и Российской Федерации при подготовке предложений по реализации ими своих полномочий в области обеспечения безопасности в информационной сфере. Желаю всем участникам конференции успехов, плодотворного обмена опытом и результативной работы.

С.В. Шпегун,

Начальник Оперативно-аналитического центра
при Президенте Республики Беларусь

Уважаемый председатель!

Уважаемые участники конференции!

Позвольте поприветствовать Вас от имени директора Федеральной службы по техническому и экспортному контролю.

Одним из приоритетов деятельности ФСТЭК России является укрепление информационной безопасности Союзного государства и решение задач по предупреждению и нейтрализации угроз безопасности информации.

В рамках научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России за прошедший год с момента проведения предыдущего совместного двухстороннего мероприятия достигнуты значительные результаты. К ним мы относим:

- технические решения по нейтрализации угроз безопасности информации в критически важных системах информационной;

- инфраструктуры, построенных на основе Grid-технологий;

- создание программно-аппаратного полигона для моделирования средств и комплексов обеспечения безопасности информационных ресурсов крупномасштабных Grid- и Cloud-подобных распределенных критически важных систем информационной инфраструктуры;

- нормы и методики для оценки защищенности информации в критически важных системах информационной инфраструктуры от преднамеренных деструктивных электромагнитных воздействий;

- меры по усилению защиты платежных систем Союзного государства за счет использования средств высоконадежной нейросетевой биометрической аутентификации;

- меры по повышению защищенности информации, передаваемой по беспроводным каналам передачи данных, и обоснование требований к средствам защиты от несанкционированного доступа и от утечки по техническим каналам, в том числе при использовании современных беспроводных технологий 3G, WiFi, WiMAX, ZigBee.

По ряду направлений работа продолжается, но уже сегодня в рамках начинающей свою работу конференции частично можно будет ознакомиться с достигнутыми результатами в докладах ведущих научных деятелей и специалистов по защите информации.

В настоящее время, исходя из необходимости международного взаимодействия, обусловленного интеграционными процессами в области экономической деятельности в рамках Союзного государства Беларуси и России, а также государств Таможенного союза являются актуальными вопросы обеспечения защиты общих информационных ресурсов, в том числе и для потенциальных стран-участниц данного союза. При этом в интересах нормативного обеспечения решения задач и системы документов по межгосударственной стандартизации. Данная система документов обеспечит упорядоченность организации и содержания работ в области защиты общих информационных ресурсов Беларуси и России, повышение эффективности и качества средств защиты информации, а также средств контроля эффективности проводимых мероприятий по защите общих информационных ресурсов.

Для этой цели проводится работа по формированию номенклатуры межгосударственных стандартов по защите общих информационных ресурсов Беларуси и России, подлежащих разработке и предложений по переводу национальных стандартов в области защиты информации в

ранг межгосударственных. Данная работа осуществляется с российской стороны в том числе на базе общественной организации Росстандарта – технического комитета по стандартизации «Защита информации» ТК 362.

Защита общих информационных ресурсов Беларуси и России может быть более эффективной с учетом взаимного опыта построения систем защиты информации каждой из сторон. На сегодняшний день с российской стороны в качестве такого опыта могут являться изданные приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказ ФСТЭК России от 11 февраля 2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Приказ, устанавливающий организационные и технические меры обеспечения безопасности персональных данных прошел государственную регистрацию в Минюсте России. Приказ доступен для скачивания на официальном сайте ФСТЭК России и в информационной системе Минюста России. Напомню, что указанный приказ вступает в силу после его официального опубликования в установленном законодательством Российской Федерации порядке.

Уважаемые участники конференции!

Мы убеждены, что успешное совместное решение отмеченных задач предоставит Союзному государству и государствам-участникам механизмы, разработанные на принципиально новых и высокоэффективных технических и организационных решениях, позволяющие осуществлять эффективное нормативно-правовое и организационное регулирование деятельности государственных субъектов Беларуси и России в области защиты информации. Будут разработаны направления и способы обеспечения безопасного функционирования критически важных систем информационной инфраструктуры и объектов информатизации органов государственного управления, а также сохранены достигнутые в ходе совместной работы и получают дальнейшее развитие научно-технический и технологический потенциалы Беларуси и России в сфере обеспечения безопасности информации.

Уважаемые коллеги!

Позвольте пожелать всем участникам плодотворной работы в ходе Восемнадцатой научно-практической конференции «Комплексная защита информации» и выразить надежду на дальнейшее взаимодействие не только в рамках формата данной конференции.

Приветственное слово ФСТЭК России

РЕЗОЛЮЦИЯ 18-Й НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

С 21 по 24 мая 2013 года в г. Бресте состоялась очередная 18-я научно-практическая конференция «Комплексная защита информации» как мероприятие Союзного государства. Организаторы конференции – Парламентское Собрание Союза Беларуси и России, Постоянный Комитет Союзного государства, аппарат Совета Безопасности Российской Федерации, Оперативно-аналитический центр при Президенте Республики Беларусь, Федеральная служба по техническому и экспортному контролю Российской Федерации, Межрегиональная общественная организация «Ассоциация защиты информации», Государственное предприятие «НИИ ТЗИ», Брестский областной исполнительный комитет и Брестский государственный технический университет. В работе конференции приняли участие около 160 ученых и специалистов Беларуси и России.

В ходе проведения конференции рассмотрены актуальные вопросы обеспечения безопасности информационного пространства государств-участников Союзного государства.

На пленарных и секционных заседаниях, круглых столах было заслушано и обсуждено более 110 докладов ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного

государства по широкому спектру научных направлений, осуществлялся обмен опытом по вопросам использования безопасных информационных и коммуникационных технологий в различных сферах жизни общества и государства.

В частности, рассмотрены вопросы создания защищенных объектов информационных технологий, технической и криптографической защиты информации, подготовки специалистов в области информационной безопасности, а также нормативно-правовые аспекты обеспечения информационной безопасности Союзного государства.

Участники конференции обменялись опытом исследований, разработки, внедрения и разрешения теоретических, методологических, нормативных, организационно-технических, правовых и гуманитарных вопросов обеспечения информационной безопасности. Рассмотрены вопросы технологического и нормативного обеспечения трансграничного обмена юридически значимого электронного документооборота.

Отмечен вклад специалистов и молодых ученых в научную и организационную деятельность в сфере защиты общих информационных ресурсов Союзного государства. По решению оргкомитета по подготовке конференции награждены дипломами конференции «За вклад в научную

и организационную деятельность в сфере защиты общих информационных ресурсов Союзного государства» Анищенко В.В., Горбач А.Н., Емельянов Г.В., Куц А.В., Харин Ю.С. и Язов Ю.К. Пять докладов победили в конкурсе «Молодых ученых», по результатам которого их авторам также вручены дипломы конференции.

Участники конференции постановили:

1. Одобрить результаты работы XVIII научно-практической конференции «Комплексная защита информации», выразить благодарность организаторам конференции за высокий уровень ее подготовки и проведения.

2. Опубликовать материалы конференции в отдельном выпуске журнала «Электроника инфо», входящего в список изданий Высшей аттестационной комиссии Республики Беларусь.

3. Провести XIX научно-практическую конференцию «Комплексная защита информации» в 2014 г. в Российской Федерации. Просить Постоянный Комитет Союзного государства сформировать рабочую группу для подготовки и осуществления организационных мероприятий.

4. Рекомендовать организаторам очередной конференции по согласованию с Постоянным комитетом Союзного государства расширить состав ее участников и пригласить ученых и специалистов государств-участников Единого таможенного пространства и ОДКБ.

5. Проинформировать руководство Постоянного Комитета Союзного государства и Парламентского Собрания Союза Беларуси и России об итогах XVIII научно-практической конференции «Комплексная защита информации» и ее предложениях.

Принята на пленарном заседании

23 мая 2013 года, г. Брест

ФОТОРЕПОРТАЖ С 18-Й НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»



Участники 18-й научно-практической конференции «Комплексная защита информации»



Встреча участников конференции в Брестском областном общественно-культурном центре



Участники 18-й научно-практической конференции «Комплексная защита информации» возлагают венок к Вечному огню мемориального комплекса «Брестская крепость-герой»



Открытие конференции в Брестском областном общественно-культурном центре



Ректор Брестского государственного технического университета П.С. Пойта рассказывает участникам конференции об университете



Обсуждение доклада на заключительном заседании конференции 23 мая 2013 года



Вручение дипломов победителям конкурса молодых ученых за лучший доклад

ОТКРЫТИЕ КОНФЕРЕНЦИИ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ УКРЕПЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

А.Н. Горбач,

**Оперативно-аналитический центр
при Президенте Республики Беларусь, г. Минск**

В современных условиях функционирование Союзного государства Беларуси и России невозможно без применения новейших информационных технологий.

Быстрое совершенствование процессов информатизации, проникновение информации во все сферы жизненно важных интересов личности, общества и государства повлекли, помимо несомненных преимуществ, появление ряда специфических проблем, которые обуславливают возрастание актуальности задачи постоянного совершенствования системы защиты общих информационных ресурсов Беларуси и России. В этой связи, одним из основных направлений деятельности в области укрепления информационной безопасности Союзного государства является решение задач по предупреждению и нейтрализации угроз безопасности информации. Этот процесс должен быть непрерывным и постоянно совершенствоваться.

В настоящее время в этой сфере деятельность Оперативно-аналитического центра при Президенте Республики Беларусь совместно с Федеральной службой по техническому и экспортному контролю, и Федеральной службой безопасности Российской Федерации концентрируется в рамках программы Союзного государства по проведению совместных фундаментально-поисковых, научно-исследовательских и опытно-конструкторских работ в области защиты информации «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011 – 2015 годы. Организация работ определяется в соответствии с Порядком разработки и реализации программ Союзного государства, утвержденным постановлением Совета Министров Союзного государства. Указанный Порядок, по нашему мнению, обладает некоторыми недостатками, которые не позволяют обеспечить непрерывным процессом совершенствования системы защиты общих информационных ресурсов Беларуси и России.

Выполняемая в настоящее время программа является уже третьей в области укрепления информационной безопасности Союзного государства. И наш опыт показывает, что разрыв в выполнении мероприятий программ составляет 1,5 – 2 года, которые уходят на организационные вопросы, связанные с одобрением постановлениями Совета Министров Союзного государства концепции и самой программы. Так предыдущая программа была завершена в 2010 году, концепция нынешней программы одобрена постановлением Совета Министров Союзного государства от 6 октября 2011 г. № 25, а программа – от 20 апреля 2012 г. № 6. С учетом этого, плановый пятилетний срок выполнения мероприятий программы сократился до 3,5 лет.

В связи с этим Оперативно-аналитическим центром сформированы предложения по внесению изменений и дополнений в Порядок разработки и реализации программ

Союзного государства. В частности, нами предлагается внести в Порядок положение о том, что для решения проблем, связанных с обеспечением безопасности Союзного государства, допускается подготовка материалов по вопросу принятия концепции и новой программы в последнем году реализации действующей программы. Это позволит обеспечить непрерывный процесс осуществления скоординированных действий по совместному решению проблем национальной безопасности Российской Федерации и Республики Беларусь, сократить неоправданные временные разрывы на этапах подготовки и принятия концепции и новой программы.

Это, конечно же, может распространяться только на будущую программу. Что же касается действующей программы, то в 2012 году сложилась сложная ситуация с ее выполнением. В связи с поздним ее утверждением, а так же необходимостью проведения процедур по выбору исполнителей мероприятий программы, договора на выполнение научно-исследовательских и опытно-конструкторских работ были заключены в августе-сентябре 2012 года. А с учетом того, что в утвержденной программе было запланировано в 2012 году выполнить объемы мероприятий 2011 и 2012 годов, исполнителям пришлось организовать работу таким образом, чтобы выполнить указанный объем за 4-5 месяцев. Соответственно и основное освоение бюджетных средств в 2012 году проводилось в конце года.

Несмотря на это, четкая организация работ исполнителей мероприятий программы позволила выполнить в кратчайшие сроки объемы работ этапов 2012 года в соответствии с заключенными договорами на исполнение научно-исследовательских и опытно-конструкторских работ.

В результате, одна научно-исследовательская работа была завершена в полном объеме и по одиннадцати мероприятиям выполнены работы первых этапов.

По завершенной работе учреждением Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики» разработаны 5 проектов стандартов, предназначенных для расширения отечественных и адаптации международных стандартов в области криптографической защиты информации, для встраивания отечественных криптографических алгоритмов в информационные системы и стандартизации взаимодействия между такими системами в рамках Союзного государства.

Серьезные промежуточные результаты получены белорусскими исполнителями по остальным выполняемым мероприятиям программы. В том числе разработаны технические проекты программно-аппаратных комплексов межгосударственной системы управления открытыми ключами и доверенных центров обеспечения электронного документооборота, программно-аппаратной платформы защищен-

ного архива электронных документов, высокоскоростного малогабаритного генератора случайной числовой последовательности гарантированного качества на физическом источнике шума; эскизные проекты устройства активной защиты аналоговой и цифровой речевой информации по низкочастотным каналам и аппаратного модуля криптографической защиты информации. В ходе выполняемых научно-исследовательских работ проведены исследования по разработке проектов нормативно-правовых документов межгосударственного обмена электронными документами Союзного государства и основных направлений исследований по совершенствованию системы защиты общих информационных ресурсов Беларуси и России.

Полученные предварительные результаты вселяют уверенность в достижении основной цели программы – совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий в соответствии с угрозами безопасности информации, прогнозируемыми на период до 2015 года и на дальнейшую перспективу, путем создания научно-технических и нормативно-методических условий для безопасного функционирования критически важных систем информационной инфраструктуры и защиты информации ограниченного доступа.

Выполняемые по программе работы направлены на решение задач по разработке на основе высоких технологий необходимых научно-технических решений для реализации мер по предупреждению и нейтрализации угроз безопасности информации в критически важных системах информационной инфраструктуры и созданию необходимых научно-технических и нормативно-методических условий для реализации мер по защите информации ограниченного доступа при использовании высоких технологий ее обработки.

Реализация программы будет способствовать повышению информационной безопасности Союзного государства и государств-участников, их социально-экономическому развитию на основе объединения интеллектуальных и материальных потенциалов.

Это позволит:

- осуществить разработку высокотехнологичных научно-технических решений для обеспечения защиты информации в Союзном государстве;

- обеспечить гармонизацию национальных нормативных правовых актов и методических документов в области защиты информации;

- создать условия для обеспечения устойчивого функционирования автоматизированных систем управления критическими объектами инфраструктуры;

- создать условия для обеспечения безопасности персональных данных в информационных системах Союзного государства.

Эффект от реализации программы ожидается за счет:

- предотвращения ущерба в результате нарушения функционирования информационных систем Союзного государства или минимизации такого ущерба в случае реализации информационных угроз;

- экономии расходов Беларуси и России на защиту национальных информационных ресурсов в результате применения средств защиты информации, единых нормативных и методических документов, разработанных совместно в ходе выполнения программы;

- развития производства конкурентоспособных технических, программно-аппаратных и программных средств защиты информации.

Кроме того, в 2012 году государственными заказчиками программы совместно с Постоянным Комитетом Союзного государства завершены работы по утверждению руководящих и нормативно-технических документов, разработанных в рамках предыдущей программы. В результате введены в действие 73 документа, создана электронная база данных с документами Союзного государства в области технической защиты информации и обеспечения безопасности информации в критически важных системах информационно-телекоммуникационной инфраструктуры Союзного государства, в том числе совместных информационных ресурсов.

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ НОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СООТВЕТСТВИЕ И ВЗАИМОДЕЙСТВИЕ СТАНДАРТОВ И ЛУЧШИХ ПРАКТИК

**В.В. Анищенко,
ОИПИ НАН Беларуси, г. Минск**

Сегодня подразделения информационных технологий (ИТ) постоянно сталкиваются с растущими требованиями к качеству и количеству электронных услуг и поддержки их информационной безопасности как со стороны руководителей, так и со стороны производственных служб. Рынок предлагает для подразделений ИТ новые продукты и решения ежедневно, при этом упущенное время при принятии решения по выбору продуктов и систем ИТ достаточно дорого может стоить государственным организациям, производственным предприятиям и бизнесу, задачи которых и призвано решать ИТ-подразделение.

В данных условиях руководителю ИТ-подразделения целесообразно использовать апробированные и уни-

фицированные подходы к управлению, а также методики и стандарты управления, которые позволят организовать бесперебойную и безопасную работу ИТ-подразделения.

С этой целью были разработаны всевозможные так называемые лучшие практики (best practices). Одной из распространенных методологий является методология COBIT, первая версия которой разработана Ассоциацией контроля и аудита информационных систем ISACA и Институтом Руководства ИТ (IT Governance Institute – ITGI) в 1992 году. COBIT представляет общепринятый подход к управлению ИТ. Сферами применения COBIT являются:

– аудит информационных систем (ИС), аудит ИТ-подразделений и определение стратегий развития по данным направлениям;

– определение уровня зрелости ИТ-процессов, уровня организации ИТ-процессов, а также уровня организации руководства информационными технологиями.

Актуальная до весны 2012 года версия 4.1 методологии COBIT представляет собой типовую модель процессов, которая поделена на 4 группы или 4 домена. Это планирование и организация, приобретение и внедрение, эксплуатация и сопровождение, мониторинг и оценка. Кроме этого, COBIT предлагает систему метрик, которая позволяет оценить эффективность процессов, эффективность целевых показателей процессов и эффективность деятельности внутри процессов.

В COBIT присутствует достаточно четкая связь целей производственного процесса (бизнеса) с целями ИТ и реализующими эти цели процессами ИТ. COBIT основан на четырех базовых понятиях: процессный подход, система сбалансированных показателей, модели зрелости и принципы проектного управления.

В апреле 2012 года была опубликована методология COBIT версии 5, в которой уточнены процессы на уровнях управления и также интегрировано содержание COBIT 4.1, Val IT (методология управления ценностью ИТ на базе COBIT) и Risk IT (методология управления рисками, связанными с ИТ на базе COBIT) в одну справочную модель.

Методология COBIT 5 основана на пяти ключевых принципах руководства и управления корпоративными службами ИТ:

– удовлетворение потребностей заинтересованных сторон;

- полное покрытие деятельности предприятия;
- применение единой, интегрированной методологии;
- возможность применения комплексного подхода;
- разделение уровней руководства и управления.

Существует много связанных с ИТ стандартов и лучших практик, но все они дают рекомендации лишь относительно части деятельности подразделения ИТ. COBIT 5 идеологически согласовывается с другими стандартами и методологиями в данной предметной области и поэтому он может выступать в качестве общей методологии для руководства и управления корпоративными ИТ.

Хотя, безусловно, COBIT представляет лучшие практики для управления ИТ, но документ важен с точки зрения ее ключевой составляющей – рекомендаций по информационной безопасности.

Важно отметить, что при разработке COBIT 5 учитывались такие ключевые стандарты по информационной безопасности как ISO 27001/27002 и NIST SP800-53 (rev1).

COBIT содержит комплексное описание системы управления ИТ, рассматривая при этом и вопросы информационной безопасности. В частности, 2 из 37 процессов COBIT 5 имеют непосредственное отношение к информационной безопасности: APO13 Управлять безопасностью и DSS05 Управлять сервисами безопасности.

Часть процессов COBIT 5 возможно использовать при внедрении некоторых областей (процессов) комплексной системы информационной безопасности (например, системы управления информационной безопасностью

в соответствии с ISO 27001). В частности, это следующие процессы: EDM03 Ensure Risk Optimization, APO09 Manage Service Agreements, APO12 Manage Risk, BAI04 Manage Availability and Capacity, BAI06 Manage Changes, BAI09 Manage Assets, BAI010 Manage Configuration, DSS02 Manage Service Requests and Incidents, DSS03 Manage Problems и др.

Комплект документов COBIT 5 содержит специальное руководство, раскрывающее более подробно подходы к информационной безопасности «COBIT 5 for Information Security», в котором выделяется следующие 10 сервисов информационной безопасности: архитектура информационной безопасности; повышение осведомленности в информационной безопасности; проектирование и планирование с учетом стандартов по информационной безопасности; оценка информационной безопасности; реализация информационной безопасности; управление правами доступа; защита от вредоносного кода, внешних и внутренних атак; реагирование на инциденты; тестирование системы информационной безопасности; мониторинг информационной безопасности.

Каждому сервису соответствуют наборы направлений, по которым они реализуются.

Кроме методологии COBIT, которая ориентирована, прежде всего, на руководство компаний, отвечающее за ИТ, существует также широко распространенная методология ITIL – Information Technology Infrastructure Library – или Библиотека передового опыта по управлению ИТ-инфраструктурой. Разработана данная методология в Великобритании в конце 80-х годов. Одной из предпосылок создания проекта ITIL стал тот факт, что правительственные организации стали все более и более зависеть от информационных технологий. Сферами управления ITIL являются оказание услуг по управлению инфраструктурой ИТ и по управлению информационной безопасностью.

Сегодня актуальной является 3-я версия ITIL 2007 года, которая состоит из 5 разделов. Это стратегия сервисов, проектирование сервисов, внедрение сервисов, эксплуатация и сопровождение сервисов, а также непрерывное улучшение сервисов. Существуют соответствующие данным разделам публикации ITIL.

Существует важное, с точки зрения обеспечения информационной безопасности, руководство по соответствию COBIT 4.1, ITIL v3 и ISO 27002.

Использованный в ITIL процессный подход полностью соответствует стандартам серии ISO 9000. Их суть – стандартизированный контроль процессов. На основе ITIL/ITSM разработан британский стандарт BSI 15000 (Standard for IT Service Management). Суть этого документа – стандартизация производственных процессов. На основе стандарта BSI 15000 практически без изменений был разработан стандарт ISO 20000 Международной организацией по стандартизации.

Что касается взаимодействия двух методологий лучших практик. Существуют формальные документы соответствия («маппинги» – mapping) процессов COBIT и ITIL, которые определяют однозначные области пересечения (т.е. интерфейсы) двух этих методологий между собой.

COBIT выступает в роли интегратора («зонтика») более детальных стандартов и лучших практик в сфере ИТ,

суммируя ключевые цели в рамках методологии, которая в свою очередь, увязана с управлением и требованиями бизнеса.

По мнению агентства Gartner COBIT и ITIL:

- это не взаимоисключающие подходы;
- они могут и должны продуктивно использоваться совместно для обеспечения качественного управления ИТ, контроля и построения структуры управления ИТ-сервисами на основе лучшего мирового опыта;
- предприятия, планирующие использовать ITIL-методологию для ИТ-подразделений, для аналогичных целей в общей структуре контроля и управления должны использовать COBIT.

Таким образом, следует комплексно продолжить локализацию лучших международных практик и стандартов:

– COBIT – методология для корпоративного управления ИТ;

– ITSM/ITIL – приемы и методы управления ИТ-отделом компании на основе решений из библиотеки передового опыта в области управления ИТ;

– СТБ 34.101 (ISO 15408) – Критерии оценки безопасности ИТ;

– ISO 20000 – Система менеджмента ИТ-сервисов;

– ISO 27000 – Система менеджмента информационной безопасности;

– ISO 25000 – Требования к качеству и оценке ПО.

После локализации данные стандарты станут незаменимыми пособиями для управления ИТ-процессами и ИТ-службами предприятий любых форм собственности в любых областях экономики стран-участников Союзного государства.

НОВОСТИ

MICROCHIP РАСШИРЯЕТ СЕМЕЙСТВО 8-BIT PIC® МИКРОКОНТРОЛЛЕРОВ, ИНТЕГРИРУЯ ИНТЕЛЛЕКТУАЛЬНУЮ АНАЛОГОВУЮ ПЕРИФЕРИЮ

Ключевые особенности:

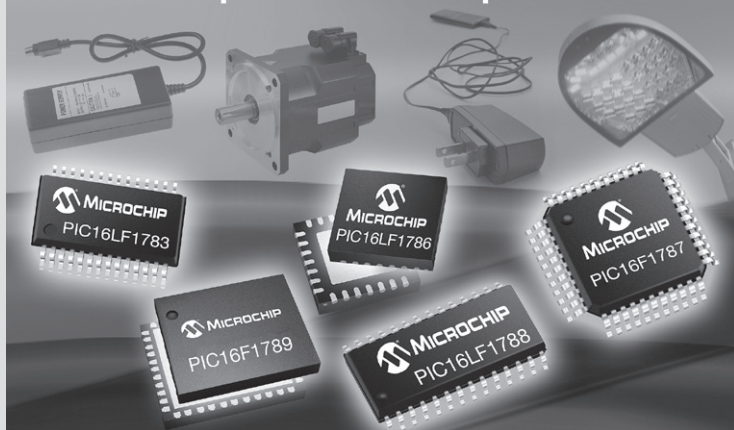
- на новых МК реализованы 12-бит АЦП, высокопроизводительные 16-бит ШИМ и высокоскоростные компараторы;
- продвинутая аналогово-цифровая периферия сочетается с низким потреблением;
- аналоговая обратная связь с минимальной нагрузкой на ядро.

Microchip объявляет о расширении семейства 8-bit микроконтроллеров PIC16F178X, повышая емкость flash памяти, интегрируя продвинутую аналогово-цифровую периферию. В новых МК были реализованы 12-bit АЦП, 16-bit ШИМы, 8-bit и 5-bit ЦАП, операционные усилители и высокоскоростные компараторы с временем отклика 50 нс. Также они поддерживают EUSART (включая LIN), I2C™ и SPI интерфейсы. PIC16F178X – первые PIC® микроконтроллеры со встроенным программируемым контроллером импульсного источника питания (PSMC), который представляет собой 16-bit ШИМ с рабочей частотой 64 МГц и обладает высокой производительностью. Благодаря богатому функционалу PIC16F178X позволяют находить эффективные и недорогие решения для поставленных перед разработчиками задач. Новые МК были выполнены с применением XLP (eXtreme Low Power) технологии, так что токи потребления составляют всего 32 мкА/МГц в активном и 50 нА в спящем режимах, что позволяет существенно продлить время жизни аккумулятора. Низкое потребление вкупе с продвинутой аналогово-цифровой периферией делают PIC16F178X отличным вариантом для светодиодных подсветок,

схем управления зарядом аккумулятора, схем питания цифровых систем и других различных приложений.

PIC16F178X доступны в корпусах с 28 и 40 выводами. Используя расширенную независимую от ядра периферию, которая включает в себя 12-bit АЦП, 16-bit ШИМы, 8-bit и 5-bit ЦАП, операционные усилители и высокоскоростные компараторы, можно выполнить аналоговую обратную связь, оптимизирующую управление приложением, что позволяет разгрузить ядро для использования его при решении широкого спектра задач, встречающихся, например, при разработке медицинских приборов. Также в МК интегрирован генератор 32 МГц, встроенная flash-память (2–16 Кслов) (3,5 – 28 Кбайт), 256 – 2 Кбайт ОЗУ и 256 байт EEPROM.

MCUs with Intelligent Analog and Core-Independent Peripherals



**ПЛЕНАРНОЕ ЗАСЕДАНИЕ
В БРЕСТСКОМ ОБЛАСТНОМ КУЛЬТУРНОМ ЦЕНТРЕ
ПРОГРАММА СОЮЗНОГО ГОСУДАРСТВА «СОВЕРШЕНСТВОВАНИЕ
СИСТЕМЫ ЗАЩИТЫ ОБЩИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ
БЕЛАРУСИ И РОССИИ НА ОСНОВЕ ВЫСОКИХ ТЕХНОЛОГИЙ»
НА 2011–2015 ГОДЫ – ОЧЕРЕДНОЙ ШАГ В УКРЕПЛЕНИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА**

В.Н. Бакун, В.Ф. Картель,
Государственное предприятие «НИИ ТЗИ», г. Минск

В условиях непрерывного совершенствования информационных технологий, обусловленного решением все более сложных и масштабных задач во всех сферах жизнедеятельности человека, возрастает зависимость государства и общества от состояния обеспечения безопасности информационных ресурсов.

Рост объема информационных ресурсов и интенсивное развитие информационных технологий закономерно влекут за собой повышение опасности угроз безопасности информации, связанных с деятельностью иностранных спецслужб, преступных сообществ и отдельных лиц в сферах государственного управления, банковской деятельности, функционирования критически важных систем информационной инфраструктуры и в других сферах.

В этой связи, одним из основных направлений деятельности в области укрепления информационной безопасности государств является решение задач по предупреждению и нейтрализации угроз безопасности информации.

Общие информационные ресурсы Беларуси и России содержат информационные системы, обеспечивающие деятельность Союзного государства в военно-техническом сотрудничестве и обороне, таможенном и экспортном контроле, эксплуатации топливно-энергетического комплекса, взаимодействия правоохранительных органов и в других областях.

Важной частью общих информационных ресурсов является информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну Российской Федерации или государственные секреты Республики Беларусь, которая включает в себя сведения, составляющие коммерческую, служебную и иные виды тайн.

Значительную долю общих информационных ресурсов Беларуси и России составляют критически важные системы информационной инфраструктуры, обеспечивающие функционирование жизненно важных элементов инфраструктуры Союзного государства. В ходе совместной деятельности Республики Беларусь и Российской Федерации может функционировать более 20 таких систем, к числу которых относятся: системы управления движением железнодорожного транспорта, географические и навигационные системы, финансово-кредитные и другие системы.

Деструктивные информационные воздействия на критически важные системы информационной инфраструктуры могут привести к значительному экономическому ущербу и другим негативным последствиям в различных сферах жизнедеятельности Союзного государства (нарушению

функционирования систем государственного управления, систем управления жизнеобеспечением городов и населенных пунктов, систем управления движением транспорта, систем управления потенциально опасными объектами).

Для совершенствования единого научно-технического обеспечения защиты общих информационных ресурсов Беларуси и России, Союзным государством более 10 лет осуществляется деятельность по реализации программ по укреплению информационной безопасности участников Союзного государства.

В период с 2000 по 2010 годы были выполнены программы «Защита общих информационных ресурсов Беларуси и России» и «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006-2010 годы». В результате выполнения указанных программ были разработаны:

- основы единой научно-технической политики по защите общих информационных ресурсов Беларуси и России;
- единая российско-белорусская система документов, регламентирующих деятельность по обеспечению защиты общих информационных ресурсов Беларуси и России от информационных угроз;
- информационно-техническая система защиты общих информационных ресурсов Беларуси и России от информационных угроз;
- система документов, регламентирующих деятельность по обеспечению безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры и контроля эффективности этих мероприятий;
- информационно-техническая система контроля безопасности информации на критически важных объектах информационно-телекоммуникационной инфраструктуры;
- перспективные технологии защиты общих информационных ресурсов Беларуси и России: от утечки по техническим каналам, от несанкционированного доступа, от компьютерных атак и вирусов на основе криптографических методов;
- аппаратные, программные и программно-аппаратные средства, обеспечивающие эффективное решение отдельных задач защиты информации;
- единые образовательные стандарты в области защиты информации.

Полученные в период с 2000 по 2010 годы результаты позволили создать базовые условия для формирования и совершенствования системы защиты общих информацион-

ных ресурсов Беларуси и России, предотвращения ущерба от реализации информационных угроз, производства конкурентоспособных средств защиты информации.

Наиболее важное значение для защиты общих информационных ресурсов имеют:

- проведенные исследования по организации мониторинга состояния обеспечения безопасности на критически важных трансграничных системах информационно-телекоммуникационной инфраструктуры Союзного государства, проведению контроля на критически важных объектах, по информационному обмену между национальными органами контроля;

- создание переносного автоматизированного программно-аппаратного комплекса по проведению специальных исследований технических средств обработки информации в расширенном диапазоне частот и контроля защищенности помещений от утечки информации по акустическим и виброакустическим каналам;

- разработка специального программного обеспечения контроля эффективности защиты распределенных информационных ресурсов от воздействия компьютерных атак.

Был получен ценный опыт решения задач по защите информации, сформированный с участием более 30 научно-исследовательских организаций Республики Беларусь и Российской Федерации.

В настоящее время реализуется программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011-2015 годы, утвержденная Постановлением Совета Министров Союзного государства от 20 апреля 2012 года № 6.

Программой определены для решения две основные задачи:

- разработка на основе высоких технологий необходимых научно-технических решений для реализации мер по предупреждению и нейтрализации угроз безопасности информации в критически важных системах информационной инфраструктуры;

- создание на основе высоких технологий необходимых научно-технических и нормативно-методических условий для реализации мер по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), при использовании высоких технологий ее обработки.

Для решения первой задачи спланирован комплекс научно-исследовательских и опытно-конструкторских работ (НИОКР), предусматривающий:

- анализ и оценку защищенности типовых критически важных систем информационной инфраструктуры от угроз безопасности информации;

- разработку с использованием высоких технологий методов и средств оценки защищенности критически важных систем информационной инфраструктуры от угроз безопасности информации;

- разработку методов и средств тестирования локальных компьютерных сетей критически важных систем информационной инфраструктуры с целью выявления скрытых каналов передачи данных.

Для решения второй задачи спланирован комплекс НИОКР, предусматривающий:

- анализ состояния и перспектив развития информаци-

онных технологий, оценку уровня защищенности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), от угроз безопасности информации;

- разработку перспективных способов и средств защиты информации при реализации наукоемких технологий обработки информации, создании доверенных сред при распределенной обработке информации с использованием информационно-телекоммуникационной среды общего пользования;

- разработку эффективных способов и систем аутентификации и разграничения доступа.

Кроме того, Программой предусмотрено решение следующих задач:

- проведения мониторинга реализации Программы;
- формирования межгосударственной системы стандартов в области защиты общих информационных ресурсов;
- обоснования и разработки основных направлений дальнейших исследований по совершенствованию системы защиты общих информационных ресурсов Беларуси и России.

В ходе реализации программы решаются задачи по разработке на основе высоких технологий необходимых научно-технических решений для реализации мер по предупреждению и нейтрализации угроз безопасности информации в критически важных системах информационной инфраструктуры и создания на основе высоких технологий необходимых научно-технических и нормативно-методических условий для реализации мер по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), при использовании высоких технологий ее обработки.

В ходе выполнения программы Союзному государству будут предоставлены механизмы, разработанные на принципиально новых и высокоэффективных технических и организационных решениях, позволяющие осуществлять эффективное нормативно-правовое и организационное регулирование деятельности государственных субъектов Беларуси и России в области защиты информации; будут разработаны направления и способы обеспечения безопасного функционирования критически важных систем информационной инфраструктуры и объектов информатизации органов государственного управления Союзного государства; будут сохранены достигнутые в ходе совместной работы и получат дальнейшее развитие научно-технический и технологический потенциалы Беларуси и России в сфере обеспечения безопасности информации.

Реализация Программы ведется по следующим направлениям:

- разработка системы взглядов на обеспечение защиты информации в распределенных информационно-вычислительных системах на основе Grid-технологий и сетей связи общего пользования, макетов информационно-вычислительных комплексов (систем) на основе Grid-технологий и требования по защите информации при реализации наукоемких технологий ее обработки;

- разработка рекомендаций по созданию доверенных сред при распределенной обработке информации с использованием информационно-телекоммуникационной среды общего пользования;

– создание макетов, опытных образцов перспективных средств высоконадежной аутентификации и разграничения доступа;

– разработка методического и программного обеспечения мероприятий по контролю защищенности информации в критически важных системах информационной инфраструктуры от деструктивных информационных воздействий, методы и средства тестирования локальных вычислительных сетей указанных систем с целью выявления скрытых каналов утечки информации;

– разработка алгоритмического и программного обеспечения инфраструктуры открытых ключей на информационном пространстве Союзного государства;

– разработка методического документа в области защиты информации ограниченного доступа, не составляющей государственную тайну (государственные секреты), и требований к средствам защиты информации;

– разработка номенклатуры первоочередных межгосударственных стандартов в области защиты общих информационных ресурсов Беларуси и России.

Государственным заказчиком от Республики Беларусь является Оперативно-аналитический центр при Президенте Республики Беларусь. Исполнителями от Республики Беларусь ведутся работы по 16 мероприятиям Программы, в том числе по 7 научно-исследовательским работам (НИР) и 9 опытно-конструкторским работам (ОКР).

Главным исполнителем Программы от Республики Беларусь является Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» (Государственное предприятие «НИИ ТЗИ»). Главному исполнителю Программы, в соответствии с заключенным контрактом, Государственным заказчиком переданы функции по текущему управлению реализацией Программы.

Вместе с тем, Государственное предприятие «НИИ ТЗИ» самостоятельно выполняет ряд мероприятий Программы.

НИР «Разработка основных направлений исследований по совершенствованию системы защиты общих информационных ресурсов Беларуси и России» (шифр «Идеолог») предполагает постоянный мониторинг проводимых исследований в Республике Беларусь по защите общих информационных ресурсов и систем информационно-телекоммуникационной инфраструктуры Союзного государства, формирование предложений по совершенствованию системы защиты общих информационных ресурсов, а также анализ мировых тенденций в развитии систем защиты информации.

В ходе ОКР «Разработка программно-аппаратного комплекса межгосударственной системы управления открытыми ключами» (шифр «Инфраструктура») разрабатывается программно-аппаратный комплекс, предназначенный для решения задач, связанных с предоставлением основных сервисов удостоверяющего центра инфраструктуры открытых ключей для обеспечения юридически значимого обмена электронными документами между юридическими и физическими лицами Республики Беларусь и Российской Федерации. Комплекс будет реализовывать криптографические сервисы по генерации личных и открытых ключей подписи и идентификации, выработку и проверку электронной цифровой подписи, архивирование личных ключей подписи и шифрование с применением технологии разделенного секрета.

Выполнение ОКР «Разработка программно-аппаратного комплекса доверенных центров обеспечения электронного документооборота» (шифр «Доверие») предполагает создание программно-аппаратного комплекса, обеспечивающего трансграничный обмен электронными документами с проверкой электронных цифровых подписей, созданных с использованием различных стандартов (алгоритмов), проверкой действительности сертификата открытых ключей и выработки квитанций. Комплекс обеспечит оказание потребителем услуг доверенной третьей стороны при обмене электронными документами между Республикой Беларусь и Российской Федерацией.

В результате выполнения ОКР «Разработка устройства криптографической защиты информационного обмена в вычислительных сетях» (шифр «Ручей») будет создано специализированное высокоскоростное аппаратно-программное устройство криптографической защиты конфиденциальной информации в сетях передачи данных, взаимодействующих по протоколу IP V4, IP V6, обеспечивающего криптографическую защиту информационного обмена между локальными сетями и/или отдельными станциями. При этом защищенные устройством сегменты локальных вычислительных сетей и отдельных ПЭВМ образуют единую высокоскоростную виртуальную сеть передачи конфиденциальной и служебной информации ограниченного распространения.

Кроме работ, выполняемых Государственным предприятием «НИИ ТЗИ», к наиболее значимым разработкам текущей Программы можно отнести:

– создание программно-аппаратного комплекса обнаружения и локализации радиопередающих средств технических систем несанкционированного съема информации (шифр «Озон»), исполнитель ОКР – ООО «СЕНКОМ СИСТЕМС»;

– создание программно-аппаратной платформы архива электронных документов (шифр «Архив ЭД Система»), исполнитель ОКР – ООО «ЛайтВелОрганизейшен»;

– разработка и изготовление высокоскоростного малогабаритного генератора случайной числовой последовательности гарантированного качества на физическом источнике шума (шифр «Ключ-ВС»), исполнитель ОКР – НИИ ПФП им. А.Н. Севченко;

– разработка аппаратного модуля криптографической защиты информации ограниченного распространения (шифр «Астра»), исполнитель ОКР – ЗАО «НТЦ Контакт»;

– разработка устройства активной защиты аналоговой и цифровой речевой информации по низкочастотным каналам (шифр «Бас»), исполнитель ОКР – ЗАО «НТЦ Контакт».

Наряду с выполнением опытно-конструкторских работ белорусскими исполнителями мероприятий Программы проводится ряд научно-исследовательских работ, направленных на совершенствование единой научно-технической политики по защите общих информационных ресурсов Беларуси и России. Продолжается работа по развитию единой российско-белорусской системы документов, регламентирующих деятельность по обеспечению защиты общих информационных ресурсов Беларуси и России от информационных угроз (НИР шифр «Обмен», исполнитель – ЗАО «Авест»); по разработке дополнений и расширений к отечественным и международным стандартам в области криптографической защиты (НИР шифр «Секрет», исполнитель – Учреждение БГУ НИИ ППМИ).

Учреждением БГУ НИИ ППМИ проводится НИР «Разработка методов, алгоритмов и программного обеспечения стеганографической защиты мультимедийной информации с использованием технологии цифровых водяных знаков» (шифр «Знак»). Работа предполагает разработку математических методов, алгоритмов и программного обеспечения встраивания цифровых водяных знаков в графические изображения формата JPEG, в видеофайлы формата MPEG-4, аудиофайлы формата MP3 и мультимедийные файлы.

Кроме того, по НИР «Разработка серии электронных учебных пособий «Математические основы компьютерной безопасности» (шифр «Учебник», исполнитель – Учреждение БГУ НИИ ППМИ) предусмотрено создание 3 новых электронных пособий для подготовки и переподготовки специалистов по специальности «Компьютерная безопасность»:

- «Дополнительные главы теории вероятностей. Дискретные случайные величины и процессы»;
- «Дополнительные главы математической статистики. Оценивание параметров и проверка гипотез о распределениях дискретных случайных величин и процессов»;
- «Теория конечных автоматов».

Таким образом, Программа охватывает все стороны укрепления информационной безопасности Союзного государства и направлена на обеспечение безопасности информации в критически важных системах информационной инфраструктуры Союзного государства, совместный поиск эффективных решений странами участниками Союзного государства, что позволяет прогнозировать и решать возникающие угрозы безопасности информации на уровне мировых тенденций развития технологий.

АКТУАЛЬНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ БЕЗОПАСНОСТИ ОБЪЕКТОВ РАЗЛИЧНЫХ КАТЕГОРИЙ

В.В. Маликов,

**Учреждение образования «Центр повышения квалификации руководящих работников и специалистов»
Департамента охраны МВД Республики Беларусь**

В настоящее время в мире и Беларуси одной из важных не решенных научно-практических задач является обеспечение комплексной безопасности как критически важных объектов информатизации, так и типовых объектов различных категорий с учетом адекватных моделей уязвимостей, мотивации/оснащенности нарушителей, а также разработка обоснованного каталога требований к системам защиты и их компонентам.

С целью оценки уровня информационной безопасности в Беларуси, а также повышения эффективности внедрения и использования средств и систем защиты информации в системах безопасности объектов различных категорий, в УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь совместно с компанией «Softline», журналом «Технологии безопасности», УО «Белорусский государственный университет информатики и радиоэлектроники» проводится исследование, включающее следующие разделы:

1. Статистическое исследование уровня информационной безопасности:

- анализ уровня инцидентов информационной безопасности в Республике Беларусь и мире по открытым источникам;

- статистическое исследование «Республика Беларусь и мировая практика: краткий обзор, основные тенденции в сегменте информационной безопасности»;

- основные направления исследований по обеспечению информационной безопасности объектов различных категорий в Республике Беларусь.

2. Моделирование состояния защищенности объектов различных категорий:

- классификация объектов по типовым группам параметров информационной безопасности с учетом возможного ущерба;

- построение моделей типовых нарушителей, анализ их оснащенности и мотивации;

- построение моделей типовых уязвимостей с привязкой к типовым группам объектов.

3. Экспериментальное исследование надежности средств и систем защиты информации:

- классификация и оценка средств, и систем защиты информации, представленных на рынке Республики Беларусь;

- оценка технической и экономической эффективности использования средств и систем защиты информации в системах безопасности типовых групп объектов;

- моделирование проникновений на типовые группы объектов на основе моделей типовых уязвимостей.

4. Рекомендации по применению:

- повышение эффективности построения и использования систем защиты информации в системах безопасности объектов различных категорий;

- типовая методика проведения аудита систем защиты информации и оценки уровня защищенности объектов различных категорий;

- рекомендуемые для использования средства и системы защиты информации.

Для реализации первого (статистического) раздела исследования анализируются следующие источники данных:

1. Кадровые агентства:
 - вакансии специалистов по информационной безопасности (ИБ);
 - запрашиваемое знание технологий/программного обеспечения (ПО).
2. Ассоциация правообладателей Республики Беларусь, представительства компаний правообладателей ПО/технологий:
 - экспертная оценка уровня лицензионного/пиратского ПО в отраслях экономики;
 - потенциальные/реальные инциденты информационной безопасности: источник – процесс – результат.
 - количественные оценки владения долей рынка в информационных технологиях (ИТ).
3. Управление «К» МВД Республики Беларусь, открытые отчетные данные по преступлениям в сфере высоких технологий в странах СНГ:
 - отчетные данные по структуре преступлений в сфере высоких технологий;
 - описание раскрытых схем преступлений: источник – процесс – результат.
4. Крупные отечественные компании разработчики/интеграторы «Софтлайн», «Белсофт» и др.:
 - статистика продаж/модернизации ПО и услуг по отрасли ИБ;
 - статистика в потребности и фактического обучения по отрасли ИБ.
5. Национальный статистический комитет Республики Беларусь:
 - оценка уровня рынка ИТ, оценка потребления ИТ (физические/юридические лица), затраты на ИТ/ИБ, экспорт ИТ-услуг;
 - результаты реализации «Стратегии развития информационного общества в Республике Беларусь»;
 - основные результаты переписи населения.
6. Базы знаний по уязвимостям и сборники эксплойтов:
 - базы знаний по уязвимостям: ICS-CERT, NVD, CVE, Bugtraq, OSVDB, Mitre Oval Repositories, exploit-db, Siemens Product CERT;
 - сборники эксплойтов: SAINTexploit, Metasploit Framework, Immunity Canvas, Agora Pack, Agora SCADA+, D2 Exploit Pack, White Phosphorus exploit pack, VulnDisco Exploit Pack.
7. Компании «Ernst & Young», «ВирусБлокАда», «Dr.Web», «Лаборатория Касперского»:
 - оценка уровня вирусной активности в Беларуси/СНГ: уязвимые технологии, типовые эксплойты, типовой уровень ущерба;
 - уровень ИБ различных предприятий, типовые схемы реализации атак: источник – процесс – результат.
8. Министерство образования Республики Беларусь (ВУЗы, организации дополнительного образования взрослых):
 - номенклатура/ количество/качество выпускников по ИТ/ИБ;
 - количество ИТ-специалистов, распределенных в государственные/коммерческие организации;
 - тенденции по целевой подготовке ИТ-специалистов по заказам организаций;
 - тенденции по качеству абитуриентов для ИТ-специальностей.

9. Участники Государственных программ Беларуси (до 2020 г.) в сфере ИТ, ИБ, электронного документооборота, систем электронных платежей:

- уровень финансирования программ;
- потенциальные разработки и технологии для использования в реализации программ.

10. Национальный банк Республики Беларусь:

- инциденты ИБ в системах электронных платежей;
- методики прогнозирования, выявления, документирования и расследования инцидентов ИБ.

В настоящее время проведена оценка статистических данных международного исследования в области информационной безопасности за 2012 г., проведенного компанией «Ernst & Young» и подготовлен аналитический обзор «Республика Беларусь и мировая практика: краткий обзор, основные тенденции в сегменте информационной безопасности».

Основные результаты проведенной экспертной оценки:

1. В Беларуси C-level (уровень правления и высшего руководства) направления безопасности представлен, как правило, CSO (Chief Security Officer). CISO себя называют руководители подразделений ИБ, которые, как правило, занимаются только безопасностью ИТ-систем, а не общей информационной безопасностью организации.

2. Основная структура финансово-экономической модели опрошенных фирм (не торгуются на фондовой бирже, локальная территория деятельности), в целом, соответствует общей структуре построения национальной экономики Беларуси на современном этапе.

3. Компетентная оценка уровня информационной безопасности фирм, как правило, выводится по результатам независимого аудита, проведенного на основе международных норм и практик, сотрудниками специализированных агентств. Обязательность проведения таких аудитов, как правило, составная часть требований для IPO и участия в транснациональных бизнес-процессах. Как пример, можно отметить требования со стороны международных платежных систем VISA/MasterCard и др., в части обязательного периодического проведения как внутреннего, так и внешнего аудита на предмет соответствия требованиям стандартов PCI DSS (PA DSS) и др.

4. Учитывая общий уровень затрат на ИБ в Беларуси, эффективность проведения только внутренних аудитов силами специалистов фирм, как правило, не является достаточной по отношению к уровню современных вызовов и угроз сегмента ИБ.

5. Следует отметить, что в Беларуси более 1 млн. долл. США компании на ИБ не тратят. Экономика определяет сущность доходов/расходов. При этом если взять затраты на ИБ менее 0,1 млн. долл. США у 56 % респондентов, то среднемесячные затраты ориентировочно составят 8,33 тыс. долл. США.

6. Отмечается факт незыблемой уверенности «бывших» силовиков МВД, КГБ и др., стоящих у руководства служб безопасности, в свои профессиональные навыки и методы оперативной оценки персонала. Применение запретительных – до 70%, а не технологических мер ИБ подтверждает «силовой» след служб ИБ.

7. Предположение:

а) если оценка внешними организациями (33 %) и оценка в рамках внешнего аудита финансовой отчетности (33 %) являются отдельными (независимыми) внешними аудитами;

б) официальная сертификация на соответствие отраслевым стандартам безопасности (10 %) и официальная сертификация на соответствие внешним стандартам безопасности (10 %) являются отдельными (независимыми) внешними сертификациями;

в) все остальные оценки входят в состав только внутренних или внешних оценок;

г) каждая фирма в той или иной степени проводит внутренний аудит, то численная оценка проведения аудитов только собственными силами составит минимум 14 %.

8. Ограниченность бюджетов на ИБ и, соответственно, уровня оплаты (и лояльности) персонала у нас определяет повышенный риск внутренних инсайдеров.

9. Признание увеличения уровня угроз и уменьшения инцидентов (при минимальных затратах на ИБ) показывает, что около 33-38 % организаций из числа «затраты на ИБ менее 0,1 млн. долл. США – 56 %» находятся в группе высокого риска осуществления инцидентов ИБ со стороны злоумышленников.

Таким образом, дальнейшее проведение указанного выше исследования, позволит получить новые научно обоснованные результаты, которые повысят эффективность внедрения и использования средств и систем защиты информации, а также обеспечат гарантированную защиту объектов различных категорий.

СОЮЗНОЕ ЗАЩИЩЕННОЕ ВЗАИМОДЕЙСТВИЕ: ОТ ТЕОРИИ К ПРАКТИКЕ

А.М. Сапрыкин,
директор ИП «С-Терра Бел»,
представитель НП «Инфофорум»
в Республике Беларусь

Аннотация

Защищенное союзное (межгосударственное) информационное взаимодействие в сложившихся условиях на пространстве Союзного государства (а также ЕЭП, СНГ) наиболее перспективно реализовать на основе национальных технических стандартов для применяемых СКЗИ в сочетании с использованием сервиса доверенной третьей стороны.

Компании «С-Терра Бел» (РБ), «С-Терра СиЭсПи» и «Газинформсервис» (РФ) участвуют в реализации нескольких проектов защищенного информационного взаимодействия министерств, ведомств и организаций Союзного государства.

Проекты: двусторонние и многосторонние сценарии защищенного взаимодействия.

Реалии: возникшие проблемы при реализации проектов по защищенному взаимодействию министерств и ведомств Союзного государства (ЕЭП, СНГ).

Тезисы

Достоинства решений по защищенному информационному взаимодействию на основе национальных технических стандартов:

- нет необходимости в согласовании ТЗ и дополнительной сертификации СКЗИ;

- не требуется политической воли и согласования на уровне правительств;

- защита информации остается в законодательно-правовом поле каждого из государств.

Реалии и проблемы – описание на основе реализуемых в настоящее время проектов по линии взаимодействия ГАИ-ГИБДД, ФСКН-МВД РБ, фондов соцобеспечения и др.

В Минске в июле 2012 года проведена практическая демонстрация трансграничного (межгосударственного) информационного взаимодействия на основе национальных СКЗИ Беларуси и России.

Схема защищенного электронного документооборота при трансграничном защищенном (межгосударственном) информационном взаимодействии.

VPN (IPsec) – универсальная основа организации защищенного союзного (межгосударственного) информационного взаимодействия на основе национальных технических стандартов. Особенности использования сервиса ДТС (DVCS), а также применения ЭЦП.

Проблемы:

- сложность вывоза и ввоза СКЗИ;

- как итог, первые проекты по организации защищенного взаимодействия министерств и ведомств РФ и РБ длительное время «буксуют»;

- различия в условиях применения и уровнях защищаемой информации СКЗИ;

- пока проще использовать международные стандарты.

Существует необходимость в упрощении процедур ввоза-вывоза СКЗИ для союзных проектов (ЕЭП), к примеру, как это предусмотрено в постановлениях Правительства РФ в отношении «контролируемых товаров, предназначенных для технического обслуживания или ремонта морских и воздушных судов» (без согласования).

Группа компаний С-Терра имеет сертифицированные в соответствии с национальными техническими стандартами России, Беларуси (а также Казахстана и Украины) программные и программно-аппаратные VPN продукты, а это означает однородность и совместимость сетевых СКЗИ. Кроме того, наличие общей службы Технического сопровождения на гарантийный и последующий сроки эксплуатации продукции.

Решения компаний «С-Терра Бел» (РБ), «С-Терра СиЭсПи» и «Газинформсервис» (РФ) могут использоваться для организации защищенного союзного (межгосударственного) взаимодействия министерств, ведомств и организаций стран-участниц СГ (а также ЕЭП, СНГ).

О НЕКОТОРЫХ АСПЕКТАХ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРЕДУПРЕЖДЕНИЯ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ В ТЕРРОРИСТИЧЕСКИХ И ИНЫХ ПРОТИВОПРАВНЫХ ЦЕЛЯХ

А.Н. Лепехин, Академия МВД Республики Беларусь,

Д.В. Перевалов, Институт национальной безопасности Республики Беларусь, г. Минск

Анализ текущего законодательства показывает, что тема информации пользуется все большим вниманием законодателя. И это происходит, несомненно, под влиянием требований самой жизни. Информация – важнейший ресурс управления и всех форм жизнеобеспечения общества. И неслучайно, что центральными категориями правовой системы, имеющими особое значение для реализации прав граждан и соблюдения интересов государства в информационной сфере являются: «информация», «информационная технология», «информационный ресурс», «доступ к информации» и «распространение информации».

Вместе с тем, изучение современного состояния нормативного закрепления рассматриваемой проблемы, а научные публикации в данной сфере показали, что не нашли должного юридического закрепления вопросы превенции террористической и противоправной деятельности в информационных сетях, а также регулирование данной сферы общественных отношений.

Результаты эмпирического исследования показывают, что информационным ресурсам, размещенным в информационных сетях, присущи особенности (доступность, анонимность, ограниченный характер контроля и др.), которые позволяют террористам, террористическим группам или организациям модифицировать классические формы террористической деятельности и создают возможность использования их для осуществления преступлений террористического характера и иных противоправных проявлений, способных угрожать целостности государств и дестабилизировать международную обстановку.

По мнению авторов, в условиях современного глобального мира проблема использования информационных сетей в террористических и иных противоправных целях может быть решена путем применения государствами – участниками международных отношений комплекса мер, принимаемых ими как самостоятельно, так и, в целом, в рамках различных международных организаций с помощью широкого спектра сил, средств и методов воздействия со стороны государства и общества. И ярким примером такого международного сотрудничества, является сотрудничество государств-участников Содружества Независимых Государств, осуществляемое в рамках Программы сотрудничества государств-участников Содружества Независимых Государств в борьбе с терроризмом и иными насильственными проявлениями экстремизма, в соответствии с которой были разработаны Рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей (далее ОТКС) для предупреждения их использования в террористических и иных противоправных целях.

В развитие нормативного закрепления обозначенного направления правового регулирования борьбы с терроризмом и иными противоправными деяниями в компьютерных сетях представляется обоснованной разработка в рамках Содружества Независимых Государств Модельного закона об основах регулирования эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях.

Разработка подобного Модельного закона обусловлена следующими обстоятельствами:

1) необходимостью создания условий для эксплуатации сегмента сети Интернет, используемого юридическими и физическими лицами государств-участников СНГ, обеспечивающих невозможность или максимальную затрудненность использования его в террористических и иных противоправных целях;

2) необходимостью создания целостной, законченной, иерархически структурированной и многоуровневой системы нормативных правовых актов, регулирующих эксплуатацию ОТКС в целях недопущения их использования в террористических и иных противоправных целях, как в системе международных правовых актов СНГ, так и в национальных законодательствах государств – участников;

3) потребностью формирования системы субъектов, обеспечивающих безопасную эксплуатацию сегмента сети Интернет, используемого юридическими и физическими лицами государств-участников СНГ, повышения эффективности деятельности составляющих ее компетентных государственных органов, защиты интересов СНГ, прав и законных интересов граждан государств-участников;

4) целесообразностью оптимизации затрат и ресурсов при выработке решений и реализации мер по предупреждению использования ОТКС в террористических и иных противоправных целях.

Таким образом, нормативное закрепление вопросов превенции использования информационных сетей в террористических и иных противоправных целях в форме принятия Модельного закона об основах регулирования эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях, по нашему мнению, позволит обеспечить оптимизацию использования имеющихся средств, информационных, материальных и технических ресурсов и повышение эффективности деятельности компетентных государственных органов в области эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях, а также повысить уровень защищенности прав и законных интересов личности и обеспечения безопасности общества и государства в информационной сфере.

СИСТЕМЫ И СРЕДСТВА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ В СЗИ НСД: СНИЖЕНИЕ ТРУДОЗАТРАТ БЕЗ СНИЖЕНИЯ ЗАЩИЩЕННОСТИ

С.В. Конявская, Д.В. Манзенков,
ОКБ САПР, г. Москва

При внедрении системы терминального доступа (далее – СТД) одним из решающих мотивов является предполагаемый эффект значительного снижения нагрузки на администраторов – как администраторов СБТ, так и сетей, и безопасности информации.

Расчет на снижение трудозатрат и, соответственно, на возможность уменьшения количества обслуживающего персонала вытекает из верных предпосылок – даже при условии построения системы, в которой комплексно защищены все элементы инфраструктуры, действия по настройке и поддержанию функционирования как ресурсов системы, так и ее подсистемы информационной безопасности, в среднем проще и требуются реже. По сути дела, после ввода настроенной системы с заданными правилами разграничения доступа в действие обязанности АИБа должны сводиться к периодическому контролю корректности настроек и анализу журналов событий.

Схематично можно выделить следующие этапы, на которых требуются действия административного персонала:

- 1) ввод в действие и первоначальная настройка системы;
- 2) мониторинг и аудит;
- 3) НШС разных типов;
- 4) ввод в систему нового пользователя;
- 5) изменение прав существующему пользователю;
- 6) существенные изменения системы или требований к ней.

Очевидно, что все работы из данного списка тем менее хлопотны, чем более централизовано управление системой. Именно это является одной из наиболее существенных причин развития от автономных АРМ через классические терминальные системы к терминальным системам с централизованным управлением образами терминальных станций (КАМИ-терминал, Центр-Т или других альтернативных решений, обязательно предполагающих формирование образов и их доставку на рабочие станции пользователей без физического посещения рабочих мест администраторами), разработки и внедрения разнообразных средств централизованного мониторинга и управления различными подсистемами.

Казалось бы, действия, которые необходимо производить на клиентских АРМах, стремятся к нулю – пользователь подключает ШИПКУ и вводит PIN-код. Если необходимо изменить состав поддерживаемого оборудования, терминальных протоколов, адрес терминального сервера – практически любой параметр ПО терминальной станции, изменения эти производятся на специальном АРМе и затем доставляются пользователю без участия администраторов и без работ с терминальной станцией, как таковой. Даже журнал работы терминального клиента до старта терминальной сессии ведется (и, соответственно, анализируется) централизованно: на Сервере хранения и сетевой загрузки.

Однако поскольку в обязанности администраторов информационной безопасности (далее – АИБ) входит разблокировка сессии пользователя после неверного ввода последнего паро-

ля, разблокировка ШИПОК после превышения допустимого количества вводов неверного пароля, смена паролей, когда пользователь их просто забыл и вспомнить не может, а работать ему надо, и так далее, – на деле оказывается, что АИБы постоянно заняты. Причем для оказания помощи пользователю (разблокировать ШИПКУ или прислонить таблетку администратора, если в качестве терминального клиента используется ПЭВМ), зачастую им нужно отправляться физически в другое здание, которое, возможно, существенно удалено.

Казалось бы, нагрузку такого рода снизить невозможно, и остается только пренебречь ею, поскольку, в конце концов, действия эти не слишком сложные и не требуют значительной квалификации. Сейчас эти задачи решаются организационно.

Однако это негативно сказывается на продуктивности использования рабочего времени – уже не только АИБами, но и пользователями. А в случае с недобросовестными пользователями возможен и осознанный саботаж – заблокировал ШИПКУ и можешь не работать на законных основаниях, терминальная станция не загружается.

Для того, чтобы избежать перечисленных особенностей работы с паролями, можно предложить заменить их на аутентификацию с помощью биометрического признака, который невозможно забыть или потерять.

В качестве конкретной реализации изменения подсистемы аутентификации в этом направлении можно предложить интеграцию в ПАК «Аккорд TSE» биометрической аутентификации на основе сканирования сосудистого русла ладони руки.

Технология построена на методе верификации, то есть не поиска эталона, соответствующего предъявленному признаку, по базе данных, а сравнения предъявленного рисунка сосудистого русла с предъявленным же эталоном, который записан в персональный идентификатор пользователя (в зависимости от необходимой архитектуры это может быть ТМ-идентификатор, ШИПКА, смарт-карта).

Пользователь подносит руку к сканеру и совмещает идентификатор со считывателем (прислоняет ТМ-идентификатор, подключает ШИПКУ или устанавливает смарт-карту в считыватель). Из идентификатора система получает эталон, со сканера – предъявляемый биометрический признак, производится верификация, результат которой обрабатывается Аккордом, как пароль пользователя.

Метод верификации с предъявленным эталоном, в отличие от поиска подходящего эталона в базе, позволяет избежать создания базы биометрических персональных данных, которая, помимо всех прочих следствий из сопровождения дополнительной базы данных, еще и является ИСПДн класса К1 и нуждается в соответствующей защите. Очевидно, что создавать дополнительный объект защиты, совершенствуя подсистему защиты информации, не целесообразно.

Кроме того, психологически пользователь больше доверяет верификации, производимой на основе носимого им с собой



контейнера, чем с какой-то виртуальной удаленной базой данных, которую он себе плохо представляет.

Поскольку рисунок сосудистого русла ладони руки не является паролем, хоть и заменяет в системе ввод последнего, на него не распространяются требования к парольной защите. Единственный аспект, который может оказаться противопоставлением к переходу на эту технологию – это невозможность смены аутентифицирующей информации в случае компрометации.

Однако единственной возможностью компрометации этих данных представляется их подмена или считывание в канале между сканером и ПК. Реализация такой угрозы крайне маловероятна, так как для нее потребовалась бы атака с использованием не только глубоких и специфических знаний и навыков, но и сложной измерительной аппаратуры. Для тех рабочих мест, атака на которые злоумышленника, обладающего необходимыми характеристиками, возможна (то есть угроза утечки по этому каналу признается актуальной), следует использовать комбинированный считыватель, совмещающий сканер сосудистого русла со считывателем контактной смарт-карты. В этом случае верификация производится самим считывателем и биометрические данные по соединительному кабелю не передаются.

В предлагаемом решении применяется технология сканирования сосудистого русла PalmSecure фирмы Fujitsu, реализованная на двух типах устройств:

– совмещенный с манипулятором мышь-сканер сосудистого русла, дополненный подставкой для удобства размещения руки



над сканером (PalmSecure). После прохождения верификации мышь вынимается из подставки и используется по назначению; – сканер сосудистого русла, совмещенный со считывателем контактной смарт-карты (PalmSecure).

Характеристики сканера:

Способ сканирования – бесконтактный.

Время аутентификации – менее 1 с.

Коэффициент ложного отказа – 0,01 %.

Вероятность допуска «чужого» – 0,00008 %.

Объем эталонного образца – 860 байт/3,5 Кбайт.

Последняя характеристика имеет ключевое значение для выбора технологии, так как объем памяти идентификатора, в общем случае, весьма невелик, и запись эталонных образов, например, отпечатков 8 пальцев (именно столько рекомендуют хранить производители сканеров отпечатков пальцев) в большинстве видов идентификаторов просто невозможна.

Кроме этого, необходимо отметить очень высокие характеристики точности (чрезвычайно низкий процент ошибок обоих типов) и отсутствие неприятных ассоциаций с данной технологией, в отличие от дактилоскопии.

Все это делает аутентификацию по сосудистому руслу ладони руки привлекательным направлением развития подсистем безопасности информации, в том числе в системах терминального доступа, повышающим комфортность работы пользователя, их психологическую удовлетворенность условиями труда, а также снижающим нагрузку на управляющий персонал системы.

DLP-СИСТЕМЫ : ОБЪЕКТНО-ОРИЕНТИРОВАННАЯ МОДЕЛЬ

**В.А. Артамонов, Е.В. Артамонова,
МНОО «Международная академия информационных технологий» (ООН)**

В основу построения математической модели DLP-системы (системы защиты конфиденциальных данных от внутренних угроз) положим принципы объектно-ориентированного подхода и поэтапной декомпозиции слабо формализуемых сред. Весьма распространенной конкретизацией объектно-ориентированного подхода являются компонентные объектные среды с введением самостоятельных понятий: компонент и контейнер.

Неформально компонент можно определить как многократно используемый объект, допускающий обработку в

инструментальном (в том числе графическом) окружении и сохранение в долговременной памяти.

Контейнеры могут включать в себя множество компонентов, образуя общий контекст взаимодействия с другими компонентами и с окружением. Контейнеры могут выступать в роли компонентов других контейнеров.

Компонентные объектные среды обладают всеми достоинствами, присущими объектно-ориентированному подходу:

– инкапсуляция объектных компонентов скрывает сложность реализации, делая видимым только предоставляемый внешне интерфейс;

– наследование позволяет развивать созданные ранее компоненты, не нарушая целостности объектной оболочки;

– полиморфизм по сути дает возможность группировать объекты, характеристики которых, с некоторой точки зрения, можно считать сходными.

Введенные понятия компонента и контейнера необходимы нам потому, что с их помощью мы можем естественным образом представить защищаемую систему (продукт) ИКТ и сами защитные средства (сервисы безопасности). В частности, контейнер может определять границы контролируемой зоны, задавая тем самым так называемый «периметр безопасности».

Таким образом, руководствуясь изложенными выше принципами, перейдем к поэтапному формированию модели DLP-систем, начиная от политик безопасности, как совокупности правил разграничения доступом (ПРД) субъектов к объектам в рамках контролируемых этими системами контейнеров.

Дискреционная политика безопасности – политика безопасности, основанная на дискреционном управлении доступом, которое определяется двумя свойствами:

- все субъекты и объекты системы идентифицированы;
- права доступа субъектов на объекты системы определяются на основе некоторого внешнего по отношению к системе правила.

Основным способом задания дискреционной политики безопасности является построение таблицы прав доступа субъектов к объектам.

Здесь Права $i-j$ – набор прав доступа субъекта i к объекту j (например, «RWE» – набор прав на чтение (Read), запись (Write) и выполнение (Execute)).

Мандатное разграничение доступа предполагает назначение объекту грифа секретности (метки конфиденциальности), а субъекту – уровня допуска. Доступ субъектов к объектам в мандатной модели определяется на основании правил «не читать выше» и «не записывать ниже». Это означает, что пользователь не может прочесть информацию из объекта, уровень доступа которого выше, чем его уровень допуска. Также пользователь не может перенести информацию из объекта с большим уровнем доступа в объект с меньшим уровнем доступа.

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

Комплекс средств защиты (КСЗ), а в данном контексте мы подразумеваем DLP-систему, при вводе/выводе новых данных должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей

нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов и объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

DLP-сервис должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и иерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в иерархические категории в классификационном уровне объекта.

Реализация мандатных правил разграничения доступа должна предусматривать возможности сопровождения – изменения классификационных уровней субъектов и объектов специально выделенными субъектами (например, «офицерами безопасности»).

В DLP-системе, как в КСЗ, должен быть реализован диспетчер доступа (монитор обращений), т.е. средство, осуществляющее перехват всех обращений субъектов к объектам в пределах выделенного контейнера, а также разграничение доступа в соответствии с заданными ПРД. При этом, решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации. Оценка сложности лингвистического анализа информации покидающей контейнер будет базироваться на модификации формализма Ференца Лейтольда в части более точного моделирования компьютеров и операционных систем [1].

Для этого предлагается сигнатурный метод обнаружения утечки информации из контейнера по строке или подстроке ее кода. Естественно, таким образом невозможно обнаружить так называемые полиморфные утечки. Но для обнаружения обычных или олигоморфных утечек такой способ годится: олигоморфные утечки могут обнаруживаться по строке или подстроке кода расшифровщика. В случаях, когда обнаружение осуществляется по подстроке кода (либо даже по полному коду распаковщика для олигоморфных утечек) возможны ложные срабатывания. Приведем оценку вероятности ложных обнаружений при следующих допущениях:

- длина сигнатуры – N ;
- общая длина анализируемых данных – $L \gg N$;

	Субъект 1	Субъект 2	...	Субъект k	...
Объект 1	Права 1-1	Права 2-1		Права k-1	
Объект 2	Права 1-2	Права 2-2		Права k-2	
...	...	...	...	...	...
Объект n	Права 1-n	Права 2-n		Права k-n	
...	...	...	..	...	...

- количество символов в алфавите – n , и встречаются они в анализируемых данных с равной вероятностью;
- количество контролируемых DLP – системой объектов – M .

В этом случае оценка количества ложных обнаружений будет примерно равна:

$$p \approx L \cdot M \cdot \frac{1}{n^N}.$$

Можно также подсчитать вычислительную сложность алгоритма, выполняющего поиск утечек по сигнатуре. Для выполнения поиска требуется последовательно сравнить все ячейки анализируемой строки данных с первыми ячейками сигнатур. В общем случае, это $L \cdot M$ сравнений. Далее, при обнаружении совпадения потребуется провести сравнение со второй ячейкой сигнатуры. Учитывая вероятность совпадения значения первой ячейки, количество сравнений второй ячейки будет

$$L \cdot M \cdot \frac{1}{n}.$$

Аналогично, третьей:

$$L \cdot M \cdot \frac{1}{n^2}.$$

и т. д. Общее количество сравнений составит

$$\begin{aligned} s &= L \cdot M \left(1 + \frac{1}{n} + \frac{1}{n^2} + \dots + \frac{1}{n^{N-1}} \right) = \\ &= L \cdot M \cdot \frac{\frac{1}{n^N} - 1}{\frac{1}{n} - 1}. \end{aligned}$$

В худшем сценарии, когда все сигнатуры полностью различны, а n и N достаточно велики, количество сравнений составит $s = L \cdot M \cdot N$. Следовательно, сигнатурный поиск может быть выполнен за полиномиальное время. Необходимо понимать, что полученные оценки приблизительны и соответствуют худшему варианту поиска случайной подпоследовательности в случайной последовательности. На практике код программы анализа и код утечки информации не являются случайными последовательностями и с учетом знания их структуры алгоритм поиска может быть существенно оптимизирован, а оценка времени уменьшена.

Проблема обнаружения утечек эвристическими методами

Определение 1. Проблема обнаружения утечек по интерфейсу ввода/вывода информации является задачей теории алгоритмов: существует ли эвристический алгоритм, с помощью которого можно было бы определить произошла ли утечка информации, или нет.

Предполагается, что все данные о структуре программ и машины, на которой они выполняются доступны (очень сильное предположение с нашей стороны – ибо большинство эвристических алгоритмов и программ в обнаружении утечек недоступны. И данное действие сродни шаманству в его закрытом исполнении). Неизвестными являются только данные о наличии утечек. Согласно

тезису Тьюринга-Черча (в нашей его модификации), если бы существовал алгоритм обнаружения, можно было бы создать Машину Тьюринга (с одной лентой), которая бы выполняла этот алгоритм. Покажем, что такой Машины Тьюринга не существует.

Определение 2. Машина Тьюринга с одной лентой может быть определена, как совокупность семи элементов:

$$T = \langle Q, S, I, d, b, q_0, q_f \rangle,$$

где Q – множество состояний Машины Тьюринга, S – множество символов, которые могут быть записаны на ленте, I – множество символов входящей последовательности, $I \in S$, $b \in S \setminus I$ – пустой символ, q_0 – начальное состояние Машины Тьюринга, q_f – конечное состояние Машины Тьюринга, $d: Q \times S \rightarrow Q \times S \times \{l, r, s\}$ – множество функций перехода, которые состоянию и символу ленты ставят в соответствие новое состояние, новый символ и перемещение по ленте: на шаг влево, на шаг вправо, остаться на месте. Машина начинает свою работу в состоянии q_0 и в дальнейшем меняет состояния согласно функциям перехода в зависимости от текущего состояния и значения ячейки ленты. Попутно ячейки ленты перезаписываются новыми значениями согласно тем же функциям перехода. Машина Тьюринга может содержать и большее количество лент, но вычислительная способность такой машины будет находиться в полиномиальной зависимости от вычислительной способности Машины Тьюринга с одной лентой.

Теорема 1. Не существует Машины Тьюринга, которая могла бы определять наличие утечки контейнера ввода/вывода в произвольной программе.

Доказательство. Рассмотрим программу P , которая эмулирует работу Машины Тьюринга (произвольной). Программа P печатает на выходе 1, если эмулируемая Машина Тьюринга завершает свою работу. Построим простой алгоритм утечки, который сперва запускает программу P на случайном, но фиксированном (для данной утечки) входе B , после чего начинает выполнять собственно часть контейнерного ввода/вывода. Используя эту конструкцию можно создать программу V для любой Машины Тьюринга, и эта программа будет программой утечки в том случае, если она сможет произвести несанкционированный ввод/вывод информации, т. е. в том случае, когда Машина Тьюринга завершает свою работу на фиксированном для программы V входе или, что тоже самое, если программа P печатает единицу для данной Машины Тьюринга и данного входа. Предположим, что существует Машина Тьюринга, способная обнаруживать все факты несанкционированной утечки информации, т. е. такая Машина Тьюринга T , которая читает код программы ввода/вывода и печатает 1, если в коде этой программы содержится код несанкционированного вывода (утечки), и печатает 0, если этого кода нет. Применим машину T к программе V . Если T печатает 1, значит, программа P и соответствующая ей Машина Тьюринга завершают свою работу на некотором входе B . Если T печатает 0, значит, программа P и соответствующая ей Машина Тьюринга никогда не завершит свою работу на некотором входе B . Учитывая, что вход B и эмулируемая программой P Машина Тьюринга могут быть любыми, получаем, что Машина Тьюринга T способна для любой Машины Тьюринга и любого входа определить, завершит ли данная Машина Тьюринга работу на данном входе. Однако мы знаем, что это невозможно. Полученное противоречие доказывает теорему.

Заключение

Из вышеизложенного видно, что используя различный математический аппарат нами получен эквивалентный вывод о неразрешимости абсолютного определения факта несанкционированной утечки информации через периметр абстрактного наперед заданного контейнера, т.е. не существует алгоритма, который бы позволил однозначно определить является ли ввод/вывод инсайдерским. Речь идет даже не о нехватке ресурсов, а о принципиальной невозможности создать подобный алгоритм. В связи с этим

проблема естественным образом переходит из теоретической области в практическую, где применяются частные решения для задач обнаружения утечек. В частности решаются задачи определения утечек по сигнатурам или используются эвристические алгоритмы, а это уже искусство нежеле, наука.

Литература:

1. Материалы статьи «Формализм Ф. Лейтольда». [Электронный ресурс] – Режим доступа: <http://ra32.ru/>.

СТАТИСТИЧЕСКИЕ И НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

**А.И. Трубей, В.А. Дмитриев, В.В. Анищенко,
ОИПИ НАН Беларуси, г. Минск**

История поиска информационных излучений по техническим каналам началась в далеком 1918 году, когда известный американский криптоаналитик Герберт Ярдли был привлечен для исследования методов обнаружения, перехвата и анализа сигналов военных телефонов и радиостанций. Проведенные исследования позволили установить, что подобное оборудование обладает демаскирующими излучениями, которые могут быть использованы для перехвата секретной информации. По мере развития технологий совершенствовались как средства перехвата ПЭМИ, так и средства защиты от перехвата ПЭМИ. В ход идут всевозможные методы маскировки: использование ППРЧ, расширение спектра сигнала до шумоподобности, сверхкороткие выходы в эфир в наиболее безопасное время, выходы в частотные диапазоны, не подвергающиеся контролю со стороны служб защиты. Уже в середине 80-х годов отмечены случаи применения иностранными спецслужбами «закладок» с частотой излучения до 40 ГГц. Технические разработки становятся все более совершенными, алгоритмы передачи информации позволяют создавать устойчивые, не подверженные помехам каналы связи на гораздо более высоких частотах, чем ранее.

В зависимости от природы информационного сигнала можно провести следующую классификацию ТКУИ, обрабатываемой СВТ [1, 2]:

1. Естественные технические каналы утечки информации:

1.1. ТКУИ, возникающие за счет побочных (паразитных) электромагнитных излучений (электромагнитные каналы утечки информации).

1.2. ТКУИ, возникающие за счет наводок побочных (паразитных) электромагнитных излучений (электрические каналы утечки информации).

2. Специально созданные технические каналы утечки информации:

2.1. ТКУИ, создаваемые путем высокочастотного облучения СВТ.

2.2. ТКУИ, создаваемые путем внедрения в СВТ электронных устройств перехвата информации («закладных устройств»).

Особенностью средств радиоперехвата является то, что они ориентированы на поиск произвольных по характеристикам радиоизлучений. Основным способом обнаружения таких сигналов является пороговый энергетический метод, а наиболее важной проблемой его реализации – способ выбора порога обнаружения.

Обеспечение защиты информации от утечки по техническим каналам выполняется тремя основными методами: пассивным, активным или их комбинацией. Пассивный метод заключается в экранировании источника излучения, использовании фильтрации на линиях, а также радиопоглощающих материалов в экранированных объемах. Активный метод предполагает применение специальных широкополосных передатчиков помех.

Защищенность информации, обрабатываемой СВТ, от утечки по электромагнитным каналам обеспечивается при выполнении следующего условия [3].

$$\delta \leq \delta_n, \quad (1)$$

где δ – отношение сигнал / шум при обработке сигналов, излучаемых СВТ на входе приемника;

δ_n – предельно допустимое (пороговое) значение отношения сигнал / шум.

Большинство генераторов шума обеспечивает защищенность СВТ с большим запасом, то есть:

$$\delta \ll \delta_n. \quad (2)$$

Это приводит к значительному засорению эфира, борьба за чистоту которого является важнейшей задачей. В Европе вообще запрещено применение генераторов шума как средств активной защиты [3]. Поэтому необходимо применять адаптивные по мощности и спектру к уровню опасных сигналов генераторы шума, которые, с одной стороны, обеспечивают гарантированную защиту информации, а с другой – не засоряют эфир. Для адаптации генератора шума с целью маскировки электромагнитного излучения СВТ необходимо провести расчет пороговых значений δ_n . Нужно выбирать генераторы под конкретные СВТ, интенсивность излучения шума которых обеспечивается условием:

$$\delta \approx \delta_n. \quad (3)$$

В качестве критерия для оценки возможностей средств радиоперехвата будем использовать вероятность обнаружения сигнала P_o . Данная вероятность характеризует возможность средств радиоперехвата при фиксированной (допустимой) вероятности ложной тревоги $P_{лт}$ осуществить выделение сигнала на фоне шума на входе приемника.

Эффективность радиоперехвата, в конечном счете, определяется требуемым отношением сигнал / шум на входе приемника. В общем случае, это отношение обусловлено параметрами радиоприемного устройства, уровнем сигнала, условиями распространения радиоволн. В частности, многолучевое распространение радиоволн в условиях городской застройки снижает показатель эффективности по отношению к потенциально достижимому в 20 – 30 раз. В таблице 1 приведены вероятности обнаружения сигналов P_o для различных статистических и нейросетевых алгоритмов [4].

Установлено, что статистические алгоритмы обеспечивают фиксированное значение вероятности ложной тревоги $P_{лт} \leq 10^{-3}$. Вероятность ложно тревоги для сети Хемминга без параметра – $P_{лт} \leq 10^{-4}$. [4]. При этом, следует отметить, что для ведения радиоперехвата значения вероятностей $P_{лт}$ должны лежать в диапазоне $10^{-6} - 10^{-3}$.

Проведем обоснование критериев оценки возможностей по скрытию информации, обрабатываемой СВТ (работы на излучение радиоэлектронных средств, информации, передаваемой радиоэлектронными средствами). При определенных допущениях (процесс на входе приемного устройства является случайным и подчиняется нормальному закону распределения, база сигнала – $\Delta F_{np} T_a \geq 10$, $T_a \leq T_{лт}$, значимость ошибок первого и второго рода одинакова и т.д.) вероятность правильного обнаружения сигнала с неизвестными параметрами P_o можно рассчитать по формуле [5]

$$P_o = \Phi \left| \frac{\delta \sqrt{\Delta F_{np} T_a} - \Phi^{-1}(1 - P_{лт})}{1 + \delta} \right|, \quad (4)$$

где ΔF_{np} – полоса пропускания тракта приемника, Гц;

T_a – время осреднения (анализа) процесса, с.

Выбор порогового значения $P_{оп}$ целесообразно осуществлять с точки зрения минимизации вероятности полной ошибки, которая рассчитывается по формуле [5]:

$$P_{ош} = P^*(1 - P_o) + (1 - P^*)P_{лт}, \quad (5)$$

где P^* – априорная вероятность наличия сигнала на входе приемного устройства.

Анализ формулы (5) показывает, что для случая наибольшей неопределенности ($P^* = 0,5$) значения вероятностей полной ошибки $P_{ош}$ становятся соизмеримыми с вероятностями правильного обнаружения сигнала P_o ($P_{ош} \approx P_o$) при $P_o \approx 0,33(1 + P_{лт})$.

Поэтому в качестве порогового значения при решении задач обнаружения сигнала целесообразно принять значение вероятности правильного обнаружения $P_{оп} \approx 0,33(1 + P_{лт})$.

Для обеспечения достаточной для инженерных расчетов точности ошибка измерения $P_{ош}$ не должна превышать от значения вычисляемой величины ($P_{ош} \leq 0,05 P_o$). Поэтому при решении задачи измерения параметров сигнала в качестве порогового значения вероятности получим $P_{оп} \approx 0,91(1 + P_{лт})$.

Из формулы (4), получаем предельно допустимое (пороговое) значение отношения сигнал / шум на входе приемного устройства [5].

$$\delta_n = \frac{\Phi^{-1}(P_{оп}) + \Phi^{-1}(1 - P_{лт})}{\sqrt{\Delta F_{np} T_a} - \Phi^{-1}(P_{оп})}. \quad (6)$$

Средний интервал между ложными тревогами рассчитаем по формуле [5]:

$$T_{лт} = \frac{\sqrt{12}}{\Delta F_{np}} \exp \left(\frac{[\Phi^{-1}(1 - P_{лт})]^2}{2} \right). \quad (7)$$

В таблице 2 приведены результаты вычислений по данной формуле при решении задачи скрытия сигнала $P_{оп} \approx 0,33(1 + P_{лт})$, а в таблице 3 – при решении задачи скрытия передаваемой информации $P_{оп} \approx 0,91(1 + P_{лт})$ (при $T_a \approx T_{лт}$).

Сравнение значений отношения сигнал / шум, вычисленных для конкретного объекта СВТ (при заданных значениях вероятностей обнаружения сигнала и ложной тревоги), с полученными пороговыми значениями позволяет оценить уровень надежности технической защиты информации (если $\delta \leq \delta_n$, то полагаем, что перехват информации невозможен). Это позволит обосновать целесообразность использования тех или иных технических

Таблица 1 – Зависимость вероятности обнаружения сигнала от отношения сигнал / шум

Алгоритм	Отношение сигнал/шум										
	0.001	0.3	0.5	0.6	0.7	0.8	1	1.2	1,5	2	3
Статистические алгоритмы											
Минимаксный	0.5	0.51	0,697	0,815	0,912	0,965	0,999	0,999	0,999	0,999	0,999
Байеса	0.5	0.56	0,8	0,92	0,97	0,99	0,999	0,999	0,999	0,999	0,999
Знаковый	0.5	0.505	0,525	0,561	0,6	0,648	0,754	0,878	0,968	0,999	0,999
Ранговый	0.5	0.507	0,567	0,617	0,709	0,801	0,942	0,994	0,999	0,999	0,999
Сеть Хемминга с параметром	0.5	0.715	0,857	0,9	0,92	0,94	0,965	0,99	0,993	0,999	0,999
Сеть Хемминга без параметра	0.5	0.51	0,538	0,611	0,699	0,8	0,91	0,976	0,999	0,999	0,999
РБФ-сеть	0.5	0.759	0,913	0,943	0,966	0,977	0,988	0,993	0,997	0,999	0,999
Карты Кохонена	0.504	0.532	0,638	0,68	0,712	0,73	0,745	0,746	0,746	0,748	0,75

Таблица 2 – Зависимость δ_n от $P_{лг}$ при скрывании (факта наличия) сигнала

Вероятность ложной тревоги $P_{лг}$	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
Отношение сигнал/шум δ_n	0,128	0,055	0,022	0,008	0,003	0,0012

Таблица 3 – Зависимость δ_n от $P_{лг}$ при скрывании передаваемой информации

Вероятность ложной тревоги $P_{лг}$	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
Отношение сигнал/шум δ_n	0,235	0,088	0,032	0,012	0,004	0,0014

средств защиты и исключить из дальнейшего рассмотрения неопасные средства перехвата или воздействия на информацию, а также избежать излишнего засорения эфира при применении активных мер защиты. Аналогичные результаты получены также для скрывания ПЭМИ видеосистемы и клавиатуры компьютера.

Литература:

1. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная техника. – 2010. – № 2. – С. 39–56.
2. Нагорный С.И., Артамошин С.А. О применяемых технологиях предотвращения утечки информации по тех-

ническим каналам // Защита информации. Inside. – 2012. – № 2. – С. 82–86.

3. Акимов В.И., Данилов Н.С., Суворов П.А. Предложения по созданию адаптивных генераторов шума системы зашумления информативных сигналов средств электронно-вычислительной техники // Специальная техника. – 2012. – № 3. – С. 9–13.

4. Прасолова А.Е. Нейросетевые и статистические алгоритмы в задаче обнаружения сигналов // Телекоммуникации. – 2010. – № 2. – С. 2–6.

5. Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам // Специальная техника. – 2006. – № 6. – С. 53–61.

ИЗОЛЯЦИЯ ПРИЛОЖЕНИЙ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ПОРТАТИВНЫХ УСТРОЙСТВ

В.Ю. Коваленко, Д.А. Костюк,
БрГТУ, г. Брест

Одной из особенностей встраиваемых систем (ВС) является их длительное функционирование без перезагрузки и/или какого-либо специфического обслуживания. Поэтому для ВС часто характерны повышенные требования к надежности работы системного и прикладного программного обеспечения и устойчивости к сбоям, происходящим по вине как пользователя, так и из-за внутренних ошибок, а также достаточно актуальной становится устойчивость к попыткам проникновения и взлома. С другой стороны, для портативных ВС большая длительность работы сочетается с сильно ограниченным сроком работы без подзарядки. Для увеличения срока непрерывной работы от батареи подобные системы часто оснащают весьма ограниченными ресурсами (на текущий момент типичны частоты центрального процессора до 1ГГц, а чаще 200–400 МГц).

Высокой надежности функционирования многозадачной среды можно добиться несколькими путями: использованием только высококачественного и многократно оттестированного кода; изоляцией от внешних сетей, включая Интернет, использованием дополнительных средств защиты, таких как супервизоры, фаерволы, антивирусные программы. Однако ни одно из решений не является универсальным, а их совокупность оказывается слишком ресурсоемкой для работы на портативном устройстве.

Одним из способов добиться приемлемой производительности при высокой изоляции приложений друг от друга является виртуализация, подразумевающая запуск приложения в изолированной среде (англ. sandbox), когда его действия жестко контролируются виртуальной машиной (ВМ) [1]. Приложение изолировано от других программ и взаимодействует с ними через специальные интерфейсы,

а доступ к ресурсам (памяти, портам и т.д.) инкапсулируется и также находится под контролем. В настоящее время это решение широко используется на серверах и высокопроизводительных системах, периодически применяется на рабочих станциях, однако, оно пока не характерно для маломощных портативных систем [2].

В настоящее время в сегменте ВС наблюдается интенсивный рост доли систем под управлением Unix-подобных операционных систем (ОС), в первую очередь, GNU/Linux. Для данного класса программных платформ, благодаря их длительному доминированию в сегменте серверов, сравнительно легко реализуем ряд подходов, обеспечивающих изоляцию отдельных программных компонент и, таким образом, повышающих общую надежность функционирования системы. В рамках данной работы нами выполнена адаптация одного из таких решений для нужд портативных ВС, работающих под управлением GNU/Linux.

Виды виртуализации зависят от того, насколько полно осуществляется эмуляция аппаратного обеспечения для виртуализированной ОС или приложения, и сильно различаются по степени потребления ресурсов хост-системы. К наименее ресурсоемким относятся следующие разновидности:

– частичная или нативная (native) виртуализация предполагает, что виртуальная машина имитирует лишь то количество аппаратного обеспечения, которое необходимо, чтобы она могла быть запущена изолированно; подход позволяет запускать гостевые ОС, разработанные только для той же архитектуры, что и у хост-системы;

– паравиртуализация избавляет от необходимости симулировать аппаратное обеспечение, однако, вместо этого используется специальный программный интерфейс для

взаимодействия с гостевой ОС, а сама гостевая ОС должна быть модифицирована, чтобы его использовать;

– виртуализация уровня приложений предполагает, что в ВМ запускаются не гостевые операционные системы, а отдельные приложения с необходимыми элементами для работы (файлами реестра, конфигурационными файлами, пользовательскими и системными объектами); этот подход применим только если виртуализованное приложение написано для той же ОС, которая установлена на хост-системе, но зато позволяет добиться высокой производительности при совпадении аппаратных архитектур гостевой и хост-систем.

Для сформулированной задачи наиболее разумно использовать именно метод виртуализации уровня приложений – изоляции (контейнеров, jail), который позволяет значительно повысить производительность и скорость отклика системы [3]. Контейнеры представляют собой специальные изолированные области, как в оперативной памяти, так и на системном диске без возможности доступа к внешним ресурсам и данным. При старте программа запускается внутри этого пространства и ее ошибки никак не влияют на работу других программ или самой системы. Также, реализуется изоляция от атак с помощью зараженных приложений (невозможность выйти за предел контейнера). Это справедливо и для такого критически важного параметра, как процессорное время, распределение которого между контейнерами тоже может контролироваться.

Существует несколько реализаций технологии контейнеров, но наиболее подходящей для портативных ВС под управлением ОС GNU/Linux, на наш взгляд, является технология lxc. В своей работе lxc не использует напрямую ни регистры процессора, ни какие-либо другие аппаратные особенности аппаратуры, на которой исполняется. Работа полностью основана на высокоуровневых особенностях ядра Linux, которые, в силу легкой портируемости этой операционной системы, делают продукт легко переносимым.

Предлагаемый подход был опробован в рамках разработки в Брестском государственном техническом университете информационно-вычислительной системы по наблюдению и прогнозированию наводнений [4], в состав которой входит портативный электронный терминал, позволяющий использовать беспроводные коммуникации и

систему позиционирования GPS для отображения паводковой ситуации и ее прогноза применительно к точке нахождения оператора, либо для автоматизированного ввода результатов изменений с автоматическим определением их геолокации и включением точки измерения в банк данных сервера [5].

По результатам тестирования разработки можно сделать следующие выводы:

– выбранная технология изоляции приложений практически не влияет на производительность системы (потеря находится в пределах нескольких процентов);

– повышается устойчивость к сбоям внутри приложений и попыткам нарушения работоспособности системы в целом.

Литература:

1. Костюк, Д.А. Построение прозрачных виртуализованных окружений для изоляции уязвимых программных систем / Д.А. Костюк, С.С. Дереченник // Комплексная защита информации: матер. XVI научно-практич. конф., Гродно, 17–20 мая 2011 – г. Гродно, 2011. – С. 209–212.

2. Калиновский, Р.В. Технология виртуализации для смартфонов. Сборник конкурсных научных работ студентов и магистрантов / Р.В. Калиновский, Д.А. Костюк (науч. рук.). – Часть 1. – Брест: изд-во БрГТУ, 2007 – С. 99–102.

3. Коваленко, В.Ю. Обеспечение повышенной надежности и длительности работы программного обеспечения встраиваемых систем на базе ОС GNU/LINUX / В.Ю. Коваленко // Материалы 8-й Международной молодежной НТК «Современные проблемы радиотехники и телекоммуникаций РТ-2012». – Севастополь, 2012. – С. 369.

4. Волчек, А.А. Распределенная сетевая система отслеживания паводковой ситуации / А.А. Волчек, В.Ю. Коваленко, Д.А. Костюк, Д.О. Петров, Н.Н. Шешко. // Проблемы природопользования: итоги и перспективы: матер. Междунар. науч. конф., г. Минск, 21–23 ноября 2012 г. НАН Беларуси [и др.] – Минск: Минсктиппроект, 2012. – С. 120–123.

5. Коваленко, В.Ю. Разработка системного программного обеспечения для портативного терминала контроля паводковой ситуации / В.Ю. Коваленко // Современные информационные технологии в образовании и научных исследованиях (СИТОНИ-2012). Матер. III междунар. науч.-техн. конф. студентов и молодых ученых / Сб. науч. трудов. – Донецк: ДонНТУ, 2012. – С. 257–261.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В УСЛОВИЯХ СОВРЕМЕННОГО СОСТОЯНИЯ И ДАЛЬНЕЙШЕГО РАЗВИТИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

А.Ф. Мельник,

Государственное предприятие «НИИ ТЗИ», г. Минск

Защита информации от утечки по техническим каналам является одной из важнейших задач в области обеспечения безопасности информации, обрабатываемой средствами вычислительной техники (СВТ). Как известно, под техническим каналом утечки информации (ТКУИ) понимают совокупность источника информации, линии связи (физической среды), по

которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линии связи, и технических средств перехвата информации [1].

Среди всего разнообразия ТКУИ, обрабатываемой СВТ, в настоящее время особое место занимают электромагнитные и электрические каналы утечки информации, к которым

относятся канал побочных электромагнитных излучений (ПЭМИ) и канал электрических наводок на соединительные линии, посторонние проводники, линии электропитания и заземления, выходящие за пределы контролируемой зоны объекта СВТ.

Носителем информации в СВТ является электрический ток, параметры которого (амплитуда, частота либо фаза) изменяются по закону изменения информационного сигнала. При прохождении электрического тока по токоведущим элементам СВТ вокруг них возникает электрическое и магнитное поля. В силу этого элементы СВТ можно рассматривать как излучатели электромагнитного поля, несущего информацию. Причем наиболее интенсивное электромагнитное излучение формирует достаточно протяженные электрические цепи передачи данных, линейные размеры которых сравнимы с длинами волн излучаемых сигналов ПЭМИ и которые, вследствие этого, представляют собой эффективные излучающие антенны. Как правило, такими электрическими цепями являются цепи интерфейсов обмена данными между устройствами СВТ. Частотный диапазон таких ПЭМИ зависит от частот, с которыми информационные сигналы могут циркулировать по цепям блоков, узлов и элементов СВТ.

Если вспомнить недавнюю историю в области защиты цифровой информации, то проблемами обеспечения ее защиты от утечки по каналам ПЭМИ и наводок в бывшем СССР стали основательно заниматься с середины 70-х годов прошлого века.

В то время в СССР наиболее массовыми СВТ общего назначения были электронные вычислительные машины (ЭВМ) производства Минского завода ЭВМ им. Г.К.Орджоникидзе: «Минск-22», «Минск-32» и ЕС-1020. Максимальное быстродействие этих ЭВМ составляло от единиц до нескольких десятков тысяч операций в секунду (по смеси Гибсона), а максимальные частоты тактовых генераторов не превышали единиц мегагерц. Максимальное быстродействие отечественных ЭВМ более высокой производительности на то время не превышало нескольких миллионов операций в секунду (например, ЭВМ ЕС-1060 – 2 млн. оп/с, ЭВМ ЕС-1061 – 4 млн. оп/с, ЭВМ ЕС-1065 – около 10 млн. оп/с).

Максимальная скорость обмена наиболее быстродействующего селекторного канала ввода-вывода ЭВМ Единой системы с накопителями на съемных магнитных дисках составляла от 800 Кбайт/с (в ЭВМ ЕС-1020) до 1300 Кбайт/с (в ЭВМ ЕС-1060) [2].

Появившиеся в конце 80-х годов отечественные ПЭВМ Единой системы также не обладали высокими по нынешним меркам тактовыми частотами и скоростью обмена данными. Так, например, наиболее распространенная ПЭВМ ЕС-1841 имела тактовую частоту микропроцессора 4,77 МГц и скорость обмена с накопителями на жестких магнитных дисках (НЖМД) типа «винчестер» 5 Мбит/с [3].

Соответственно, тактовые частоты процессоров и быстродействие интерфейсов обмена данными широко распространенных в то время стационарных и персональных ЭВМ и определило частотный диапазон, в котором согласно ТНПА по защите информации бывшего СССР должны были проводиться специальные исследования (СИ) СВТ.

В настоящее время, которое характеризуется стремительным развитием информационных технологий, можно выделить следующие две основные тенденции, оказываю-

щие влияние на нынешнее состояние обеспечения защиты информации, обрабатываемой СВТ, от утечки по каналам ПЭМИ и наводок.

Тенденция первая – снижение промышленных радиопомех от СВТ и повышение помехоустойчивости передачи данных.

Жесткое нормирование допустимых значений промышленных радиопомех (т.н. «зеленые» нормы), а также обязательная сертификация СВТ на соответствие международным стандартам по электромагнитной совместимости вынудило разработчиков предпринять ряд мер, направленных на снижение промышленных радиопомех от СВТ в процессе их функционирования. Эти меры коснулись улучшения электромагнитного экранирования устройств и информационных цепей, применения новых разновидностей микросхем с пониженным напряжением электропитания и малыми перепадами выходных напряжений, использования дифференциальных интерфейсов обмена данными с малыми перепадами напряжения, обеспечения выполнения требований по согласованию нагрузок при проектировании узлов и блоков СВТ и т.п. Следует также упомянуть в этой связи разработку новых последовательных интерфейсов обмена данными, основанных на методе низковольтной дифференциальной передачи сигналов (LVDS) и использовании специальных алгоритмов избыточного кодирования (например, в сетях ЛВС Fast Ethernet, в интерфейсах SATA, DVI), что позволило снизить уровни промышленных радиопомех и вероятность перехвата информативных сигналов ПЭМИ от линий передачи данных указанных интерфейсов [4, 5]. В то же время применение специальных алгоритмов кодирования в вышеуказанных интерфейсах вносит специфику в проведение СИ из-за сложности (или невозможности) создания теста, формирующего дискретный линейчатый спектр.

Таким образом, вышеперечисленные меры по снижению уровней промышленных радиопомех от оборудования СВТ и линий передачи данных отдельных интерфейсов при прочих равных условиях повышают защищенность информации, обрабатываемой современными СВТ, от ее утечки по электромагнитным и электрическим каналам.

Тенденция вторая – повышение быстродействия и производительности современных СВТ.

Эту тенденцию рассмотрим на примере ПЭВМ, как наиболее распространенном СВТ для обработки защищаемой информации. По сравнению с приведенными выше техническими характеристиками ПЭВМ ЕС-1841 современная типовая ПЭВМ общепромышленного исполнения имеет тактовые частоты микропроцессора в пределах 2 500 – 3 000 МГц, что значительно выше тактовой частоты микропроцессора ПЭВМ ЕС-1841, которая была равна 4,77 МГц. Однако сама по себе высокая тактовая частота микропроцессора, влияющая на быстродействие и производительность ПЭВМ, практически не влияет на защищенность обрабатываемой микропроцессором информации от утечки за счет ПЭМИ и наводок. Это связано с тем, что уровни ПЭМИ информативных сигналов микропроцессора значительно меньше уровней ПЭМИ от цепей интерфейсов обмена данными, которые вследствие своей протяженности представляют собой эффективные излучающие антенны и поэтому наиболее опасны с точки зрения возможной утечки обрабатываемой информации по электромагнитному каналу.

Если рассматривать эволюцию интерфейсов обмена данными в СВТ, то следует отметить ярко выраженную

тенденцию их развития, направленную на повышение максимальных скоростей обмена данными, а также переход от параллельных к последовательным интерфейсам.

Так, например, параллельные интерфейсы обмена с НЖМД типа IDE, ATA и SCSI в современных ПЭВМ повсеместно заменены на последовательный интерфейс SATA, который имеет следующие модификации:

SATA-1 с пропускной способностью 150 Мбайт/с (1,2 Гбит/с);

SATA-2 с пропускной способностью 300 Мбайт/с (2,4 Гбит/с);

SATA-3 с пропускной способностью 750 Мбайт/с (6,0 Гбит/с).

Легко заметить, что пропускная способность интерфейса обмена с НЖМД SATA-3 более чем в тысячу раз превышает пропускную способность интерфейса обмена с НЖМД ПЭВМ EC-1841.

Совершенствуются также интерфейсы передачи данных для цифровых дисплеев. Так, например, ассоциацией VESA разработан видеоинтерфейс DisplayPort, который рекомендуется к использованию в качестве наиболее современного интерфейса соединения аудио- и видеоаппаратуры и, в первую очередь, для соединения компьютера с дисплеем. Максимальная пропускная способность одного канала видеоинтерфейса DisplayPort составляет 2,7 Гбит/с.

Что касается совершенствования универсального последовательного интерфейса USB в части повышения его пропускной способности, то версия интерфейса USB 3.0 обеспечивает скорость обмена данными до 5 Гбит/с.

В настоящее время первые компьютеры с интерфейсом SATA-3 (с пропускной способностью 6,0 Гбит/с), с интерфейсом USB 3.0 (с пропускной способностью 5,0 Гбит/с), а также с поддержкой интерфейса DisplayPort (с пропускной способностью 2,7 Гбит/с) уже поступили в продажу.

Следует обратить внимание, что рабочие частоты обмена данными интерфейсов DisplayPort и, в особенности, SATA-3 и USB 3.0 [6-8] существенно превышают верхнюю границу рекомендуемого частотного диапазона проведения СИ СВТ (1800 – 2000 МГц), обрабатывающих информацию ограниченного распространения, не содержащую сведений, составляющих государственные секреты [9]. Можно предположить, что в процессе дальнейшего повышения производительности СВТ эта проблема будет обостряться.

Таким образом, вышеперечисленные меры, предпринятые разработчиками СВТ по повышению пропускной способности интерфейсов обмена данными, а также повсеместный переход на последовательные интерфейсы, создают в настоящее время реальную угрозу утечки информации ограниченного распространения, которая может обрабатываться в СВТ общих информационных ресурсов Союзного государства через электромагнитный канал в виде ПЭМИ от вышеуказанных интерфейсов.

Кроме того, рабочие частоты интерфейсов SATA-3 и USB 3.0 уже попадают в СВЧ-диапазон, проведение СИ в котором может иметь свои особенности, в настоящее время не достаточно изученные и опробованные на практике. В частности, на закон распространения электромагнитных излучений от исследуемого СВТ в СВЧ-диапазоне могут оказывать влияние габаритные размеры проверяемых устройств и, возможно, другие факторы.

Все это требует серьезной научной проработки и проведения соответствующих исследований с целью выработки методик проверки защищенности информации, обрабатываемой современными высокопроизводительными СВТ. Такие работы, например, могут быть проведены специалистами Беларуси и России в рамках Союзной программы по защите общих информационных ресурсов.

Литература:

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М.: Горячая линия. – Телеком, 2005. – 416 с.
2. Единая система ЭВМ, под ред. А. М. Ларионова. – М., 1974.
3. http://ru.wikipedia.org/wiki/%D0%95%D0%A1_%D0%9F%D0%AD%D0%92%D0%9C
4. Бурлаков К.Ю., Демин К.В., Сак В.В., Шакиров М.З. Определение отношения сигнал/шум для ПЭМИ ЛВС типа Fast Ethernet // Защита информации. – Конфидент, № 4-5, 2002.
5. Digital Visual Interface DVI (Revision 1.0). – 02 April 1999.
6. <http://ru.wikipedia.org/wiki/USB>
7. <http://ru.wikipedia.org/wiki/SATA>
8. <http://ru.wikipedia.org/wiki/DisplayPort>
9. Хорев А.А. Оценка эффективности защиты средств вычислительной техники от утечки информации по техническим каналам. – Специальная техника, № 5, 2007.

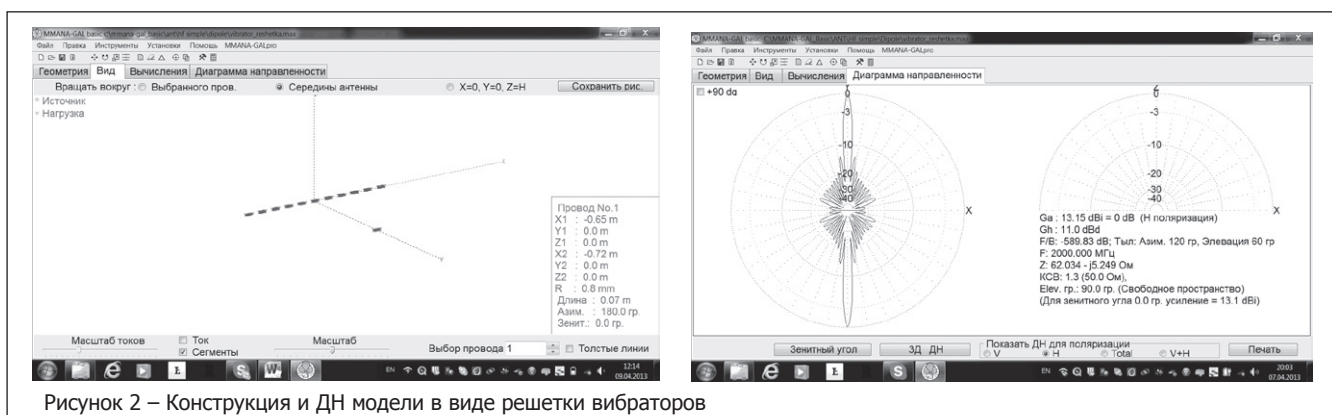
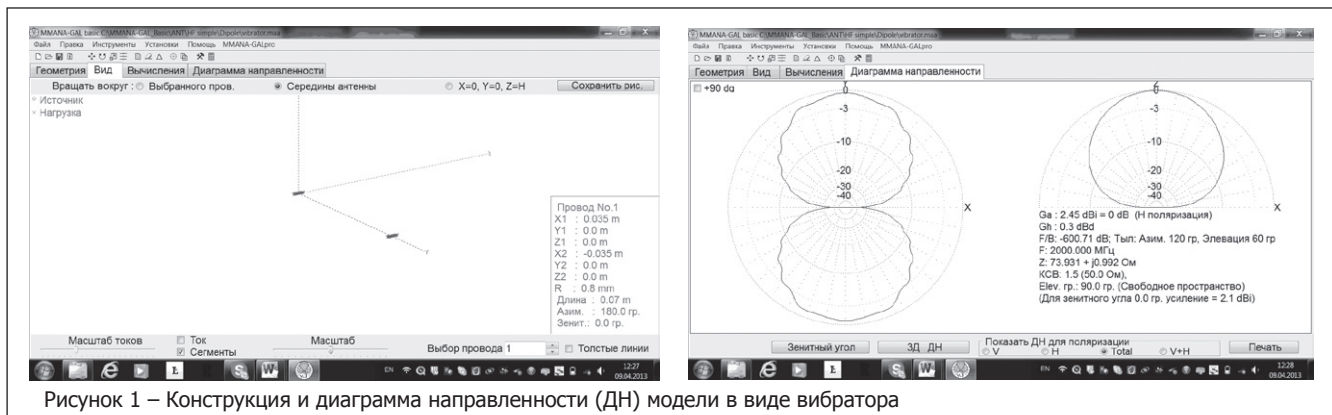
О ПРОБЛЕМАХ ИССЛЕДОВАНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В УЛЬТРАВЫСОКОЧАСТОТНОМ ДИАПАЗОНЕ

В.Э. Яскевич,
НТЦ КГБ Республики Беларусь

Рост скорости обработки информации современными средствами вычислительной техники (СВТ) с неизбежностью приводит к расширению полосы частот их побочных электромагнитных излучений и наводок (ПЭМИН). Причем количественные изменения диапазона частот в сторону его расширения на высоких частотах приводят

к качественным изменениям в требованиях к методикам исследований ПЭМИН.

Рассмотрим одну из сторон этих изменившихся требований – возможность применения аналитических выражений для расчетов электромагнитных полей на основе предварительных их измерений вблизи средств СВТ. Как известно,



Расстояние от излучателя, м	Токи в измерительной антенне для структуры рисунок 1, А	Токи в измерительной антенне для структуры рисунок 2, А
1	$5,25 \cdot 10^{-4}$	$1,56 \cdot 10^{-3}$
5	$1,05 \cdot 10^{-4}$	$9,89 \cdot 10^{-4}$
10	$5,27 \cdot 10^{-5}$	$6,15 \cdot 10^{-4}$

существуют строгие аналитические выражения только для излучения электромагнитных полей элементарными диполями – излучателями, с размерами существенно меньше длины излучаемой ими волны. Эти аналитические выражения активно использовались при исследованиях ПЭМИН СВТ. Оценим ошибку, которая может возникнуть при оценке ПЭМИН в диапазоне ультравысоких частот (УВЧ) на частоте 2 ГГц при использовании для расчетов полей аналитических выражений, описывающих излучение электромагнитных полей диполями. Для этого выполним численный эксперимент, воспользовавшись общедоступным программным обеспечением MMANA-GAL, версия 3.03 5.02.2012. MMANA-GAL – это программа для расчета и анализа любых антенн, которые можно представить, как произвольный набор тонких проводов. Расчет производится методом моментов.

Проведем электродинамический анализ двух проволочных структур, моделирующих процессы исследования ПЭМИН. Принципиально используемая методика позволяет достаточно детально моделировать проводящие конструкции СВТ. Однако воспользуемся простейшими моделями для максимальной оценки исследуемого явления. В первом случае исследуемый объект представим в виде полуволнового вибратора, размером 7 см (рисунок 1). Во втором (рисунок 2) – в виде линейной решетки 11 полуволновых вибраторов, размером 7 см при об-

щей длине излучающей структуры 1,5 м (характерный размер комплекта оборудования настольного персонального компьютера). Полагаем, что вибраторы возбуждаются встроенными в середину генераторами напряжения 1 В, частотой 2 ГГц. В обоих случаях рядом с объектом исследования размещается модель измерительной антенны в виде полуволнового вибратора длиной 7 см. Измерительная антенна включена в матрицу взаимодействия общей электродинамической структуры. Размещая измерительную антенну на разных расстояниях от излучателя и рассчитывая ток в центре измерительного вибратора, мы имеем возможность оценить затухание электромагнитных волн вокруг исследуемых объектов.

В следующей таблице представлены рассчитанные значения токов в измерительной антенне для двух исследуемых структур на трех расстояниях от объекта 1 м, 5 м и 10 м.

Сила тока в измерительной антенне прямо пропорциональна величине электромагнитного поля и, в принципе, возможно найти некий коэффициент антенны для пересчета рассчитанных токов в значение поля. Но так как нас интересуют относительные величины, проанализируем непосредственно силу тока в измерительной антенне. Для модели, представленной на рисунке 1, затухание электромагнитного поля соответствует теории излучения элементарного диполя и происходит обратно пропорционально расстоянию.

Для модели, представленной на рисунке 2, затухание существенно отлично от зависимости $1/R$. Если измерить поле на расстоянии 1 м от структуры, представленной на рисунке 2, а затем воспользоваться теорией элементарного диполя для пересчета его значения на расстоянии в 10 м относительная ошибка будет составлять $20\log(6.15/1.56) = 12$ дБ, причем, результат будет заниженным, что неприемлемо для исследований ПЭМИН.

Безусловно, с точки зрения электродинамики, полученные результаты очевидны. Антенные решетки относятся к апертурным антеннам, и их поля в дальней зоне формирует определенная поверхность. Поэтому измерения в одной точке недостаточны для прогноза распределения электромагнитного поля излучения в дальней зоне. Причем дальняя зона для структуры, представленной на рисунке 2, находится на расстоянии от излучателя $R > 2D^2/\lambda > 30$ м, где D – размер излучателя (1,5 м), а λ – длина волны, равная 15 см.

Важный вывод, который следует из представленного выше анализа – если появляется необходимость исследовать ПЭМИН СВТ в УВЧ-диапазоне от 300 МГц до 3 ГГц, необходимо в корне изменять подход к измерениям ПЭМИН: требуется регистрация поверхностного амплитудно-фазового распределения электромагнитных полей вблизи устройств СВТ и далее на основе теоремы об эквивалентных поверхностных токах выполнять пересчет значения поля в интересующей нас точке. Для измерений здесь сложным моментом является регистрация фазового распределения поля. Последующие расчеты представляют собой интегрирование по поверхности комплексных величин распределения эквивалентных поверхностных токов, что также не является тривиальной задачей. По-видимому, увеличение электрических размеров СВТ в УВЧ-диапазоне с неизбежностью требуют этих методических усложнений.

ВЛИЯНИЕ РЕЖИМА БЕГУЩИХ ВОЛН НА ПРОСТРАНСТВЕННУЮ СТРУКТУРУ ПЭМИ ТЕХНИЧЕСКИХ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ

УДК 621.370

А.Г. Филиппович,

Оперативно-аналитический центр при Президенте Республики Беларусь

Проведено исследование процесса возбуждения ПЭМИ в типовом техническом средстве обработки информации (ТСОИ) методом интегральных уравнений [1]. Процесс моделирования состоял из двух этапов. На первом этапе проводился расчет амплитудно-фазового распределения (АФР) источников поля на проводящих поверхностях ТСОИ. Затем по результатам расчетов АФР рассчитывались диаграммы излучения.

Модель типового ТСОИ [2, 3] показана на рисунке 1. При моделировании в качестве источника ПЭМИ рассматривался видеоинтерфейс. Геометрическое расположение ТСОИ от-

носительно сферической системы координат выбрано так, как показано на рисунке 1.

Моделирование проводилось практически во всем частотном диапазоне ПЭМИ (до 1800 МГц). В результате расчетов установлено, что на частотах свыше 900 МГц на проводящей поверхности ТСОИ устанавливается смешанный режим волн источников ПЭМИ (тока на поверхности кабеля видеоинтерфейса и плотности тока на проводящих поверхностях системного блока и монитора).

На частотах сигнала ПЭМИ свыше 900 МГц отчетливо прослеживается формирование режима бегущей волны. Расчеты показывают, что фазовая скорость бегущих волн источников ПЭМИ в зависимости от частоты колеблется от 96% до 98,8% от скорости света. Это означает, что

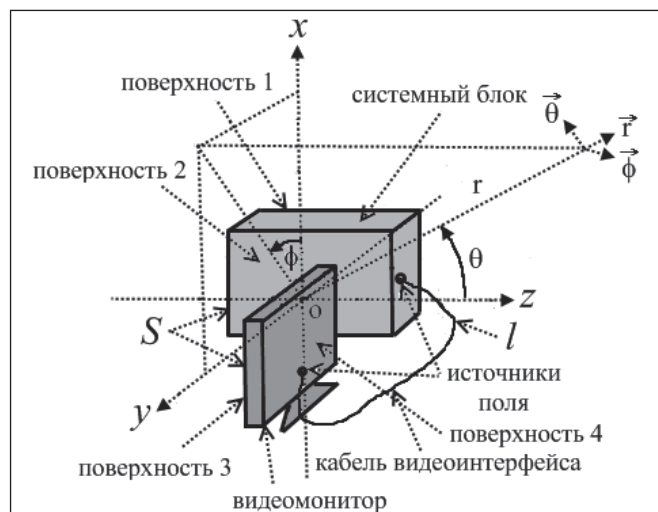


Рисунок 1 – Электродинамическая модель ТСОИ

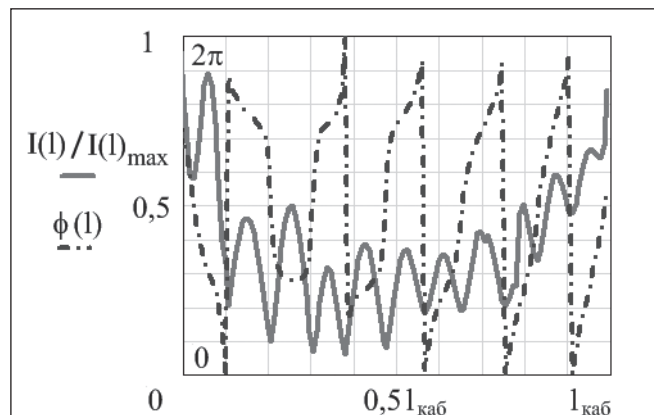


Рисунок 2 – Распределение тока на поверхности кабеля видеоинтерфейса на частоте 1100 МГц

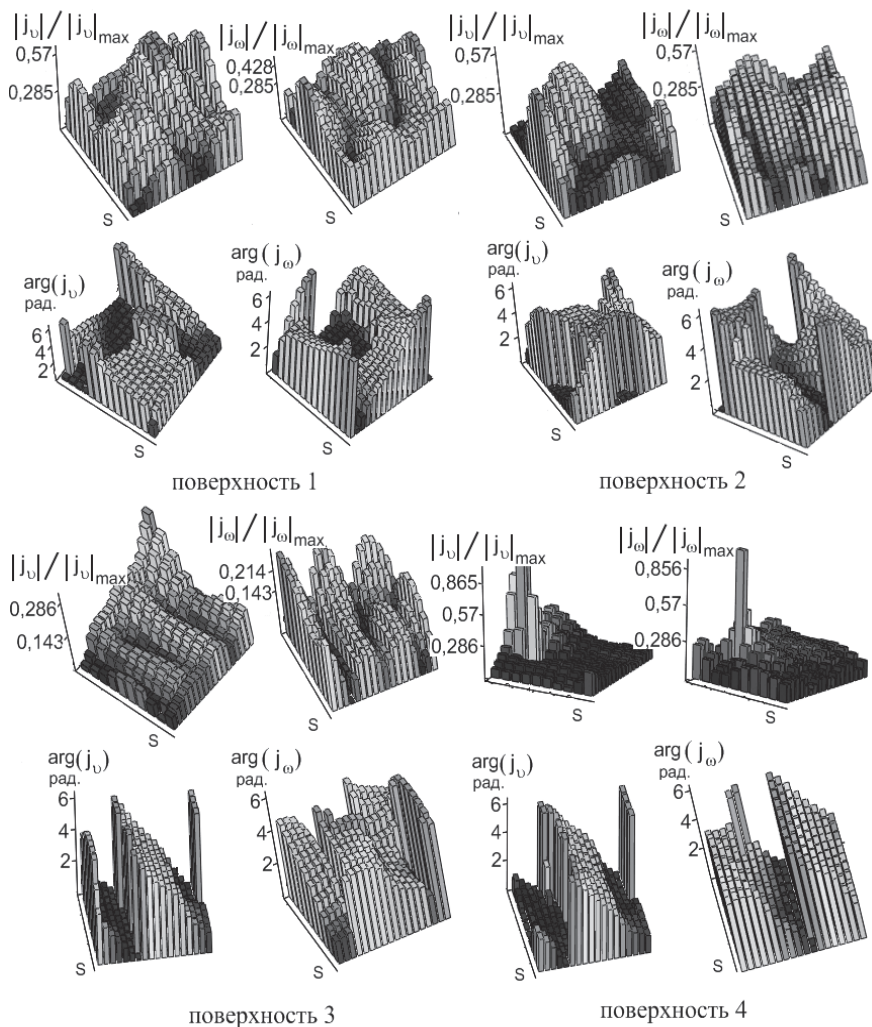


Рисунок 3 – Распределение плотности тока на проводящих поверхностях системного блока и монитора на частоте 1100 МГц

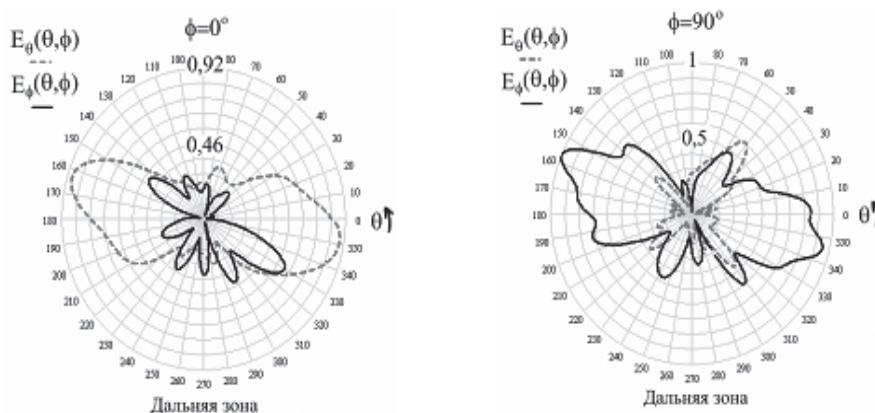


Рисунок 4 – Диаграммы излучения ТСОИ на частоте 1100 МГц

проводящая поверхность ТСОИ выполняет функцию замедляющей системы, вдоль которой происходит направленный перенос электромагнитной энергии. В качестве примера на рисунках 1 и 2 приведены графики амплитудно-фазовых распределений на частоте 1100 МГц.

Возможность направленного излучения ПЭМИ подтверждают расчеты диаграмм излучения ТСОИ для случаев выраженного режима бегущей волны. На рисунке 4 приведены диаграммы излучения на частоте ПЭМИ 1100 МГц, подтверждающие данное положение.

Очевидно, что режим бегущих волн негативно сказывается на степени защищенности ТСОИ от утечки информации по каналу ПЭМИ, поскольку дальность перехвата информации средствами разведки будет увеличиваться за счет направленных свойств ТСОИ как излучателя электромагнитных волн. Для устранения эффекта образования режима бегущих волн видится целесообразным при проведении мероприятий по защите ТСОИ от утечки информации по каналу ПЭМИ предусматривать специальные технические меры:

- проведение дополнительной экранировки разъемов кабелей видеоинтерфейсов;
- применение электромагнитных поглотителей на проводящих поверхностях кабелей видеоинтерфейсов и прилегающих участков поверхностей системного блока и видеомонитора;
- установка четвертьволновых экранов на прилегающих к разъемам поверхностях кабеля видеоинтерфейсов, соответствующих частотам образования режима бегущих волн.

Возможность возникновения режима бегущих волн может быть использована для целей добывания информации. В частности, возникает задача синтеза проводящей поверхности ТСОИ для создания условий возникновения режима бегущих волн и формирования оптимальных диаграмм излучения.

Литература:

1. Филиппович, А.Г. Электродинамическое моделирование систем, состоящих из произвольных идеально проводящих объемных тел и произвольных тонких проводников конечных размеров / А.Г. Филиппович, А.В. Рунов / Физика волновых процессов и радиотехнические системы. – 2011. – т.14. – №2. – С. 39-45.

2. Филиппович, А.Г. Моделирование побочных электромагнитных излучений ПЭВМ методом интегральных

уравнений / А.Г. Филиппович // Доклады БГУИР. – 2012. – №5. – С. 28-34.

3. Филиппович, А.Г. Применение метода интегральных уравнений для оценки защищенности ПЭВМ от утечки информации по каналу побочных электромагнитных излучений / А.Г. Филиппович // Вестник Военной академии Республики Беларусь. – 2012. – №3. – С. 115-123.

КОМПОЗИЦИОННЫЕ ЭКРАНИРУЮЩИЕ ЭМИ-МАТЕРИАЛЫ С ДИЭЛЕКТРИЧЕСКИМИ И МАГНИТНЫМИ ВКЛЮЧЕНИЯМИ

Н.В. Насонова, Я.Т.А. Аль-Адеми, А.А. Ахмед, Л.М. Лыньков,
БГУИР, г. Минск

Экранирующие и радиопоглощающие материалы в области защиты информации применяются для подавления побочных электромагнитных излучений (ЭМИ) средств обработки и передачи информации, образующих каналы утечки информации, как для стационарных, так и для мобильных устройств. Наряду с созданием экранированных помещений из металлических листов все большее применение находят экранирующие композиционные материалы с наполнителями, способные поглощать электромагнитную энергию и уменьшать долю энергии, переизлучаемой в окружающее пространство. Основными видами наполнителей для таких композитов являются проводящие частицы (порошки, волокна и др.) из различных металлов или углерода [1], магнитные частицы (ферриты) [2] или включения материалов с диэлектрическими потерями [3]. Однако электромагнитные характеристики материалов не постоянны и зависят от диапазона частот, влажности, температуры эксплуатации и других факторов [4].

В работах [5, 6] показана перспективность применения водосодержащих композиционных материалов для создания экранов электромагнитного излучения, применяемых в различных областях. Кроме водных растворов, синтезируемых с использованием различных органических и неорганических добавок, обладающих высокой диэлектрической проницаемостью в диапазоне СВЧ, в состав композиционного материала предлагается включить материалы с магнитными потерями в том же диапазоне. Это, в соответствии с условием минимизации отражения электромагнитной энергии от материала с магнитодиэлектрическими потерями [7], приводит к повышению поглощения ЭМИ внутри материала и существенному снижению уровня отражаемой энергии [8].

Цель данной работы заключается в экспериментальном получении соотношения между концентрациями включений с диэлектрическими и магнитными потерями и установлении зависимости экранирующих свойств композиционных материалов от изменения температуры эксплуатации ниже точки фазового перехода воды в твердое состояние, характеризующееся резким понижением величины диэлектрической проницаемости.

Для исследований использовались тканые полотна с вплетенным ферритовым микропроводом, отличающиеся степенью скрутки ферромагнитного микропровода, т.е. концентрацией ферритового материала в объеме ткани (в образце 1 – концентрация феррита ниже, в образце 2 – концентрация выше), заполненные жидким полярным диэлектриком, в качестве которого используется вода.

Измерения экранирующих характеристик проводились на автоматизированном измерителе модуля коэффициентов передачи и отражения SNA 0.01-18 оценкой коэффициентов передачи и отражения волноводного тракта с рупорными антеннами, нагруженного на образец, в диапазоне частот 2...17 ГГц. Модуль коэффициента передачи принимался равным ослаблению ЭМИ.

Водосодержащие образцы с ферритовыми включениями обеспечивают ослабление ЭМИ на 2,8...10 дБ, вследствие диэлектрических потерь воды, распределенной в поровом объеме ткани, и явления естественного ферромагнитного резонанса. При этом доля отражаемой энергии мала – коэффициент отражения ЭМИ композиционными материалами, содержащими ферритовый материал и воду, снизился в среднем на 4 дБ и для образца с меньшей концентрацией феррита находится на уровне -12...-10 дБ в диапазоне частот 3...12 ГГц. Это может быть связано с совпадением поведения характеристик дисперсии диэлектрической проницаемости наноструктурированной воды и магнитной проницаемости используемой ферромагнитной структуры, распределенных в тканой матрице.

Как показывает анализ результатов измерений, приведенных на рисунке, понижение температуры ниже точки льдообразования приводит к снижению величины ослабления ЭМИ с 4...10 дБ до 0...4,5 дБ для образца №1 и с 3...6 дБ до 0...2,8 дБ для образца №2. Это связано со снижением способности молекул воды, встроенных в сетку льда, к ориентационной поляризации под действием внешнего электрического поля, и уменьшению общей диэлектрической проницаемости композиционного материала. Как показано на рисунке б, это изменение электромагнитных характеристик приводит к повышению величины коэффициента отражения из-за нарушения баланса между магнитными и диэлектрическими свойствами материала.

Проведенные исследования показывают, что композиционные водосодержащие материалы с ферритовыми включениями позволяют получить коэффициент отражения ЭМИ до -12...-14 дБ в диапазоне частот 2...17 ГГц путем подбора соотношения между концентрациями частиц, обладающих высокой диэлектрической и магнитной проницаемостью, однако, устанавливают требования по поиску методов стабилизации экранирующих характеристик в широком диапазоне эксплуатационных температур.

Литература:

1. Eggermont, S. Novel frequency selective electromagnetic absorber combining honeycomb waveguide and carbon nanotube composites / S.Eggermont; P.Bollen; N.Quievy, et al, // Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP). – 2011. – Pp.2201 – 2204.
2. Lee, J. Broadband Nix Zn_{0.8}s_{8-x} Cu_{0.2}Fe₂ O₄ electromagnetic absorber for 1 GHz application / J. Lee; Y. Hong; S. Bae, et al. // IEEE Transactions on IEEE Transactions on Vol. 45, Is.10, 2009. – Pp.4230 – 4233.
3. Лыньков, Л.М. Новые материалы для экранов электромагнитного излучения / Л.М. Лыньков, В.А. Богущ, Н.В. Колбун и др. // Доклады БГУИР. – 2004. – Т.2, №5. – С.152–167.
4. Gao, N. Effect of Water Absorption on Dielectric Properties of EPDM/AI(OH) Composites / N.Gao, H. Xie, Z. Peng // Proc. of The 6th International Conference on Properties and Applications of Dielectric Materials, June 21-26,2000, Xi'an Jiaotong University, Xi'an, China. - Vol. 2, 2000. – Pp.905 – 907.
5. Пассивные технические средства обеспечения информационной безопасности от утечки по электромагнитному, оптическому и акустическому каналам / Альлябад Х.М., Пулко Т.А., Насонова Н.В., Лыньков Л.М., под общ.редакцией Лынькова Л.М. – Минск: Бестпринт, 2010. – 225 с.
6. Simulation of electromagnetic radiation passing through liquid-containing nanostructured materials / N.V. Kolbun, T.V. Borbotko, A.A. Kazeka, A.M. Proudnik, L.M. Lynkou // Proc. of SPIE. – 2009. – Vol. 7377-0A.
7. Казанцева, Н.Е. Перспективные материалы для поглотителей электромагнитных волн сверхвысокочастотного диапазона / Казанцева Н.Е., Рывкина Н.Г., Чмутин И.А. // Радиотехника и электроника. – 2003. – Т. 48, №2. – С.196-209.
8. Ponomarenko, A.T. Modeling of electrodynamic properties control in liquid-impregnated porous ferrite media / A.T. Ponomarenko, N.G. Ryvkina, N.E. Kazantseva et al. // Proc. of SPIE. – 1999. – Vol. 3667. – Pp. 785-796.

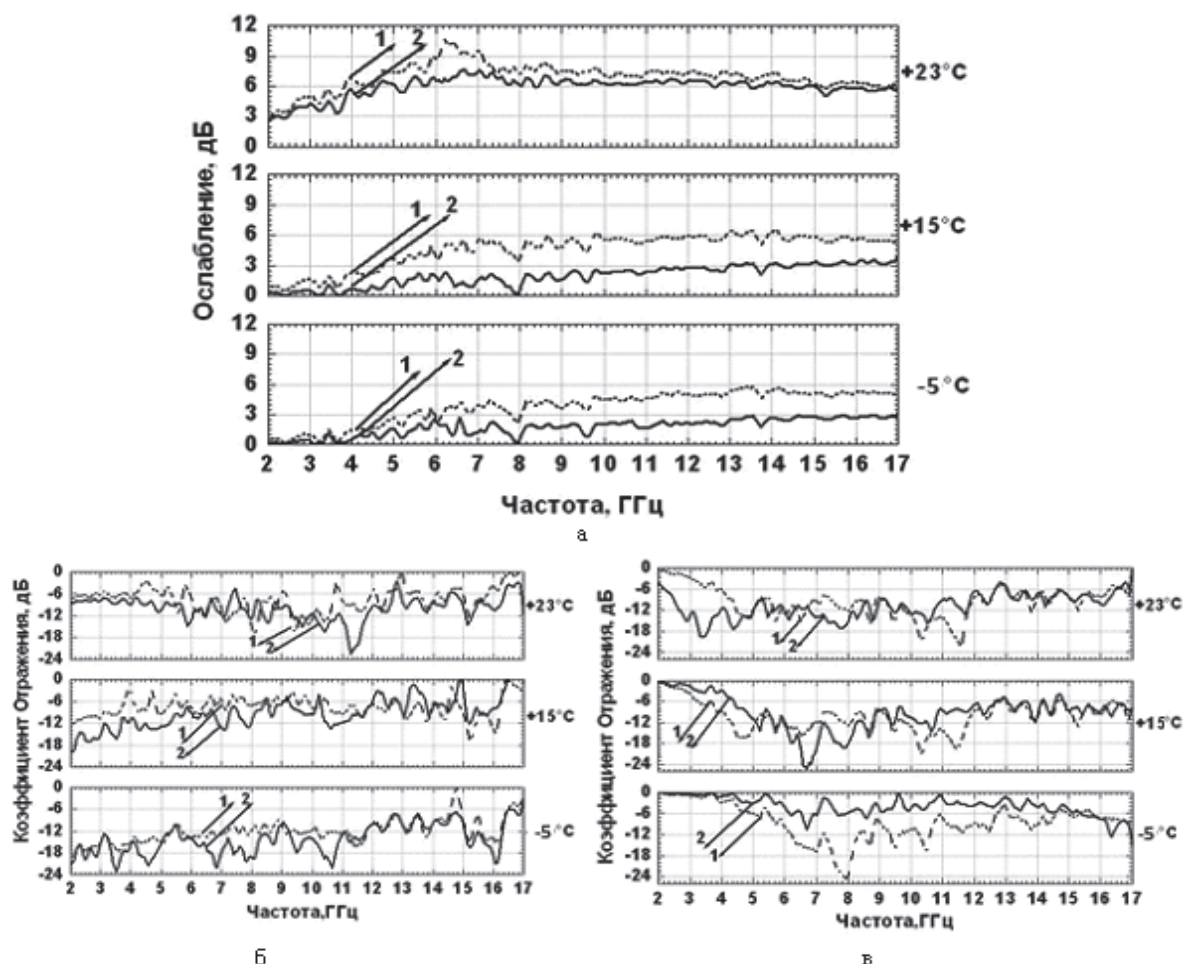


Рисунок 1 – Частотная зависимость экранирующих характеристик ослабления ЭМИ (а) и коэффициента отражения ЭМИ в режиме согласованной нагрузки (б) и КЗ (в) композиционных водосодержащих материалов: 1 – образец 1; 2 – образец 2 при разных температурах

МОБИЛЬНЫЙ ГЕНЕРАТОР ЭЛЕКТРОМАГНИТНОГО ШУМА С ПИТАНИЕМ ОТ ПОРТА USB

М.В. Жалковский, А.В. Сидоренко, БГУ, г. Минск

Широкое распространение средств вычислительной техники значительно упрощает решение ряда задач в повседневной жизни, науке и технике. Однако применение телекоммуникационных технологий способствует появлению новых проблем, одной из которых является утечка информации по каналам побочных электромагнитных излучений (ПЭМИ). Эти каналы утечки образуются вследствие наложения информативных сигналов на паразитные сигналы внутренних устройств и блоков средств вычислительной техники.

В литературе выделяют три метода защиты от ПЭМИ: активный, пассивный, а также комбинированный. Последний из указанных методов включает основные мероприятия двух предыдущих [1].

Пассивный метод заключается в экранировании источника излучения, размещении источника излучения в экранированном шкафу или в экранировании помещения в целом.

Активный метод защиты предполагает применение специальных постановщиков помех, которые обеспечивают маскировку ПЭМИ от средств вычислительной техники путем формирования и излучения электромагнитного поля шума в широком диапазоне частот.

Применение генераторов электромагнитного шума становится особенно актуальным при необходимости защиты информации на переносных средствах вычислительной техники (ноутбуках), когда невозможно применение пассивных методов защиты.

При функционировании любого генератора шума мощность шумов, как правило, пропорциональна величине постоянного тока, протекающего по какому-либо шумовому элементу (источнику шумов) [2].

В зависимости от физического источника шума генераторы шума подразделяются на следующие группы:

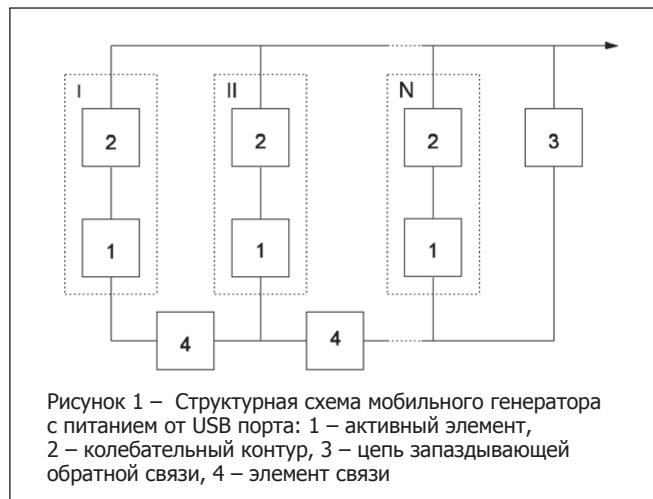
- генераторы шума на элементах с высокой рабочей температурой (генераторы на лампах накаливания);
- генераторы шума на специальном электровакуумном шумовом диоде;
- генераторы шума на полупроводниковом стабилитроне (диоде);
- генераторы шума на биполярных транзисторах;
- генераторы шума на интегральных микросхемах и микросборках.

Наилучшими параметрами из вышеперечисленных генераторов шума обладают генераторы на биполярных транзисторах. Основными элементами при построении указанных генераторов являются колебательная система резонансного типа и широкополосная цепь обратной связи, что обеспечивает условия для возбуждения ряда колебаний основного вида, а также их гармонических составляющих высших порядков и унтертонов [3].

В зависимости от схемотехнических решений выделяют два типа систем генераторов на биполярных транзисторах:

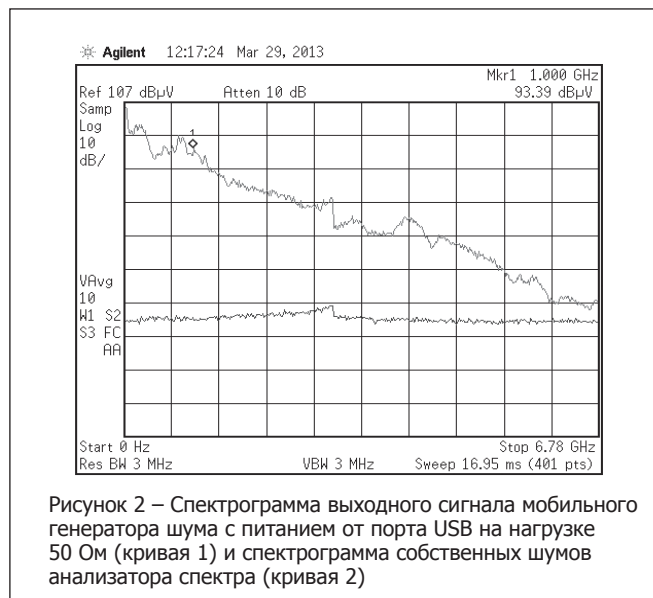
- системы связанных генераторов с идентичными параметрами;
- системы связанных генераторов с различными параметрами.

Предлагаемый мобильный генератор шума с питанием от USB порта состоит из системы связанных генераторов с идентичными параметрами. Структурная схема генератора представлена на рисунке 1.



Система связанных генераторов с идентичными параметрами (рисунок 1) выполняется на основе многотранзисторной конструкции с использованием микрополосковой технологии и содержит: однотипные активные элементы (1), колебательные контуры (2), общую цепь запаздывающей обратной связи с запаздыванием T (3), емкостные элементы связи (4), с помощью которых осуществляется связь между генераторами. Парциальные генераторы отличаются своими рабочими частотами, что определяется их местоположением на плате относительно цепи запаздывающей обратной связи.

Спектрограмма выходного сигнала мобильного генератора шума с питанием от порта USB на нагрузке 50 Ом представлена на рисунке 2.



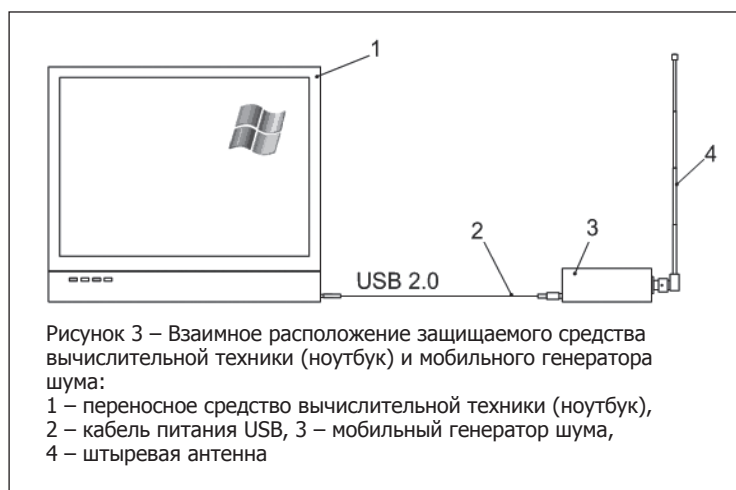


Рисунок 3 – Взаимное расположение защищаемого средства вычислительной техники (ноутбук) и мобильного генератора шума:

1 – переносное средство вычислительной техники (ноутбук),
2 – кабель питания USB, 3 – мобильный генератор шума,
4 – штыревая антенна

Наиболее подходящей излучающей системой, с точки зрения габаритных размеров, массы, простоты конструкции и скорости развертывания, является вертикальный несимметричный вибратор (штыревая антенна). При этом, противовесом антенны служит экранирующая оплетка кабеля питания (USB-кабель).

Взаимное расположение мобильного генератора шума и защищаемого средства вычислительной техники в процессе эксплуатации представлено на рисунке 3.

Алгоритм работы сводится к следующему: во время обработки информации ограниченного распространения переносное средство вычислительной техники (1) переводится в режим автономной работы (работы от внутренней батареи питания), генератор шума (3) присоединяется кабелем к порту USB, подключается и устанавливается в

рабочее положение штыревая антенна (4). После завершения обработки информации ограниченного распространения генератор отключается, а средство вычислительной техники переводится в режим работы от внешнего источника питания.

Таким образом, мобильный генератор шума может обеспечить защиту информации от утечки по каналам ПЭМИ на переносных средствах вычислительной техники без экранирования помещения и доработки компьютерной техники. При этом, пара «генератор шума – переносное средство вычислительной техники» в обязательном порядке должна проходить специальные исследования по методу максимальной оценки (рассматриваться минимально возможная контролируемая зона, наилучшее взаимное расположение генератора и средства вычислительной техники с точки зрения поляризации излучений и др.).

Литература:

1. Домарев, В.В. Безопасность информационных технологий. Системный подход. – Киев: ООО ТИД Диа Софт, 2004. – с. 992.
2. Ван дер Зил А., Шумы при измерениях / А. Ван дер Зил – М. : Мир, 1979. – 292 с.
3. Иванов, В.П., Сверхширокополосные генераторы шума и их практическое применение // Успехи современной радиоэлектроники. – 2008, № 1, с. 37-45.
4. Нечаев, Ю.Б. и др. Антенны, СВЧ-устройства и их применение: учеб пособие / Ю.Б. Нечаев, В.И. Николаев, Р.Н. Андреев, Н.Н. Винокурова: под общей редакцией Ю.Б. Нечаева, В.И. Николаева – 2-е издание. – Воронеж: ОАО Концерн «Созвездие», 2008. – 629 с.

СВЕРХШИРОКОПОЛОСНЫЕ ПРЯМОХАОТИЧЕСКИЕ ПРИЕМОПЕРЕДАТЧИКИ СЕРИИ ППС ДЛЯ СЕТЕЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

А.С. Дмитриев, А.В. Сидоренко, Ю.В. Андреев, К.С. Мулярчик,
ОИПИ НАН Беларуси, г. Минск

Рассматриваются сверхширокополосные (СШП) прямохаотические приемопередатчики экспериментальной серии ППС, предназначенные для передачи информации (данных) как в режиме «точка-точка», так и для построения самоорганизующихся сетей связи.

Приемопередатчики ППС основаны на прямохаотической технологии, предложенной авторами в 2000 г. [1, 2], в которой в качестве носителей информации используются хаотические радиоимпульсы. Приемопередатчики работают в новом нелицензируемом сверхширокополосном диапазоне частот 2,85–10,6 ГГц [3]. Этот диапазон выделен для использования СШП системами связи с полосой не менее 500 МГц на вторичной основе, т.е. спектральная плотность излучения СШП радиопередатчиков должна быть очень низкой, чтобы не оказывать помех существующим в данном диапазоне узкополосным системам связи. В то же время, необходимая для передачи энергетика обеспечивается сверхширокой полосой частот сигнала.

Из-за ограничений на спектральную плотность сигнала дальность связи составляет десятки метров, а основные области применения – беспроводные сенсорные сети сверхмалого потребления, связь персонального уровня, связь внутри зданий и помещений.

Диапазон 2,85–10,6 ГГц является «новым» и незанятым, в отличие от нелицензируемых ISM-диапазонов типа 2,4–2,485 ГГц. Работа в этом диапазоне регулируется международными стандартами IEEE 802.15.4a (низкоскоростные решения для беспроводных сенсорных сетей) и IEEE 802.15.6 (низко- и среднескоростные решения для беспроводных сетей медицинского назначения). В оба эти стандарта входят решения на прямохаотических системах связи.

Приемопередатчики ППС предназначены для передачи цифровых данных различного назначения, включая сенсорные данные, мультимедийные данные (речевые, видео), как в режиме «точка-точка», так и по сети.

Основные параметры СШП приемопередатчиков ППС

- рабочий диапазон частот 3–5 ГГц;
- ширина полосы частот несущего хаотического сигнала 2 ГГц;
- низкий уровень излучения;
- низкое энергопотребление;
- широкий диапазон скоростей передачи данных от единиц Кбит/с до 3–6 Мбит/с;
- дальность 10–30 м;
- соответствие стандартам 802.15.4a, 802.15.6;
- универсальный интерфейс USB; подключение сторонних источников данных по UART, SPI и др.

Низкое энергопотребление приемопередатчиков ППС обеспечивается использованием соответствующих электронных компонентов, программированием спящих (standby) режимов различной «глубины», тщательным планированием энергопотребления элементами приемопередатчика во время рабочего цикла.

Сетевые возможности приемопередатчиков ППС

Основное назначение СШП прямохаотических приемопередатчиков – работа в сети. Функциональные возможности приемопередатчиков обеспечиваются программным обеспечением (ПО), загружаемым в микроконтроллер, управляющий работой приемопередатчика. В настоящее время имеется ПО, позволяющее строить сети разной топологии, от простых сетей, типа «звезда», до mesh-сетей (ячеистых), включая программное обеспечение для построения самоорганизующихся ad-hoc сетей сбора данных, в том числе, мультимедийных. Каждый приемопередатчик ППС способен работать как оконечное устройство, ретранслятор, базовая станция (при соединении с ПК). Благодаря низкому энергопотреблению в ряде приложений мониторинга данных приемопередатчики способны работать до года без замены батарей (при 10% рабочем цикле).

Возможные области применения включают:

- беспроводные сети персонального уровня (UWB WPANs);
- беспроводные сенсорные сети, требующие большого времени автономной работы без замены батарей питания;
- экологически безопасные сети;
- мультимедийные сенсорные сети;
- беспроводные сети медицинского назначения (WBANs);
- самоорганизующиеся сети;
- сети со сложной структурой (Mesh-сети).

Возможности скрытной передачи данных

Особенностью сверхширокополосных приемопередатчиков серии ППС является скрытный характер передачи, который обеспечивается низкой спектральной плотностью излучения, что не позволяет обнаружить сигнал в эфире современными узкополосными средствами на расстояниях более 1–2 м. Кроме того, при физической скорости передачи данных 6 Мбит/с, передача информации со скоростью, например, 100 Кбит/с, осуществляется путем редкой посылки пакетов данных на скорости 6 Мбит/с, поэтому, от-

носительное время передачи составляет 100 Кбит/6 Мбит = 1,67%. Таким образом, дополнительная скрытность передачи обеспечивается за счет редкой передачи пакетов информации.

По сети можно пересылать зашифрованные на более высоких уровнях данные, а при необходимости в программное обеспечение приемопередатчика может быть добавлен слой шифрования данных, получаемых от внешних источников (сенсоров).

В наших работах [4, 5] сообщается об аппаратной реализации алгоритма шифрования на динамическом хаосе, которая выполнена с использованием сверхширокополосных приемопередатчиков ППС-40А.

Линейка СШП приемопередатчиков ППС

В настоящее время линейка приемопередатчиков ППС включает приемопередатчики:

- ППС-40А (базовая модель), скорость 2,5 Мбит/с, дальность 10 м, потребление 40 мВт;
- ППС-42, высокая скорость (до 48 Мбит/с), USB 2.0;
- ППС-43, энергосберегающие режимы, 6 Мбит/с, до 40 м, 10 мВт (на скорости 64 Кбит/с);
- ППС-44, улучшенные энергосберегающие режимы, 6 Мбит/с, до 40 м;
- ППС-50, увеличенная дальность, 2,5 Мбит/с, 60 м.

Наиболее близкие современные аналоги рассматриваемых устройств – это узкополосные устройства Bluetooth и Wi-Fi Direct. Они тоже позволяют создавать прямые соединения, а также работать в составе сетей. Однако они предназначены для работы через ретрансляторы и могут работать только в топологии «звезда». Энергопотребление устройств Wi-Fi Direct находится на уровне традиционного Wi-Fi – не менее 100 мА.

СШП приемопередатчики ППС выгодно отличаются от них тем, что позволяют строить сложные самоорганизующиеся сети, а их потребление как минимум в 3 раза ниже, чем у имеющихся в настоящее время на рынке устройств Bluetooth и Wi-Fi Direct.

Литература:

1. Патент № 2185032 «Способ передачи информации с помощью хаотических сигналов» Приоритет от 27.07.2000 г. Зарегистрировано 10.07.2002 г.
2. Дмитриев А.С., Кяргинский Б.Е., Максимов Н.А., Панас А.И., Старков С.О. Перспективы создания прямохаотических систем связи в радио и СВЧ диапазонах // Радиотехника. – 2000. – № 3. – С.9–20.
3. О результатах работ по конверсии радиочастотного спектра по вопросу использования полосы радиочастот 2,85–10,6 ГГц сверхширокополосными беспроводными устройствами. // Решение ГКРЧ № 09-05-02 от 15.12.2009 г.
4. Сидоренко А. В., Мулярчик К. С. Шифрование данных на основе дискретных хаотических систем и отображений // Доклады БГУИР. – 2013. – № 1. – С.62–67.
5. Сидоренко А.В., Ходасевич А.И., Мулярчик К.С., Андреев Ю.В. Организация сенсорных защищенных сетей для систем управления // Информационные технологии и системы ИТС 2012: Матер. Международной научной конференции, Минск, 24 октября 2012 г. / БГУИР. – Минск. – 2012. – С. 34–35.

ОЦЕНКА ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ ЕЕ УТЕЧКИ ЗА СЧЕТ ПЭМИ КЛАВИАТУРЫ СВТ

**В.А. Дмитриев, В.В. Анищенко, А.Б. Степанян, А.И. Трубей,
ОИПИ НАН**

Актуальность задач защиты информации от утечки по техническим каналам несомненна и занимает ведущее место в общем ряду существующих в области безопасности информации проблем.

Работающее средство вычислительной техники (СВТ), помимо обработки информации, выполняет еще и роль передатчика, передающего в эфир, в том числе и обрабатываемую информацию. Одним из основных поставщиком информации для канала побочного электромагнитного излучения (ПЭМИ) в случае СВТ является клавиатура.

Клавиатура характеризуется достаточно высоким уровнем излучения. Излучение клавиатуры относительно узкополосное и сосредоточено, в основном, в КВ- и УКВ-диапазонах. Наиболее опасными с точки зрения их последующего перехвата являются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате. С помощью этих сигналов могут передаваться, например, пароли пользователей и администраторов системы.

Сигналы данных, которые передаются по тракту USB-клавиатуры, представляют собой непериодическую последовательность прямоугольных импульсов разной длительности, поэтому спектр такого сигнала непрерывный, близкий к шумовому сигналу, а сигналы данных, которые передаются по тракту PS/2 клавиатуры, представляют собой периодическую последовательность прямоугольных импульсов разной длительности, поэтому спектр такого сигнала дискретный [1].

Для оценки защищенности конфиденциальной информации от ее утечки за счет ПЭМИ клавиатуры СВТ необходимо определить отношение сигнал/шум на выходе оптимального приемника (согласованного фильтра) и сравнить его с пороговым (предельным) значением. Для оценки отношения сигнал/шум используется инструментально-расчетный метод, который используется только при исследовании ПЭМИ клавиатуры PS/2, поскольку в USB-клавиатуре невозможно реализовать тестовый режим, позволяющий выделить информативные сигналы из спектра ПЭМИ клавиатуры.

Оценка возможности перехвата ПЭМИ клавиатуры СВТ в открытой печати впервые была рассмотрена в [1]. Однако в этой работе не учитывались реальные условия распространения ПЭМИ клавиатуры СВТ в помещении.

Наличие внутри здания стен, перегородок, мебели, радиоэлектронной аппаратуры, людей и других объектов создает сложную среду распространения радиоволн. Условия распространения ПЭМИ внутри помещений существенно отличаются от условий распространения ПЭМИ в свободном пространстве. Основными эффектами, наблюдаемыми при распространении ПЭМИ внутри помещений, являются многолучевость, обусловленная многократными отражениями радиоволн от стен и других объектов, дифракция на многочисленных острых краях предметов, расположенных внутри комнаты, и ослабление радиоволн. Эти явления создают сложную интерференционную структуру электромагнитного

излучения. Эффекты, наблюдаемые при распространении ПЭМИ, создаваемого клавиатурой компьютера, внутри помещений, приводят к быстрым замираниям амплитуды и фазы, т.е. флюктуациям сигнала ПЭМИ, приходящего к приемнику средства разведки.

Для описания статистических свойств огибающей электромагнитного излучения с быстрыми замираниями используется плотность функции m -распределения Накагами [2], которая определяется по формуле

$$W(U) = \frac{2 \cdot m^m \cdot U^{2m-1}}{\Omega^m \cdot \Gamma(m)} \cdot \exp\left(-\frac{m \cdot U^2}{\Omega}\right), \quad (1)$$

$$m = \frac{\langle U^2 \rangle^2}{\langle (U^2 - \langle U^2 \rangle)^2 \rangle} \geq \frac{1}{2}, \quad (2)$$

$$\Omega = \langle U^2 \rangle, \quad (3)$$

где m – глубина замираний, $\Gamma(\dots)$ – гамма-функция.

При оптимальном приеме импульсного сигнала, каковым является информативный сигнал ПЭМИ клавиатуры, вероятность ошибочного приема (вероятность ложной тревоги) и вероятность правильного обнаружения одиночного импульса определяются по формулам [3]:

$$P_{\text{лт}} = \int_{y_0}^{+\infty} W_n(y) dy, \quad (4)$$

$$P_o = \int_{y_0}^{+\infty} W_{c+n}(y) dy, \quad (5)$$

где $P_{\text{лт}}$ – вероятность ложной тревоги, P_o – вероятность правильного обнаружения, $W_n(y)$ – плотность вероятности огибающей напряжения шума на входе оптимального приемника, $W_{c+n}(y)$ – плотность вероятности огибающей напряжения смеси сигнал + шум на входе оптимального приемника, y_0 – пороговое значение, при превышении которого выдается решение о наличии сигнала.

Для того, чтобы распознать нажатую клавишу, необходимо перехватить ее скэн-код, который передается контроллером клавиатуры в линию передачи данных.

Если импульсы в скэн-коде являются независимыми, то вероятность правильного обнаружения скэн-кода $P_{\text{ск}}$ рассчитывается по формуле [1]:

$$P_{\text{ск}} = \prod_{i=1}^m p_{o,i} \approx (P_o)^m, \quad (6)$$

где $P_{o,i}$ – вероятность правильного обнаружения i -го импульса скэн-кода, m – число бит (импульсов).

Для клавиатуры PS/2 $m = 8$ [1].

Для определения порогового (предельного) значения отношения сигнал/шум используется критерий Неймана-Пирсона, максимизирующий вероятность пра-

вильного обнаружения при заданной вероятности ложной тревоги.

Литература:

1. Хорев А.А. Оценка возможности перехвата побочных электромагнитных излучений клавиатуры компьютера. // «Спе-

циальная техника», № 5, 2011.

2. Тихонов В.И. Статистическая радиотехника – М.: Радио и связь, 1966. – 678 с.

3. Тихонов В.И. Оптимальный прием сигналов – М.: Радио и связь, 1983. – 320 с.

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ НЕПРИМИТИВНЫХ БЧХ-КОДОВ В ЗАЩИТЕ ИНФОРМАЦИИ ОТ ПОМЕХ

УДК 519.711.4(075.8)

В.А. Липницкий,

УО «Военная академия Республики Беларусь», г. Минск

В современную информационную эпоху все аспекты комплексной защиты информации приобрели особую актуальность. Одним из важнейших аспектов является защита информации от разного рода помех и искажений в процессе ее передачи, обработки, хранения. Теория и практика помехоустойчивого кодирования информации возникли в середине XX века.

По прошествии 60-ти лет помехоустойчивое кодирование превратилось в бурно развивающуюся ветвь науки на пересечении теории информации и прикладной математики, опирающуюся на новейшие достижения современной алгебры. Разработана система разнообразных помехоустойчивых кодов с широким спектром параметров, рассчитанных на различные каналы передачи информации. Наибольший интерес и популярность как в теории, так и на практике приобрело семейство линейных кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов).

Близки к совершенным примитивные БЧХ-коды, заданные над полями Галуа $GF(2^m)$, длиной $n=2^m-1$, с проверочной матрицей $H=(\alpha^i, \alpha^{3i}, \dots, \alpha^{(2t-1)i})^T$, где α – примитивный элемент поля $GF(2^m)$. Конструктивное расстояние данного кода равно $2t+1$, он способен исправлять ошибки весом от 1 до t .

Однако реально применяются БЧХ-коды с малыми значениями t , поскольку для их коррекции приходится решать в полях Галуа алгебраические уравнения степени t . Данная процедура является переборной, так как здесь не работают даже самые стандартные формулы для квадратных уравнений.

Достижением белорусской школы помехоустойчивого кодирования является создание теории норм синдромов. Она позволила на порядок уменьшить проблемы «селектора», ввести в практику защиты информации от помех новый параметр – норму синдрома, который вводит промежуточное звено в цепочку «синдром-ошибка». Это звено – норма синдромов – облегчает и систематизирует поиск ошибки, допускает конструктивное расширение спектра корректируемых ошибок, позволяет предложить эффективные методы коррекции ошибок декодерами.

Многие вопросы, связанные со свойствами и применением БЧХ-кодов, требуют дальнейших исследований. Особенно сказанное относится к непримитивным БЧХ-кодам, нередко имеющим корректирующие параметры, существенно превосходящие конструктивные. Данный доклад посвящен перспективам применения и алгоритмам декодирования непримитивных кодов, возможностям реализации предложенных алгоритмов на микропроцессорной технике.

Литература:

1. Соломаа А. Криптография с открытым ключом. – М.: Мир. 1996. – 320 с.

2. Венбо Мао. Современная криптография. Теория и практика. – М.: 2005. – 768 с.

3. Введение в криптографию. /Под общ. ред. В.В. Ященко. – 2-е изд., испр. – М.: МЦМНО: «ЧеРо», 1999. – 272 с.

4. Diffie W. and Hellman M. Multi-user Ciphertext Techniques. – Proceedings of AFIPS National Computer Conference, 1976. – P. 109–112.

5. Diffie W. and Hellman M. New directions in cryptography. – IEEE Transactions on Information Theory. 1976. v. IT – 22. – P. 120–126.

6. Adleman L., Rivest R.L., Shamir A. A method for obtaining digital signatures and Public-key cryptosystems. – Communications on ACM. 1978. v. 21. – P. 120–126.

7. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 328 с.

8. Berlekamp E.R., McEliece R.J. and van Tilborg H.C.A. On the inherent intractability of certain coding Problems. – IEEE Transactions on Information Theory. 1978, vol. IT-24, №3. – P. 384–386.

9. Барг, С. Некоторые новые NP-полные задачи кодирования. – Проблемы передачи информации. 1994, том 30, вып. 3. – С. 23–28.

10. McEliece, R.J. A Public-key cryptosystem based on algebraic coding theory. – DSN Progress Rep. 42-44, Jet. Prop. Lab., California Inst. Technol., Pasadena, CA. – P. 114–116. Jan-Feb 1978.

11. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

12. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона. – Дискретная математика. 1992, т. 4, вып. 3. – С. 57–63.

13. Сидельников В.М. Открытое шифрование на основе кодов Рида-Маллера. – Дискретная математика. 1994, т. 6, вып. 2. – С. 3–20.

14. Карпунин Г.А. О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида – Малера. – Дискретная математика. 2004, т. 16, вып. 2. – С. 79–84.

15. Костелецкий А.В., Липницкий В.А., О проблеме ключей в криптосистеме МакЭлиса-Сидельникова. // Изв. Бел. Инж. Академии. 2005. №3(17)/3. – С. 58–64.

ВЛАГОСОДЕРЖАЩИЕ ПИРАМИДАЛЬНЫЕ КОНСТРУКЦИИ ЭКРАНОВ ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В ПОМЕЩЕНИЯХ БЫТОВОГО И ПРОМЫШЛЕННОГО НАЗНАЧЕНИЯ

Я.Т.А. Аль-Адеми, Т.А. Пулко, Н.В. Насонова,
БГУИР, г. Минск

Негативное влияние источников СВЧ-излучения на организм человека не только в промышленных, но и бытовых условиях требует пересмотра концепции универсальной защиты внутри помещения. Использование для экранирования ЭМИ-металлов вследствие высокой проводимости таких сред может привести к переизлучению электромагнитной энергии и ее проникновению в область за экраном, а также влиянию на сам источник ЭМИ и нарушению условий электромагнитной совместимости (ЭМС) электронного оборудования.

Существующий на данный момент перечень строительных материалов, эффективно экранирующих электромагнитное излучение широкого диапазона частот, ограничен. Такие строительные материалы как кирпич, бетон, шлакоблоки с добавлением кокса, обеспечивают эффективность экранирования от 10 до 20 дБ на каждые 30 см толщины.

Известен защитный экран в виде многослойной конструкции, который состоит из чередующихся слоев изоляционного материала и шунгита, измельченного на фракции от 6 нм до 15 нм. Тем не менее, эти способы недостаточно эффективны для защиты технических средств и человека, и не могут быть использованы в качестве строительных материалов для конструирования экранированных зданий и помещений [1]. Строительный материал на основе гипса с содержанием молотой массы компактированного вспененного графита из интеркалированных соединений графита в количестве от 5 до 50 мас.%, в расчете на сухую массу строительного материала, позволяет достичь защитного ослабления в микроволновом диапазоне длин волн [2]. При создании измерительных безэховых камер и экранированных помещений достаточно часто используется графит, который используется для изготовления цилиндров и конусов различных размеров, закрепляемых на стенах, полу и потолке [3]. Экранирование подобными конструкциями существенно ограничивает полезный объем внутри помещения [4], кроме того, немногие из них отвечают требованиям по технологичности, массогабаритным и эксплуатационным характеристикам, к тому же обладают высокой стоимостью.

На основании анализа эксплуатационных и экранирующих ЭМИ свойств материалов, обладающих свойствами поглощения электромагнитного излучения, для обеспечения защиты информации и электромагнитной безопасности в бытовых и служебных (производственных) помещениях предлагается использовать пирамидальные конструкции на основе гибких пористых полотен, заполненных специальными растворами, которые, в зависимости от исполнения, могут применяться в качестве отделочных панелей (для служебных, выделенных помещений) или самостоятель-

ной экранирующей конструкции (в бытовых условиях). Целью работы является разработка экранирующих ЭМИ конструкций на основе композиционных влагосодержащих материалов, сохраняющих заявленные характеристики независимо от условий эксплуатации, и исследование их экранирующих свойств (коэффициентов отражения и передачи) в диапазоне частот СВЧ.

Экспериментальные образцы экранирующих пирамидальных конструкций изготавливались из влагосодержащих трикотажных матриц ($d \approx 1,6$ мм), на основе которых формировались пирамидальные элементы полые внутри, после чего они устанавливались на основании $0,4 \times 0,4$ м². Высота пирамидальных элементов составляла 0,08 м, что коррелирует с предполагаемыми рабочими длинами волн созданной конструкции. Для заполнения пирамидальных элементов конструкции использовались вода и специальный раствор, обладающие диэлектрическими потерями в исследуемом диапазоне частот. Влагосодержание полученных образцов композиционного материала составляло не менее 65 % mass. Для определения влияния пирамидальной поверхности конструкции на экранирующие характеристики были разработаны контрольные образцы композиционных материалов на основе тех же материалов, но с плоской поверхностью.

Измерения экранирующих характеристик проводились с помощью измерителя модуля коэффициентов передачи и отражения SNA 0.01-18 в диапазоне 0,7...17,0 ГГц. Полосы качания частоты измерителя: при измерении коэффициента отражения S11 - 0,5...3,0 ГГц и 2...18 ГГц, при измерении коэффициента передачи S21 - 0,01...3,0 ГГц и 2...18 ГГц. Количество частотных точек, в которых проводятся измерения, составляет 256 в каждом из указанных диапазонов. Результаты измерений (рисунок 1) показывают, что плоский влагосодержащий композиционный материал толщиной 1,6 мм обеспечивает коэффициент передачи -2,0...-10,0 дБ в диапазоне частот 0,7...6,0 ГГц и -12,0 дБ в диапазоне частот 7,0...17,0 ГГц, при коэффициенте отражения - 8,0 дБ в исследуемом частотном диапазоне.

Ослабление энергии электромагнитного излучения происходит за счет высоких диэлектрических потерь воды в диапазоне СВЧ. Взаимодействие электрической компоненты электромагнитной волны с диполями молекул воды и с диссоциированными ионами компонентов раствора приводит к рассеянию энергии падающей ЭМВ в виде тепловых потерь за счет возникновения токов смещения и токов проводимости в локальных объемах водного раствора, объединенных в пространственную гидродисперсную структуру.

Пирамидальные конструкции экранов из влагосодержащих материалов обеспечивают коэффициент передачи

ЭМИ порядка $-2,0 \dots -22,0$ дБ в диапазоне частот $0,7 \dots 3,0$ ГГц и $-6,0 \dots -30,0$ дБ в диапазоне частот $6,0 \dots 17,0$ ГГц, при коэффициенте отражения $-2,0 \dots -28,0$ дБ во всем исследуемом диапазоне частот (рисунок 1). Повышение общей эффективности экранирования ЭМИ обеспечивается за счет дополнительного рассеяния падающих электромагнитных волн и переотражения их между гранями пирамид. При этом доля энергии электромагнитных волн, распространяющихся в направлении источника существенно снижается и коэффициент отражения такой конструкции меньше по сравнению с экраном с плоской поверхностью, эффективность которого обеспечивается только за счет диэлектрических потерь водного раствора. Синтез водных растворов, компоненты которых подбираются, исходя из требований к эффективности экранирования и эксплуатационным характеристикам, позволяет еще больше снизить коэффициент передачи за счет появления дополнительных потерь на проводимость в полученном растворном наполнителе.

Для испытания на устойчивость эксплуатационных характеристик образцы пирамидальных конструкций подвергались заморозке при температуре морозильной камеры -18°C . Для получения термограммы исследуемых

образцов в пределах среднего и дальнего ИК-диапазонов использовался тепловизор MobIR M4 (разрешение $0,12^\circ\text{C}$), показывающий распределение температурных полей по поверхности образцов элементов конструкций в спектральном диапазоне $8 \dots 12$ мкм. Показано, что экранирующие характеристики разработанных образцов не зависят от снижения температуры до -18°C благодаря понижению температуры замерзания за счет применения в качестве компонентов раствора солей щелочноземельных металлов.

Таким образом, пирамидальная конструкция влагосодержащих экранов позволяет повысить эффективность экранирования ЭМИ в частотном диапазоне $2,0 \dots 8,0$ ГГц в среднем на $10,0$ дБ по сравнению с плоским экраном независимо от температуры, что можно учесть при создании высокоэффективных экранов и поглотителей ЭМИ диапазона СВЧ.

В результате проведенных исследований предложены пирамидальная конструкция экрана ЭМИ на основе растворосодержащих материалов, позволяющая повысить эффективность экранирования ЭМИ в частотном диапазоне $2,0 \dots 8,0$ ГГц в среднем на $10,0$ дБ и снизить коэффициент отражения ЭМИ до $-2,0 \dots -28,0$ дБ по сравнению с экраном

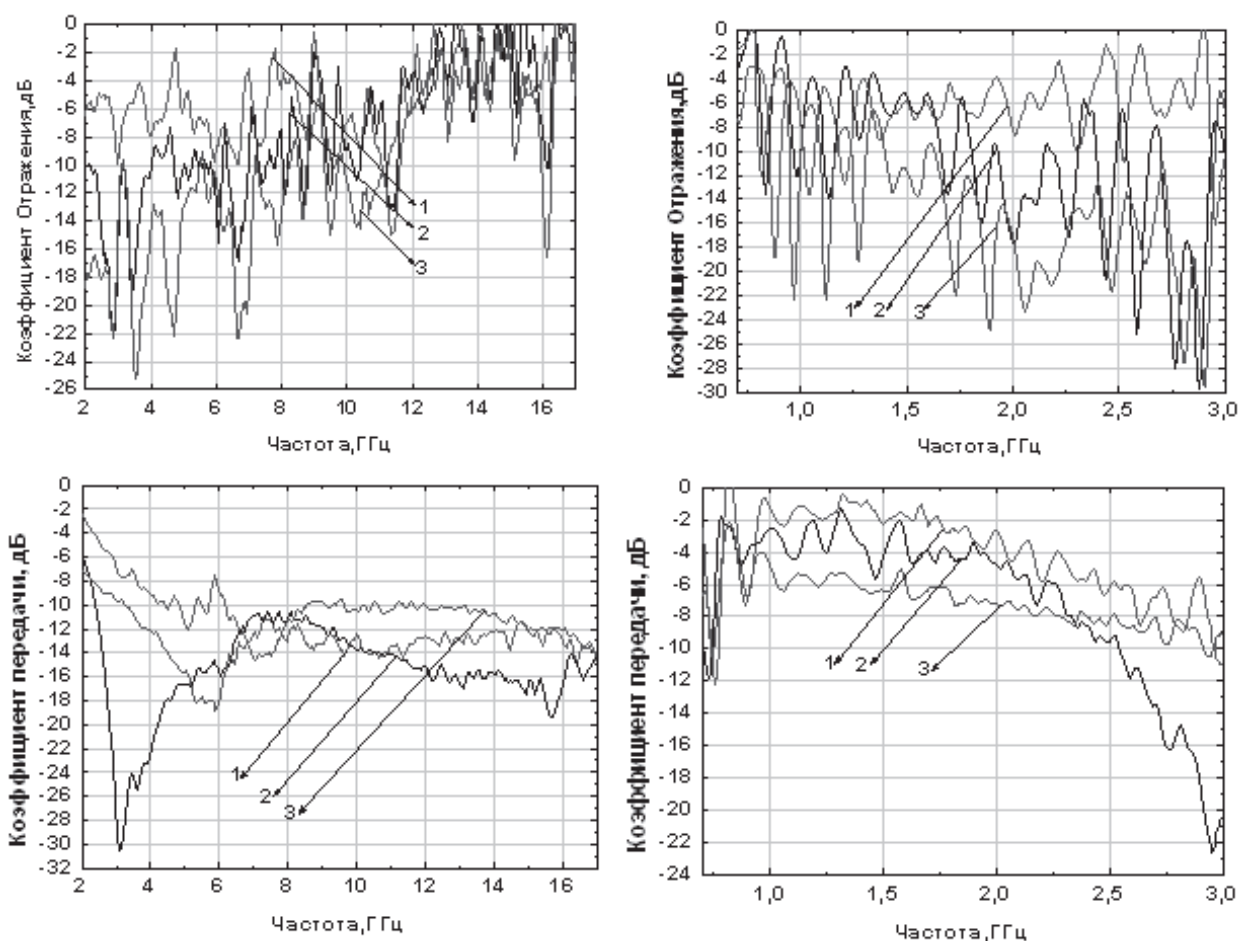


Рисунок 1 – Частотная зависимость экранирующих характеристик образцов в диапазоне $0,7 \dots 17,0$ ГГц:
1 – плоский трикотаж, пропитанный водой; 2 – пирамидальная конструкция экрана, заполненная водой;
3 – пирамидальная конструкция экрана, заполненная специальным раствором

с плоской формой поверхности, что должно учитываться при создании высокоэффективных экранов и поглотителей ЭМИ диапазона СВЧ для электромагнитного экранирования СВЧ-источников и обеспечения экологической защиты обслуживающего персонала и пользователей ПК медицинских и промышленных установок, а также в бытовых условиях.

Литература:

1. Защитный экран от воздействия электромагнитного излучения и способ его изготовления: пат. №2234176 (RU), МПК Н 01 Q017/00 / Штогрин В.И., Швырев Ю.Н., Шатохин А.Н. и др.; Общество с ограниченной ответственностью Научно-техническое внедренческое предприятие «Гироконт» (RU) – №2234176/13; за-

явл.15.02.2010; опубл. 30.10.2010 // Афіційны бюл. / Нац. центр інтелектуал. власності. – 2010. – №7. – С. 21.

2. Пат. 2405750 RU, МПК C04B28/14, C04B111/92. Строительные материалы на основе гипса с повышенной теплопроводностью и ослаблением при экранировании / Гуккерт Вернер, Шпиккерманн Винфрид, Бутц Хайнц-Йоахим, Дуквитц Штефан, Эльтинг Дитер / СГЛ Карбон АГ (DE), Ригипс ГМБХ (DE). – № 2006128334/03, заявл. 03.08.2006; опубл. 10.12.2010.

3. Ковнеристый, Ю.К. Материалы, поглощающие СВЧ-излучение / Ю.К. Ковнеристый, И.Ю. Лазарева, А.А. Раваев. – М.: Наука, 1982. – С. 85.

4. Шнейдерман, Я.А. Зарубежная радиоэлектроника. – 1972. – №7. – 310 с.

НОВОСТИ

MICROCHIP ПРЕДСТАВЛЯЕТ ПЕРВЫЕ ПРОГРАММИРУЕМЫЕ USB2 HUB-КОНТРОЛЛЕРЫ С ОДНОВРЕМЕННОЙ ПОДДЕРЖКОЙ USB2 И HSIC, И РЕЖИМАМИ НИЗКОГО ЭНЕРГОПОТРЕБЛЕНИЯ

Ключевые особенности:

- используя семь новых микросхем, можно выполнить продвинутые зарядные устройства и мост для нескольких последовательных протоколов;
- совмещение интероперабельности, новых особенностей и большого времени жизни аккумулятора;
- ПК, мобильные устройства и мониторы можно сконфигурировать без внешней памяти.

В связи с тем, что компания SMSC вошла в состав Microchip Technology Inc., Microchip анонсирует о расширении линейки USB2 Controller Hub (UCH2). Семь новых, впервые в мире программируемых, USB2 контроллеров из трех семейств, позволяют разработчикам сконфигурировать их приложения, такие как ПК или мобильные устройства, без использования внешней памяти. Более того, это первые в ассортименте Microchip USB2 HUB контроллеры, совместимые с USB2 и USB High Speed Interchip (HSIC) одновременно, поддерживающие режимы энергосбережения, такие как Link Power Management (LPM) и возможность замены настенных зарядных устройств более продвинутыми режимами заряда аккумулятора, такими как BC1.2, Apple®, SE1 и China charging. Для приложений с потребностью в обращении по нескольким протоколам, USB2 HUB контроллеры могут образовывать направленный мост к интерфейсам: I2C™, SPI, UART и вх/вых выводы общего назначения. Для подстройки под различные ОС представленные новинки обладают набором гибких решений, таких как задаваемый потребителем обмен сообщениями и FlexConnect для упрощенной инверсии портов.

Несмотря на то, что рынок ПК переходит на USB3, большинство аналитиков прогнозируют, что USB2 будет преобладать в мобильных устройствах по крайней мере до 2015 года. Это означает, что перед разработчиками ПК и мобильных устройств становится задача совмещения USB3 и USB2, одновременно обеспечивая максимальное

время автономной работы. Все семь новых микросхем UCH2 содержат все необходимое для решения задач совместимости. И пока USB2 HUB контроллеры конкурентов могут предложить только ограниченный набор режимов заряда аккумулятора и требуют внешнюю память для конфигурации, новые UCH2 производства Microchip включают конфигурацию OTP Flash памяти «Quad Page», в которой зарезервировано место для совместимости и других настроек разработчика, включая четыре отдельные возможности конфигурирования. Вдобавок, Microchip представляет ProTouch Configuration Editor software tool, упрощающий создание настроек конфигурации и программирование OTP памяти.

The ProTouch Configuration Editor software tool можно скачать уже сегодня абсолютно бесплатно по ссылке: <http://www.microchip.com/get/2M4E>. Он идет в комплекте с программным обеспечением ProLink. Также уже доступна для покупки отладочная плата для USB2534 (EVB-USB2534), которая позволяет разрабатывать USB зарядные устройства, используя новое, состоящее из трех микросхем USB253X UCH2 семейство, для популярных USB2 приложений.

USB-IF сертифицированные микросхемы: USB2532-1080AEN, USB2533-1080AEN и USB2534-1080AEN – семейство UCH2 для USB приложений общего назначения. Заказ образцов и массовые продажи возможны уже сегодня в QFN корпусах с 36 выводами. Для построения HSIC совместимых и мостовых USB приложений семейство UCH2: USB4624-1080HN и USB4604-1080HN. Заказ образцов и массовые продажи доступны уже сегодня в QFN корпусах с 48 выводами. Для мобильных приложений же разработано семейство USC2: USB3813-1080XY и USB3613-1080XY. образцы доступны уже сегодня, начало массовых продаж ожидается в июле этого года. Выполнены микросхемы в LCSP с 30 выводами.

МАТЕМАТИКА И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ОЦЕНКА КОРРЕКТНОСТИ БЫСТРЫХ АЛГОРИТМОВ ТЕСТИРОВАНИЯ КАЧЕСТВА РАБОТЫ НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД

А.И. Иванов,
ПНИЭИ, г. Пенза

Показано, что гипотеза нормальности распределения расстояний Хэмминга между кодами «Свой» и «Чужие» выполняется тем лучше, чем выше стойкость нейросетевого преобразователя биометрия-код к атакам подбора. Обсуждается предположение о том, что расстояние Хэмминга между кодами «Свой» имеет хи-квадрат распределение с почти нулевым числом степеней свободы. Даны оценки размеров тестовых баз биометрических образов «Свой», использование которых позволит подтвердить гипотезу хи-квадрат распределения с вероятностью 0.9991.

Организационно-технические мероприятия по сохранению в тайне биометрических образов человека делают биометрию высоконадежной. Вторым важнейшим свойством биометрии является ее высокая доступность. Предположительно к перспективным средствам биометрической аутентификации будут предъявляться одновременно и требования высокой надежности к атакам подбора образами «Чужой» и требования высокой доступности по распознаванию образа «Свой».

Оценка стойкости к атакам подбора преобразователей биометрия-код с отключенным механизмом размножения

ошибок в соответствии с ГОСТ Р 52633.3 [1] выполняется по блок-схеме отображенной на рисунке 1.

Обычно использование искусственных нейронных сетей [2] позволяет обеспечить стойкость биометрической защиты на уровне от 103 до 1012 попыток подстановки биометрических образов «Чужой». Если идти по пути традиционных статистических исследований, то для оценки вероятности ошибок второго рода (вероятности коллизии образа «Чужой» и образа «Свой») $P_2=10^{-12}$ придется формировать базу из 1013 биометрических образов «Чужие». Если речь идет об отпечатках пальцев, то для получения базы с 1013 биометрическими образами придется снять отпечатки у всех жителей Земли в 100 поколениях. Время активной жизни одного поколения – 30 лет, соответственно, придется собирать данные 3 000 лет. Пытаться собирать большие базы тестовых биометрических образов – это абсолютно тупиковый путь.

В связи с этой проблемой, ГОСТ Р 52633.3 требует отказаться от примитивных процедур использования больших баз данных и поиска по ним редко встречающихся коллизий «Свой» – «Чужой». Национальный стандарт рекомендует

перейти от статистического исследования кодов «Чужой» в обычном их представлении к статистическому исследованию распределений расстояний Хэмминга между кодами «Чужой» и кодом «Свой»:

$$h = \sum_{i=1}^{256} c_i \oplus x_i \quad (1)$$

где $\oplus$ – операция сложения по модулю два, c_i – i -тый разряд кода «Свой», x_i – i -тый разряд кода «Чужой».

Выигрыш от топологического перехода в пространство расстояний Хэмминга состоит в возможности отказа от тактики ожидания появления редких событий и перейти к тактике предсказания вероятности появления редких событий. Эта возможность опирается на то, что распределение расстояний Хэмминга сравниваемых кодов длиной 256 бит является нормальным.

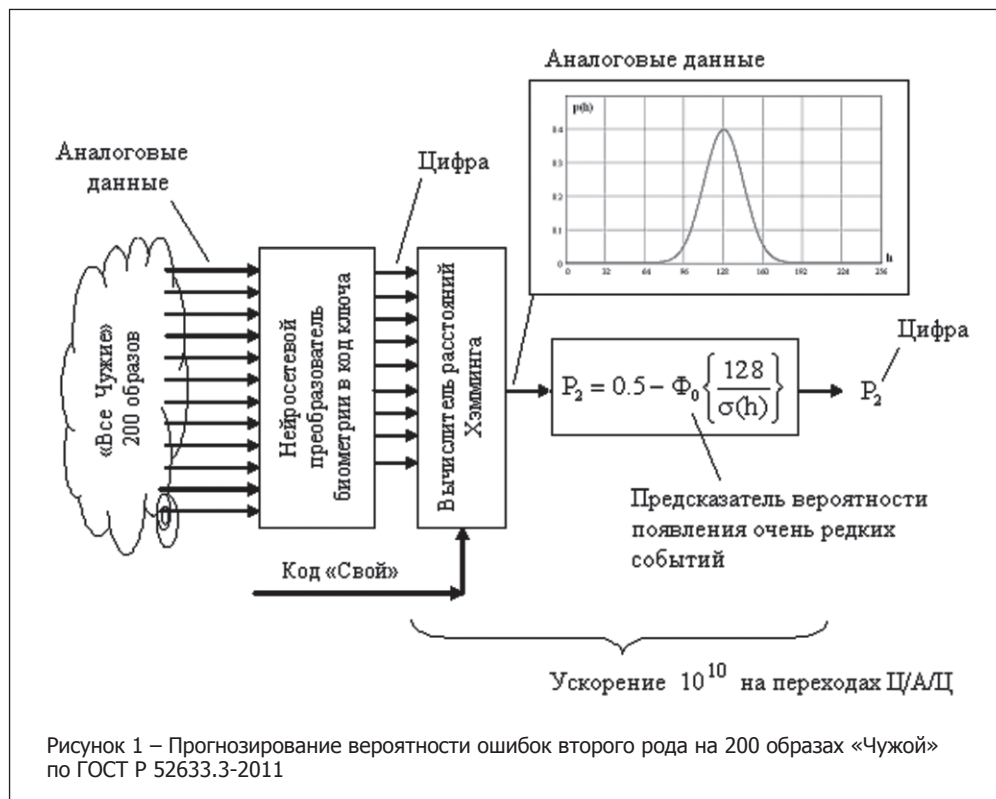


Рисунок 1 – Прогнозирование вероятности ошибок второго рода на 200 образах «Чужой» по ГОСТ Р 52633.3-2011

Для того, чтобы предсказать вероятность появления редкого события $h_i=0$, в рамках гипотезы о нормальном законе распределения значений достаточно вычислить математическое ожидание расстояний Хэмминга и его среднеквадратическое отклонение по выборке, например, из 200 кодов:

$$\begin{cases} E(h) = \frac{1}{200} \sum_{i=1}^{200} h_i \\ \sigma(h) = \sqrt{\frac{1}{200} \sum_{i=1}^{200} (E(h) - h_i)^2} \end{cases} \quad (2)$$

Далее, необходимо вычислить вероятность появления коллизии кодов «Свой» и «Чужой»:

$$P_2 = \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left\{-\frac{(E(h)-u)^2}{2\sigma^2(h)}\right\} du \quad (3)$$

Из-за того, что мы отказываемся от ожидания редких событий и начинаем их предсказывать, возникают огромные ускорения времени вычислений. В частности, отказ от просмотра базы из 10^{13} образов и использование базы всего из 200 образов приводит к ускорению вычислений в 10^{10} раз.

Столь значительный выигрыш от процедур, рекомендуемых национальным стандартом [1], опирается на гипотезу нормального распределения значений расстояний Хэмминга (1). Естественно, что эта гипотеза должна быть проверена. Подобная проверка была осуществлена в 2010 году в рамках НИР «Биометрия-11» (Заказчик ФСТЭК России, Исполнитель ОАО «Пензенский научно-исследовательский электротехнический институт»). Однако факт высокой вероятности подтверждения гипотезы о нормальности распределения расстояний Хэмминга нуждается в подтверждении иными независимыми исследователями. Для того, чтобы дать возможность самостоятельно провести подобные исследования представителям академической и криптографической общественности на сайте ОАО «ПНИЭИ» <http://пниэи.рф/activity/science/noc.htm> выложен код среды моделирования «БиоНейроАвтограф» и лабораторная работа № 6 «Оценка достоверности гипотезы нормальности закона распределения расстояний Хэмминга между кодами «Свой» и «Чужой». Исследования могут проводиться на коротких рукописных паролях, воспроизведенных манипулятором «мышь» или на длинных рукописных паролях, воспроизводимых любым графическим планшетом. Короткие рукописные пароли, воспроизведенные манипулятором «мышь», имеют низкую стойкость к атакам подбора, а длинные рукописные пароли, воспроизведенные на графическом планшете, имеют более высокую стойкость к атакам подбора. Данные о вероятности

выполнения гипотезы нормальности, полученные с использованием разных средств ввода рукописных образов, приведены в таблице 1.

Из таблицы 1 видно, что по мере снижения вероятности ошибок второго рода вероятность выполнения гипотезы о нормальном законе распределения увеличивается. То есть корректность процедур рекомендуемых стандартом [1] возрастает при росте качества, принимаемых искусственной нейронной сетью решений.

Основным свойством нейросетевых преобразователей биометрия-код является то, что они должны примеры образа «Свой» преобразовывать в код «Свой». Идеальный преобразователь биометрия код должен код «Свой» ставить в соответствие всему континууму бесконечного числа примеров образа «Свой» и не давать ошибок. Реальный преобразователь всегда ошибается и имеет некоторое значение вероятности появления ошибок первого рода (ошибочного отказа в доступе «Своему»).

Для обычных преобразователей с допустимым значением $P_1=0,1$ проблем с тестированием не возникает, достаточно базы из 20 тестовых примеров. Ситуация меняется, если по техническому заданию необходимо обеспечить $P_1=0,001$. Для подтверждения такой вероятности пользователю «Свой» потребуется воспроизвести своим почерком не менее 2 000 рукописных парольных слов. На это требуется несколько часов рабочего времени. Возникает задача ускоренной достоверной оценки малых значений вероятности на ограниченной тестовой выборке из 20 примеров. В этой ситуации достигается 100-кратное снижение трудозатрат пользователя на тестирование.

Достичь столь существенного сокращения трудозатрат удастся, опираясь на факт нулевой энтропии [2, 3] и предельно высокой корреляции кодов «Свой», а так же практически нулевого числа степеней свободы системы:

$$\begin{cases} E(r_{i,j}) \approx 1 \\ H(n) \approx 0, \\ \omega \approx 0 \end{cases} \quad (4)$$

где $r_{i,j}$ – коэффициенты парной корреляции между i -тым и j -тым разрядами, контролируемых кодов «Свой» длиной – n , $H(n)$ – энтропия кодов «Свой», $E(\cdot)$ – оператор вычисления математического ожидания, ω – остаточное число степеней свободы, исследуемой системы.

Важным, недавно полученным теоретическим фактом [4] является то, что при переходе из пространства обычных кодов в пространство расстояний Хэмминга между кодами «Свой» биномиальный закон распределения значений сильно зависимых данных стремится

Таблица 1

Рукописный образ	Рукописные образы, введенные манипулятором «МЫШЬ» «Genius» модель MC-06SP		Рукописные образы, введенные через графический планшет «Genius» модель G-Pen F350	
	«аа»	«пар»	«Пенза»	«Воронеж»
Вероятность ошибок второго рода	$P_2=10^{-2.32}$	$P_2=10^{-3.09}$	$P_2=10^{-6.24}$	$P_2=10^{-7.61}$
Вероятность выполнения гипотезы о нормальности	0.9973	0.99986	0.9999964	0.99999978

к χ^2 распределению с очень малым числом остаточных степеней свободы ω :

$$\omega = E(h) \approx \frac{1}{k} \sum_{i=1}^k h_i \quad (5)$$

где h_i – расстояние Хэмминга между кодом «Свой», использованным при обучении нейронной сети и i -тым примером кода из k примеров тестовой выборки «Свой».

Очевидно, что выражение (5) применимо только в том случае, когда в серии из k опытов обнаружена хотя бы одна ошибка с ненулевым расстоянием Хэмминга. В случае, если в серии из k опытов все расстояния Хэмминга нулевые (нет ошибок), оценку числа степеней свободы ведут исходя из предположения, что в следующем $(k+1)$ опыте будет обнаружена ошибка с минимальным расстоянием Хэмминга:

$$\omega = E(h) \approx \frac{1}{k+1}. \quad (6)$$

Исходя из гипотезы χ^2 распределению с очень малым числом степеней свободы вероятность ошибок первого рода может быть вычислена по следующей формуле:

$$P_1 \approx \int_1^{\infty} \frac{1}{2^{\frac{\omega}{2}} \cdot \Gamma\left(\frac{\omega}{2}\right)} \cdot x^{\frac{\omega}{2}-1} \cdot e^{-\frac{x}{2}} \cdot dx, \quad (7)$$

где $\Gamma(\cdot)$ – гамма функция.

Примеры оценки вероятности ошибок первого рода по формуле (7) иллюстрируют распределения, приведенные на рисунке 2.

Оценку среднего значения модулей коэффициентов корреляции вблизи предельной точки $E(h)$ менее 26 для кодов длиной 256 бит следует выполнять по следующей приближенной формуле:

$$E_{256}(|r_{i,j}|) = 1 - 3.77 \cdot \left\{ \frac{E(h)}{256} \right\}^2 \quad (8)$$

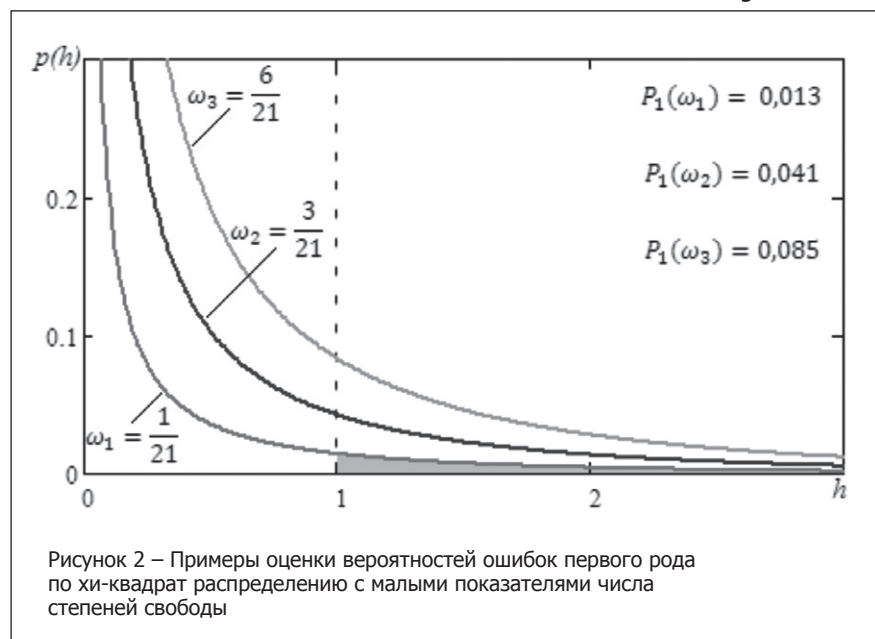


Рисунок 2 – Примеры оценки вероятностей ошибок первого рода по хи-квадрат распределению с малыми показателями числа степеней свободы

Напомним, что распределение введено и исследовано Питсом 100 лет назад для независимых событий. Однако никто не мешает обобщить это распределение и на зависимые (коррелированные) события [5]. То, что в этом случае число степеней свободы распределения становится дробным, является следствием зависимости событий их коррелированности. Имеющееся аналитическое описание распределения (5) не накладывает каких либо ограничений на значение показателя числа степеней свободы. В биометрии гипотеза независимости данных не работает, в связи с этим, приходится применять распределения зависимых данных [5].

То, что гипотеза распределения сильно зависимых данных обеспечивает 100-кратное сокращение трудозатрат на тестирование, является важным преимуществом. В связи с этим, необходимо поставить численный эксперимент, оценивающий достоверность этой гипотезы при разных условиях биометрической аутентификации. Предварительные расчеты показывают необходимость формирования под этот численный эксперимент тестовых баз, содержащих порядка 2000 биометрических примеров каждого из образов «Свой». Ожидается, что будет достаточно 1000 разных биометрических образов для того, чтобы подтвердить гипотезу с достоверностью 0,9991. Работу предполагается осуществить силами студентов и аспирантов ФГБОУ ВПО «Пензенский государственный университет» в 2013–2014 годах в рамках задач, выполняемых научной ротой при институте Военного обучения.

Литература:

1. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
2. Язов, Ю.К. и др. Нейросетевая защита персональных биометрических данных / Ю.К. Язов (редактор и автор), соавторы: В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров. – М.: Радиотехника, 2012. – 157 с.
3. Akhmetov, B. Evaluation of Multidimensional Entropy on Short Strings of Biometric Codes with Dependent Bits / B. Akhmetov, A. Ivanov, V. Funtikov, I. Urnev // «Progress in Electromagnetics Research Symposium» PIERS Proceedings, August 19-23, Moscow, RUSSIA 2012. – P. 66–69.
4. Фунтикова, Ю.В. «Оценка вероятности ошибочного отказа в доступе «Своему» на малом числе тестовых примеров» / Ю.В. Фунтикова, О.С. Захаров // Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. – Т. 8. – Пенза: 2012. – С. 63–64. – (<http://пнизи.рф/activity/science/BIT/T8-p63.pdf>).
5. Захаров, О.С. Учет корреляционных связей биометрических данных через дробный показатель степеней свободы закона распределения значений хи-квадрат. Инфокоммуникационные технологии / О.С. Захаров, А.И. Иванов. – Т. 6, № 1. – 2008. – С. 12–15.

РАЗБИЕНИЕ СЕКРЕТА И МОДЕЛИ МНОГОКАНАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В.А. Мищенко, Ю.В. Виланский, В.В. Захаров,
Институт современных знаний имени А.М. Широкова

Современные и перспективные мощности вычислительных систем ставят под вопрос стойкость многих криптографических алгоритмов шифрования. Сегодня продолжается поиск новых путей построения криптографических систем, основанных как на старых проверенных практикой концепциях, так и на новых подходах. Один из таких подходов основан на идее разбиения зашифрованного шифртекста доверительным алгоритмом зашифрования на несколько информационных каналов и передачи этой информации через несколько физических каналов.

Пусть имеется некоторый секрет S_0 в виде последовательности нулей и единиц длиной L . Может быть поставлены две задачи: хранить этот секрет от посторонних или без личного контакта конфиденциально передать секрет другому лицу открытыми каналами. Первая задача решается с помощью процедуры разделения секрета, вторая задача решается с помощью процедуры шифрования. Особый интерес представляет многоканальное шифрование на основе разбиения секрета [1] с манипуляцией информацией по различным физическим каналам.

1 Разбиение секрета с помощью криптографического алгоритма MV2

В [1, 2] рассматривается криптографический алгоритм MV2, который позволяет получить управляемое разбиение шифртекста на несколько шифртекстов меньшей длины. Механизм разбиения является универсальным и не зависит от типа текста, поскольку оперирует с байтами информации. Ниже приведена цепочка последовательного разбиения для решения задачи скрытия некоторых шифртекстов, где Y_0 – зашифрованный исходный текст любым подходящим для пользователя шифром:

$$Y_1 = \begin{cases} Y_{DT}^1 = E_1(Y_0, K_1) \\ Y_D^1 = E_2(Y_0, K_1) \end{cases},$$

причем $Y_{DT}^1 + Y_D^1 = Y_1$.

Далее последовательно справедливо:

$$Y_2 = \begin{cases} Y_{DT}^2 = E_1(Y_{DT}^1, K_2) \\ Y_D^2 = E_2(Y_{DT}^1, K_2) \end{cases}, Y_{DT}^2 + Y_D^2 = Y_2; \dots$$

$$\dots Y_m = \begin{cases} Y_{DT}^m = E_1(Y_{DT}^{m-1}, K_m) \\ Y_D^m = E_2(Y_{DT}^{m-1}, K_m) \end{cases}, Y_{DT}^m + Y_D^m = Y_m,$$

где m – число шагов алгоритма. Тексты Y_{DT}^i называют остатками C_i , которые являются ущербными текстами, а тексты Y_D^i – ущербными.

В соответствии с алгоритмом MV2 их средние длины связаны соотношениями:

$$L(Y_{DT}^i) = 0,76^i L(Y_{DT}^0);$$

$$L(Y_D^i) = 0,24 \square 0,76^{i-1} L(Y_{DT}^0); i = \overline{1, m},$$

где $Y_{DT}^0 = Y_0$.

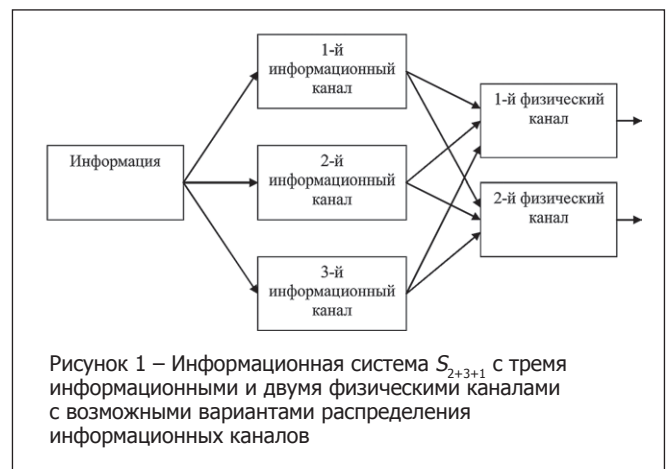
Таким образом, в результате действия алгоритма MV2 имеем $m+2$ шифртекста – один ущербный текст Y_{DT}^m , который называют ядром *Core*, и m ущербов, которых называют флагами F_i .

Процесс расшифрования происходит по схеме:

$$C_{i-1} = E_{12}^{-1}(C_i, F_i, K_i); i = \overline{m, 1}.$$

Отсюда следует, что передавать необходимо только ядро C_m и флаги F_i . Часть флагов ввиду, их соизмеримости с длиной ключа, можно передавать по недоступному ключевому каналу.

В качестве примера на рисунке 1 показана информационная система с тремя информационными и двумя физическими каналами с возможными вариантами распределения информационных каналов по физическим.



2 Модель многоканальной информационной системы

Любая информация существует во времени, передается и хранится в некотором информационном и физическом пространстве. Модель этого информационно-физического и временного пространства характеризуется $n+m+1$ измерениями, где время t выступает одним из измерений:

$$S_{n+m+1}(t) = (a \uparrow s_i(t, t_0, t_{00}); /i_k / \uparrow s_i(t, t_1, t_2); /p_j / s_i(t, t_3, t_4); method(/i_k / \rightarrow /p_j /)), \quad (1)$$

где a – исходный информационный объект; $/i_k/$ – множество информационных каналов распределения информации мощности n ; $/p/$ – множество физических каналов передачи информации мощности m .

$method(/i_k/ \rightarrow /p/)$ – способ распределения информационных каналов по физическим каналам.

Для модели (II.11.1) справедлив общий протокол функционирования:

Начало

A: $a \rightarrow si_k(t, t_0, t_0); f(a) \rightarrow /i_k a_k/ si_k(t, t_1, t_2); method(/i_k/ \rightarrow /p/) \rightarrow (/i_k a_k/ \rightarrow /p a_k/ si_k(t, t_3, t_4)) \rightarrow B$

B: $method^{-1}(/i_k/ \rightarrow /p/) \rightarrow (/p a_k/ \rightarrow /i_k a_k/ si_k(t, t_5, t_6)) \rightarrow f(a); a = f^{-1}(/i_k a_k/ si_k(t, t_7, t_8))$

Конец

Здесь

$f(a) \rightarrow /i_k a_k/ si_k(t, t_1, t_2)$ – процесс шифрования и разделения информации на множество информационных каналов;
 $/i_k a_k/ \rightarrow /p a_k/ si_k(t, t_3, t_4)$ – процесс распределения множества информационных каналов по множеству физических каналов;

$si_k(t, t_1, t_2)$ – селектирующая функция интервала [3].

Причем в зависимости от методов преобразования информации справедливо неравенство

$$L(a) \leq \sum_k L(i_k). \quad (2)$$

где L – длина информации в некоторых единицах.

Соотношение (2) подразумевает разбиение информации на информационные каналы и распределение информационных каналов по физическим каналам передачи.

Эти два действия будут называться манипулированием информацией. В общем случае, во времени любой информационный канал может подвергаться вторичному преобразованию (1), используя новые физические каналы.

Таким образом, представление (1) может генерировать большое число вариантов многоканальных информационных систем с временной координатой t , варьируя количеством информационных и физических каналов.

3 Модели систем $S_{m+n+1} S_{m+n+1}$ (m – количество физических каналов; n – количество информационных каналов)

Рассмотрены некоторые варианты построения систем: $S_{2+3+1}; S_{2+4+1}; S_{4+4+1}$ и ряд других.

Построение таких систем нашло применение в массовых технологиях современного рынка: LABEL, LABEL DOC (защита интеллектуальной и материальной собственности), SEMAIL (двухканальная электронная почта).

Литература:

1. Мищенко, В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский. – Минск: Энциклопедикс, 2007. – 291 с.
2. Мищенко, В.А. Криптографический алгоритм MV2 / В.А. Мищенко, Ю.В. Виланский, В.В. Лепин. – Минск: Энциклопедикс, 2007. – 177 с.
3. Мищенко, В.А. Теория селектирующих функций в практических приложениях / В.А. Мищенко. – Минск: Медисонт, 2012. – 247 с.

О СОВЕРШЕННЫХ МОДУЛЯРНЫХ СХЕМАХ РАЗДЕЛЕНИЯ СЕКРЕТА

Т.В. Галибус, Г.В. Матвеев,
 БГУ, г. Минск

Разделение секрета является широко используемым криптографическим примитивом. Схема модулярного разделения секрета, предложенная Миньоттом, оказалась несовершенной, т.е. частичные секреты (ключи) участников дают возможность получить некоторую информацию о секрете, даже если группа участников не является полномочной, т.е. не имеет доступа к конфиденциальной информации. Для устранения указанного недостатка Асмут и Блюм предложили усовершенствование исходного модулярного подхода, которое затем было исследовано Пренелем и другими авторами, с целью качественного улучшения модулярных пороговых схем, построенных в кольце целых чисел. Напомним, что семейство подмножеств произвольного множества участников P называется структурой доступа, если оно обладает свойством монотонности, т.е.

$$A \in \Gamma, A \subset B \subset P \Rightarrow B \in \Gamma.$$

Реализацией структуры доступа или схемой разделения секрета называется такой алгоритм, который позволяет вычислить некоторый секрет лишь группам участников, образующих подмножества из множества P .

Принципиально иной подход был предложен нами

в работе [1]. Он заключается в замене кольца целых чисел на кольцо многочленов от одной переменной $F_q[x]$ над конечным полем. Оказалось, что в этом кольце можно реализовать не только совершенно, но даже идеально любую пороговую структуру доступа. Сразу же возникла задача об обобщении этого результата на случай кольца многочленов от многих переменных $F_q[x_1, x_2, \dots, x_n]$. В этой связи, в работе [2] было сформулировано условие на модули участников совершенной схемы.

В работе [3] было показано, что для совершенной реализации общих структур доступа нужны специальные идеалы $I_1, I_2, \dots, I_k$ в кольце $F_q[x_1, x_2, \dots, x_n]$. Они были названы равноостаточными, потому что должны удовлетворять условию:

$$RP(I_{i_1} I_{i_2} \dots I_{i_m}) = RP(I_{j_1} I_{j_2} \dots I_{j_m}),$$

где $i_1, i_2, \dots, i_m; j_1, j_2, \dots, j_m$ – произвольные m -выборки из $1, 2, \dots, k$, а RP означает множество приведенных мономов.

К настоящему времени равноостаточные идеалы удалось построить лишь для обратного лексикографического упорядочения.

Литература:

1. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets // SYNASC'08. – California: IEEE Comp. Soc. CPCS, 2009. – P. 197–200.
2. Шенец, Н.Н. Об информационном уровне модулярных схем разделения секрета / Н.Н. Шенец // Докл. Нац. акад. наук Беларуси. Сер. физ.-мат. наук. – 2010. – Т. 54, №6. – С. 9–12.
3. Галибус, Т.В. Идеалы симметрических отношений и разделение секрета / Т.В. Галибус // Вестн. Белорус. гос. ун-та. Сер. 1, Физика. Математика. Информатика. – 2011. – № 2. – С. 141–143.

СИСТЕМА МАРКИРОВКИ И КОНТРОЛЯ ДВИЖЕНИЯ МАТЕРИАЛЬНЫХ ОБЪЕКТОВ НА ОСНОВЕ АЛГОРИТМОВ КРИПТОГРАФИЧЕСКОГО РАЗБИЕНИЯ СЕКРЕТА

В.В. Захаров,**Институт современных знаний имени А.М. Широкова**

Массовый поток контрафактных товаров на мировом рынке является вызовом для международных организаций, союзов и отдельных государств. Объем контрафакта в отдельных отраслях сравним с объемом легального производства, а зачастую и превышает его, что ведет к существенным потерям для бюджета государства.

Всемирная таможенная организация (ВТО) и международная торговая палата (МТП) по данным 2012 года, считают, что подделки ежегодно вынимают около 600 млрд евро из мировой экономики, что эквивалентно потере оригинальными товарами по всему миру примерно 5–7 % рынка. Ожидается, что к 2015 году эта сумма достигнет 1,7 трлн долл. США.

Однако, если подделка одежды, бытовой техники и других товаров народного потребления может привести только к потере денег и (или) времени потребителя, то подделка лекарств несет угрозу здоровью и жизни покупателя.

До сих пор меры по борьбе с поддельными лекарствами включали: меры, принимаемые регулятивными органами в области лекарств, и инициативы по сотрудничеству между различными органами правопорядка; нанесение простых, легко интерпретируемых и недорогих маркеров подлинности; координацию на международном уровне надзора за поддельными и некачественными лекарствами и просвещение пациентов и работников здравоохранения.

В настоящее время некоторые страны уполномочивают компании подтверждать подлинность их продукции путем создания «родословной», которая заверяет происхождение лекарства и дальнейшее обращение с ним.

Управление США по контролю качества пищевых продуктов и лекарственных препаратов рекомендовало фармацевтическим компаниям перейти к использованию технологии радиочастотной идентификации (РЧИ) для лучшего отслеживания лекарств. Некоторые фармацевтические компании экспериментально применяют РЧИ и оптически изменяющиеся устройства или, по крайней мере, используют штрих-коды или другие технологии, такие как веб-порталы, которые помогают отслеживать и идентифицировать лекарства.

Используют голограммы, чернила, изменяющие цвет, и водяные знаки, которые способствуют подтверждению подлинности упаковок и таблеток. Экспериментируют с использованием чернил и красителей, предлагают для некоторых продуктов специальную упаковочную пленку в целях предотвращения подделок.

Однако такой подход к применению современных средств защиты, на первый взгляд, позволяющих отличить подделку от оригинала, на самом деле лишь увеличивает время изготовления подделки и стоимость единовременных затрат преступника на приобретение специального оборудования и материалов, и, следовательно, уменьшает вероятность подделки, но незначительно.

Возможным решением этой проблемы является создание системы, в которой проверка маркировки (ярлыка) производится удаленно, непосредственно у производителя (или у его доверенного представителя), а результат поступает пользователю по каналам связи.

Уникальность ярлыка, монтируемого на товар, является необходимым требованием обеспечения возможности дистанционной проверки. Действительно, современный опыт показывает, что для современного промышленного «пирата», осуществляющего массовое производство поддельного товара, не существует препятствий для воспроизведения любого массового, не являющегося уникальным защитного элемента. Одной из возможных компроматаций систем с обратной связью является продажа партии подделок до начала продажи подлинного товара. Для такой операции злоумышленник должен иметь возможность предвидеть проверочные значения, наносимые на ярлык. Соответственно, для реализации надежной системы проверки с обратной связью с производителем необходимо для каждой единицы товара обеспечить уникальные, непредсказуемые проверочные данные. Если товар массовый и не дорогой, то необходимо также обеспечить дешевизну ярлыка, содержащего такие проверочные данные. Кроме того, необходимо иметь недорогие, достаточно надежные устройства для считывания этих данных для ввода в систему. Одним из самых дешевых и распространенных носителей иденти-

фикационной информации является штрих-код. Соответствующая аппаратура для его считывания имеется практически везде. Однако информационная емкость штрих-кода не очень велика. А унификация системы проверки (что необходимо для глобального использования) требует добавления информации, идентифицирующей конкретного производителя среди сотен других и единицы товара среди миллионных партий. Таким образом, даже только на идентификатор товара требуется значительная (для штрих-кода) информационная емкость. А ведь еще необходимо добавить некоторые непредсказуемые данные для аутентификации.

Именно такой подход реализован в рассматриваемой далее системе LABEL, которая в первую очередь ориентирована на защиту потребителя от фальшивых лекарств. При необходимости система может быть оперативно перестроена для защиты любых товаров.

Система LABEL предназначена для обеспечения защиты товаров от подделки путем создания защищенных от фальсификации товарных ярлыков и их надежной, адресной проверки на всех этапах движения товара.

Метод решения проблемы заключается в следующем:

- в создании для каждой единицы товара и партий любого уровня уникального, секретного идентификатора и разбиении его на части с помощью двухканального криптографического алгоритма MV2. Причем одна часть секрета хранится у производителя, а другая наносится на ярлык – относительно недорогой носитель, крепящийся к товару. Восстановление идентификатора без знания обеих частей секрета невозможно;

- в создании сети проверочных терминалов, обеспечивающих возможность считывания, проверки подлинности ярлыка и предоставлении полной информации о товаре и его производителе на всех этапах движения товара. Причем в каждой проверке принимает участие производитель.

Система LABEL выполняет следующие функции:

- идентификация и аутентификация участников бизнес-процессов;
- создание абсолютно защищенных от подделок товарных ярлыков, уникальных для каждой единицы и/или партии товара, обеспечение их учета и активизации;
- надежная адресная проверка товарных ярлыков по месту их происхождения;

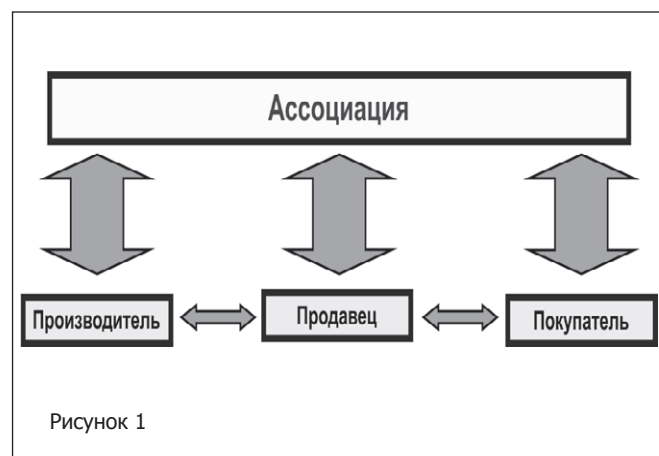


Рисунок 1

- контроль, проверка и учет перемещения и продаж товаров от единичных образцов до крупных партий;
- блокирование продаж просроченных товаров и товаров с поддельными ярлыками.

Участниками системы LABEL являются: контролирующий орган (далее, ассоциация), производитель товара, продавец и покупатель.

Ассоциация владеет регистрационным центром (далее, Регцентр) и сетью проверочных терминалов.

Регистрационный центр управляет системой LABEL, для чего выполняет следующие основные функции: регистрация участников системы – производителей и проверочных терминалов; предоставление участникам системы по их запросу разрешенной информации о других участниках; управление криптографическими ключами системы.

Производитель товара обеспечивает выпуск защищенных товарных ярлыков и их проверку на подлинность, для чего выполняет следующие основные функции: производство ярлыков; учет ярлыков; крепление ярлыков на товаре; проверка подлинности ярлыков.

Продавец выполняет следующие функции: активизация партии товара – сообщение производителю о поступлении в продажу партии товаров; проверка подлинности товарного ярлыка при продаже товара; предоставление покупателю информации о результате проверки подлинности товарного ярлыка.

Покупатель имеет возможность проверить подлинность товарного ярлыка при покупке товара непосредственно у продавца и на независимом проверочном терминале.

Положительные стороны системы:

- позволяет защитить оригинальную продукцию, торговую марку предприятия от подделки;
- повышает собираемость налогов и сборов;
- обеспечивает привлечение покупателей, обеспеченных качеством и безопасностью приобретаемых товаров;
- поднимает имидж торгового предприятия, что позволяет увеличить объем торговли, в целом, и продаж оригинальной продукции, в частности;
- может рассматриваться как основа процесса логистики торговой организации: заказ, движение и оформление товара, статистика продаж;
- основа маркетинговых исследований и планирования;
- построение системы гарантий доверия покупателя к торговому предприятию, предлагающему товары, в подлинности которых он уверен;
- небольшие затраты на техническое оснащение предприятия.

Литература:

1. Мищенко, В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский. – Минск: Энциклопедикс, 2007. – 291 с.
2. Патент ЕА 003679. Способ шифрования и дешифрования информации и устройство для его осуществления.
3. Патент ЕА 004904. Способ шифрования, передачи, хранения конфиденциальных сообщений и система для осуществления способа.

УВЕЛИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ КРИПТОЗАЩИЩЕННЫХ ТУННЕЛЕЙ

С.А. Пузырев,

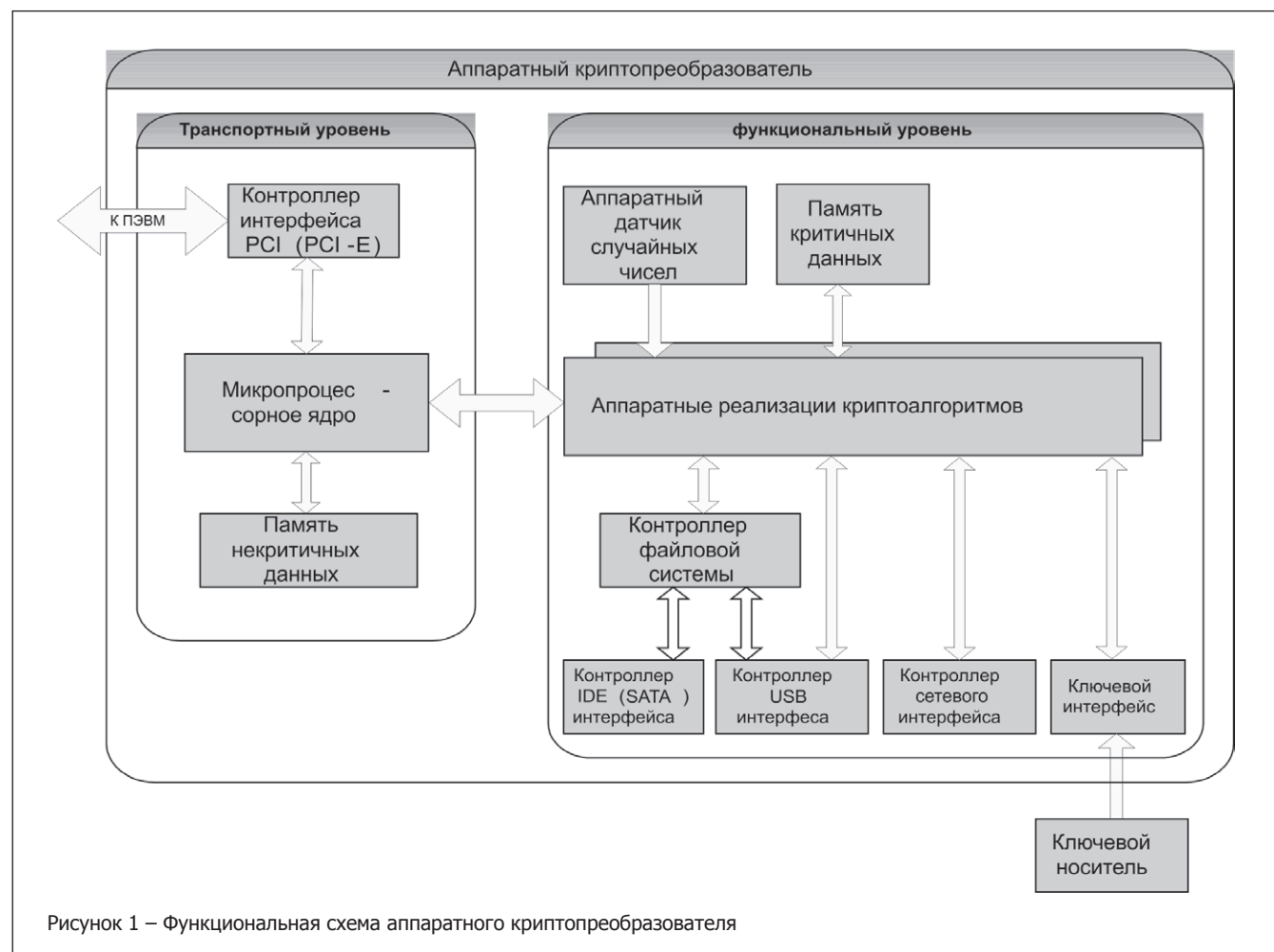
Военная академия Республики Беларусь

Создание современных компьютерных систем и появление глобальных компьютерных сетей радикально изменило характер и диапазон проблем защиты информации. Одним из критичных видов информации является персональная информация, накапливаемая в базах данных автоматизированных систем обработки либо у индивидуальных пользователей. Так как такая информация может быть очень ценной или особо важной, то возможны разнообразные злонамеренные действия по отношению к компьютерным системам, обрабатывающим или передающим персональную информацию. Таким образом, владелец персонального ПК становится самым незащищенным звеном информационного взаимодействия и следовательно нуждается в средствах гарантированной защиты информации.

Проведя анализ публикаций по возможным угрозам безопасности информации можно сделать вывод о том, что одним из самых уязвимых звеньев в информационно-вычислительных системах являются коммуникации. Технологии и протоколы, положенные в основу информационного

обмена обладают массой недостатков, которые позволяют успешно реализовать угрозы безопасности информационно-вычислительных систем. Для решения этой проблемы разработано довольно большое количество программных и программно-аппаратных решений, которые позволяют снизить количество успешных реализаций угроз безопасности информационного обмена, однако, исключить их практически полностью позволяют только устройства криптографического преобразования информации. В этом случае стойкость информационного обмена сводится к стойкости используемых криптографических протоколов. Однако такой подход успешно реализуем только в случае использования Интернет или других коммуникаций для передачи информации ограниченного распространения между несколькими абонентами, т.е. организации криптотуннелей. Основными недостатками существующих разработок аппаратуры криптографического преобразования является:

- низкая скорость криптопреобразования;
- внесение временных задержек в процесс информационного обмена;



- использование универсальных микропроцессоров для криптографических вычислений;
- использование криптографических алгоритмов иностранной разработки;
- высокая стоимость;
- слабая защищенность от программных средств криптопреобразования от вмешательства потенциального нарушителя;
- использование программными средствами криптопреобразования большого количества вычислительных ресурсов процессоров вычислительных систем.

Автором статьи реализовано аппаратное устройство высокоскоростного криптографического преобразования двоичной информации, которое не использует микропроцессорные устройства, а представляет собой комбинационный прибор, сформированный из типовых логических элементов. Устройство вносит минимальные задержки в процесс криптографического преобразования, обусловленные только переходными процессами. Такой подход к построению криптопреобразователя позволил значительно увеличить скорость, снизить задержки и исключить стороннее вмешательство в процесс криптографической обработки данных. Разработано два варианта устройства, реализующие алгоритмы криптопреобразования ГОСТ 28147-89 и BelT. Данное устройство может быть выполнено в виде отдельной микросхемы, либо включено в состав контроллера интерфейса.

Функциональная схема разработанного устройства представлена на рисунке 1.

Аппаратный криптопреобразователь является основой системы защиты информации от несанкционированного доступа. При взаимодействии в сети соединения возможно установить только с устройствами, имеющими в своем составе аппаратные криптопреобразователи с установленной идентичной ключевой информацией. Остальной трафик игнорируется, в том числе трафик потенциального нарушителя. Осуществляется полное либо частичное преобразование IP-трафика по выбранному алгоритму (ГОСТ-28147-89, BelT), что делает трафик криптотуннеля недоступным для устройств, которые не включены в криптотуннель. Способ преобразования IP-пакетов зависит от того, какие линии связи используются для организации обмена – коммутируемые или нет. Это

обусловлено особенностями функционирования коммутированного оборудования.

Ключевыми элементами должен быть снабжен каждый абонент криптотуннеля. Ключевой носитель может представлять собой микросхему EEPROM, подключаемую через специализированный интерфейс.

При построении ЛВС обычно используются типы защищенных каналов ЛВС – ЛВС. Это обусловлено высокой стоимостью программно-аппаратных средств криптографического преобразования сетевого трафика. Для построения защищенных криптотуннелей ЛВС – рабочая станция, ЛВС – удаленная рабочая станция, рабочая станция – рабочая станция используются в подавляющем большинстве программные средства. Разработанное аппаратное устройство криптопреобразования позволит создавать высокоскоростные криптотуннели любого типа с практически одинаковыми затратами. Возможно создание USB сетевых адаптеров Ethernet с встроенными функциями аппаратного криптопреобразования.

Разработанный аппаратный криптопреобразователь возможно применить для создания персональных и коллективных криптографических средств для высокоскоростного преобразования конфиденциальной информации на практически любых интерфейсах современных информационно-вычислительных систем.

Литература:

1. Зима, В.М. Безопасность глобальных сетевых технологий / В.М. Зима, А.А. Молдован, Н.А. Молдован – 2-е изд. – СПб.: БХВ-Петербург, 2003.
2. Бочков, М.В. Адаптивная защита информации от несанкционированного доступа в вычислительных сетях / М.В. Бочков, С.Н. Бушуев, В.А. Логинов, И.Б. Саенко. – СПб.: ВАС, 2005.
3. Коняевский, В.А. Управление защитой информации на базе СЗИ НСД «Аккорд» – М.: Радио и связь, 1999.
4. Агиевич, С.В. Алгоритм блочного шифрования BelT / С.В. Агиевич, В.А. Галинский, Ю.С. Харин // Управление защитой информации, 2002. – Т. 6, № 4. – С. 407–411.
5. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Издательство стандартов, 1989.

КОНТРОЛЬ ЦЕЛОСТНОСТИ КОДА FIRMWARE В ГАРВАРДСКОЙ АРХИТЕКТУРЕ

М.М. Грунтович,
ОКБ САПР, г. Пенза

Недавно мне подбросили интересную задачу: придумать, как можно обеспечить контроль целостности внутреннего ПО (firmware) устройства с гарвардской архитектурой процессора, когда код не может быть доступен для чтения, как данные. Задача сама по себе, быть может, не большой важности и сложности, но мне показалось, что на ее примере можно продемонстрировать то, как важно не заикливаться в рамках исходной постановки задачи, а видеть ее по возможности шире.

За счет этого иногда удается решать неразрешимые, на первый взгляд, задачи, или получать изящные, эффективные решения типовых задач.

Классическое решение в фон-неймановской и модифицированной гарвардской архитектуре

Напомню, что классическая гарвардская архитектура характеризуется тем, что физически разделяются внешние хранилища команд и данных, а также шины адреса,

шина команд и шина данных. Помимо этого, различают также модифицированную гарвардскую архитектуру, в которой используется одна внешняя шина адреса и данных для загрузки как команд, так и данных, различаются только внутренние шины процессора.

В фон-неймановской архитектуре (совместное хранение команд и данных в памяти компьютера) задача контроля целостности кода firmware обычно решается следующим образом. Пишется программный модуль, который читает код как данные, вычисляет его контрольную сумму и сравнивает с эталоном. Собственно, так можно поступить и в случае модифицированной гарвардской архитектуры. А именно, когда внешняя шина адреса одна для данных и для кода, можно пытаться читать код firmware как данные. Это срабатывает, если в устройстве не предусмотрено блокирование таких запросов, иначе, мы фактически находимся в условиях задачи для классической гарвардской архитектуры.

Что же делать в случае, когда команды можно только исполнять, т.е. они не могут быть прочитаны по шине данных? Похоже на то, что решить поставленную задачу в рамках обычной вычислительной системы, процессор + долговременная память, не удастся. Но можно попробовать расширить либо постановку задачи, либо систему.

Расширение постановки задачи

Сначала поставим вопрос, зачем вообще нужен контроль целостности firmware? Видится, по крайней мере, два варианта ответа:

- контроль целостности необходим самому firmware как этап проверки работоспособности изделия;
- контроль целостности необходим внешнему проверяющему (пользователю, ревизору) для получения доверия к изделию.

В обоих случаях проверяющего интересует не собственно неизменность кода, а то, что он правильно выполняет заявленный функционал и не делает ничего больше. Значит, есть смысл контролировать именно это? Как проверить то, что устройство правильно работает более-менее понятно: обычно его заставляют выполнять хитроумно придуманные тестовые задания. При этом доступ к коду firmware, как к данным, не требуется.

А вот как проверить то, что устройство не умеет делать еще что-то помимо того, что умеет делать эталон? Честно говоря, кроме традиционного предварительного анализа эталона и контроля целостности кода firmware, к сожалению, ничего в голову не приходит.

Итак, расширенная постановка задачи, похоже, не привела к успеху. Пробуем расширять объект исследования, т.е. вычислительную систему.

Расширение системы

в классической гарвардской архитектуре

Систему, построенную по классической гарвардской архитектуре, можно попробовать расширять одним из следующих способов.

1. Наделим вычислитель еще одной функцией, выполняющей подсчет контрольной суммы области памяти кода. Сделать это можно либо путем модификации процессора за счет расширения системы команд, либо путем модификации расширенной машины, а именно, операционной системы, расширив ее функцией подсчета контрольных сумм областей памяти кода. Такое расширение системы не приведет к нарушению ее безопасности, однако, позволит обойти запреты архитектуры. Глубина модификации зависит от уровня требований безопасности к системе. Использование системного программного обеспечения допустимо тогда, когда оно априори считается доверенным. При этом следует иметь в виду, что проверяющий может потребовать подтверждение неизменности уже этого кода.

2. Второй способ предполагает расширить систему, добавив в нее специализированный процессор, который имеет доступ к памяти команд на чтение, но уже как к данным. Чтобы чрезмерно не удорожать изделие, можно выбрать достаточно маломощный процессор. Однако его наличие позволит «добраться» до кода firmware, не внося уязвимости в вычислительную систему. В этом случае, правда, надо иметь в виду, что опять придется проверять целостность кода спецпроцессора.

К сожалению, оба предложенных способа не всегда реализуемы, поскольку требуют модификации вычислительной системы, а программист, чаще всего, не имеет возможности влиять на ее структуру.

А задача, сформулированная в начале статьи, на практике решилась следующим образом. В вычислительной системе пластиковой карточки, где firmware не имеет возможности читать код, как данные, при более глубоком изучении функций операционной системы все же была найдена возможность подсчета контрольной суммы кода. Не могу точно сказать, каким путем она реализована, то ли аппаратно, то ли через обращение к системному программному обеспечению, но, по существу, это первый из предложенных выше способов решения задачи за счет расширения системы.

ПАК «АККОРД-Б». НОВОЕ СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

М.М. Грунтович, А.Ю. Родионов, В.А. Тюнин,
ОКБ САПР, г. Пенза

В линейке средств криптографической защиты информации, не содержащей сведений, составляющих государ-

ственную тайну, выпускаемых ОКБ САПР – пополнение. Специалисты компании завершили разработку нового

изделия – программно-аппаратного комплекса криптографической защиты информации «Аккорд-Б».

В отличие от других изделий ОКБ САПР по данной тематике, персонального средства криптографической защиты «ШИПКА», выполненного в форм-факторе USB-токена, и ПАК «Аккорд-У», являющегося криптографическим расширением электронного замка, ПАК «Аккорд-Б» является высокоскоростным изделием, обеспечивающим выполнение больших потоков операций криптографической защиты:

- шифрование/расшифрование и имитозащита данных по ГОСТ 28147;
- формирование и проверка цифровой подписи по ГОСТ Р 34.10;
- вычисление значения хеш-функции по ГОСТ Р 34.11;
- вычисление общего ключа по схеме Диффи-Хеллмана на основе параметров ГОСТ Р 34.10.

Помимо этого, устройство обеспечивает безопасное хранение ключей пользователя, как долговременных, так и временных, генерация качественной случайной последовательности с помощью встроенного аппаратного ДСЧ.

Аппаратный модуль «Аккорд-Б» выполнен в виде карты расширения ПЭВМ с интерфейсом PCI Express. Базовые криптографические алгоритмы в нем реализованы с помощью высокопроизводительной ПЛИС с архитектурой FPGA в виде самостоятельных функциональных блоков, что позволяет выполнять разнотипные операции криптографической защиты параллельно.

Программное обеспечение ПАК «Аккорд-Б» функционирует под управлением 32-битных и 64-битных операционных систем семейства Windows не ниже Windows 7 и Windows Server 2008. Вызов функций криптографической защиты со стороны прикладного программного обеспечения производится через обращение к специализированной библиотеке по интерфейсу стандарта PKCS#11. К слову, эта библиотека единая для всех изделий линейки криптографических продуктов ОКБ САПР.

В ходе разработки изделия специалистами ОКБ САПР применен ряд оригинальных аппаратных и программных решений, позволивших реализовать многопоточное высокоскоростное выполнение функций криптографической защиты. Работа ПАК «Аккорд-Б» по состоянию на данный момент характеризуется следующими показателями:

- хранение до 4000 долговременных ключей;
- генерация временного ключа ДХ: 0,00475 с;
- экспорт временного ключа: 0,003 с;
- импорт временного ключа: 0,0005 с;
- а при выполнении операций над 1 КБ пакетами данных с временными ключами:
 - шифрование/расшифрование по ГОСТ 28147: 0,00037 с (2700 пакетов/с);
 - хеширование по ГОСТ 34.11-94: 0,00039 с (2500 пакетов/с);
 - формирование подписи по ГОСТ 34.10-2001: 0,0036 с (280 подписей/с);
 - проверка подписи по ГОСТ 34.10-2001: 0,00645 с (155 подписей/с).

Если учесть то, что одновременно устройство способно выполнять несколько операций цифровой подписи, суммарное количество операций формирования ЭЦП увеличивается до 2900/сек, проверки – 1500/сек. В настоящее время ведется дальнейшая работа над совершенствованием

внутренних механизмов изделия в целях повышения, в том числе, и скорости вычислений.

Предполагается выпуск изделия «Аккорд-Б» в двух модификациях: с внешним носителем мастер-ключа и с хранением мастер-ключа в энергонезависимой, недоступной для проникновения памяти аппаратного модуля. Мастер-ключ используется в ПАК «Аккорд-Б» для защиты долговременной ключевой информации пользователя, хранящейся во флеш-памяти.

Секретные долговременные и временные ключи, используемые для выполнения криптографических операций, в открытом виде существуют только в аппаратном защищенном ключевом кэше и в функциональных блоках, непосредственно выполняющих криптографические операции. Функциональные блоки имеют доступ к двум независимым шинам данных: открытой и ключевой. По первой они получают входные данные и передают результаты операций, по второй циркулируют секретные криптографические ключи. Внутренний процессор аппаратного модуля, исполняющий интерфейсные функции между функциональными блоками и шиной PCI Express, не имеет доступа к ключевой шине.

Таким образом, обеспечивается двухуровневая защита от утечки ключевой информации. Во-первых, программное обеспечение внутреннего процессора обеспечивает невозможность передачи ключевых объектов в открытом виде за пределы аппаратного модуля, поскольку выполняет только запросы по спецификации PKCS#11. А во-вторых, само внутреннее программное обеспечение не имеет доступа к секретной ключевой информации в открытом виде, поскольку оно исполняется на внутреннем процессоре.

Изделие ПАК «Аккорд-Б» ориентировано на рынок Удостоверяющих центров, ЦОДов и аналогичных потребителей, где требуется обработка больших объемов информации, защищенной с помощью криптографических преобразований. Не исключено использование полученного опыта при разработке новых изделий подобной направленности, например, с меньшими потоками одновременно выполняемых операций.

В ходе работ над новым изделием неоценимую помощь нам оказали коллеги из подразделения Федерального государственного автономного научного учреждения «ЦИТИС», возглавляемого Хвостовым А.С. Предоставленное ими тестовое программное обеспечение, опыт использования аппаратных СКЗИ, а также доброжелательность и терпение обеспечили коллективу разработчиков необходимую поддержку.

НАНОТЕХ

ООО "Нанотех"
г. Минск, ул. Седых 12А, пом. 2Н

- Монтаж печатных плат**
(автоматический и ручной)
- Печатные платы**
(одно-, двухсторонние, многослойные, на алюминии)
- Трафареты для пасты**
(лазерной резкой из нержавеющей стали)
- Паяльные пасты**
(безотмывочные, канифольные, водосмываемые, и др.)



pcb@pcb.by
www.pcb.by

тел: +375 17 237 29 34
тел: +375 17 237 29 35
тел/факс: +375 17 237 29 36
тел/факс: +375 17 281 35 36

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВЗАИМООТНОШЕНИЕ ФОРМ ЗАЩИТЫ И ВИДОВ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.П. Елисеев,
РГГУ, г. Москва

В процессах комплексной защиты информации, в решении актуальных вопросов безопасности информационного пространства государства в условиях глобализации на первый план выдвигаются вопросы создания и надежного функционирования защищенных объектов на основе новейших информационных технологий. Совершенствование средств и механизмов организационной и технической защиты информации в свою очередь предполагает повышенные требования к разработке математического аппарата, открывающего принципиальные возможности реализации новых направлений и технологий обеспечения информационной безопасности.

Но по ходу разрешения проблем техники и математики неизбежно обнаруживается, что наиболее мощным фактором эффективного овладения информационными пространствами государства и общества является профессионально-личностный потенциал разработчиков и пользователей информационных технологий.

Повышение качества комплексной защиты информации требует все более глубокого, методологического обоснования теории и практики активного, осознанного и творческого управления процессами информатизации.

Если методология информатизации – это, прежде всего, ее понимание, то следует вначале поставить наиболее «простые» вопросы именно об адекватном понимании того, что есть вообще информация и что представляет собой процесс информатизации, включая его безопасность. Самой постановкой этих вопросов перед специалистами в области информационной безопасности подразумевается действительная проблематичность и смысловая весомость «очевидных», простых решений, на самом деле коренным образом предопределяющих стратегию и тактику защиты и овладения информационными пространствами заинтересованных во взаимодействии субъектов.

В целом, функционирование и развитие системы информационной безопасности может быть представлено, как процесс управления ретрансляцией адекватных деятельности человека ценностей или, вообще, управление движением некоторых идеальных сущностей. В психологии человека этот процесс предполагается заведомо безопасным и вполне управляемым. Так, например, рассматриваются когнитивный и сенсорный планы ретрансляции информации, когда происходит перенос смыслов или смысловой перенос – из одной области мыслей и чувств в другую, в результате чего человек непрерывно существует в идеальном пространстве переносных смыслов, в пространстве его психологически

укорененной культуры, обеспечивающей его безопасную жизнедеятельность по отношению к природе.

Аналогично понимается перенос знаний, умений и навыков, когда успех в освоении какого-то одного вида деятельности влечет за собой успех в другой деятельности. В иных терминах успешный перенос информации может быть определен как положительный трансфер, в противоположность отрицательному трансферу или, иначе, ситуации, в которой овладение одним видом деятельности служит препятствием в исполнении другого вида деятельности. При этом успешность переноса, рассматриваемого в качестве трансфера, зависит от того, насколько верно определяется сходство задач в плане способов их решения и в предположении либо отрицательного переноса (интерференции информации), либо положительного переноса (индукции информации).

Отстаивая универсальный характер проблем переноса (т.е. трансфера), Ю.М. Лотман исходит из структурного единства ретранслируемых текстовых и личностных семиотических характеристик. Парадоксальность феномена культуры, в отличие от «плоского эволюционизма», состоит в том, что ее развитие, как целого, пронизано частными структурами трансляции текстов. Информационные потоки становятся тем более лично ценными и тем успешнее взаимно снимаемыми и ретранслируемыми, чем проще их символика, обладающая «гораздо большей смысловой емкостью».

С точки зрения семиотически единой личности, высшие психические функции человека, если и возникают, по замечанию Л.С. Выготского, «дважды», то лишь в силу принятия аксиомы абсолютного противопоставления внутреннего и внешнего, – аксиомы, столь необходимой в обыденном сознании и в классической психологии как объективной науке. Но в процессе познания, с позиций неклассической психологии человека, противоречие внутреннего и внешнего снимается Л.С. Выготским благодаря выдвиганию принципа диалектического (генетического) единства объективно и субъективно существенного и несущественного, как в развитии мышления и речи, так и в самодвижении развивающейся личности.

В процессах становления человека, как общественного индивида, основное значение имеет непосредственное или опосредствованное ретранслирование жизненно необходимой информации. При этом информация понимается не как совокупность сведений и т.п., а в точном смысле слова, как вообще «неоднородность» (и вместе с тем, «мера неоднородности»), или, буквально, как любая трансформация или формоизменение некоторого содержания в единстве материи и движения.

Диалектикой становления личности и деятельности человека предполагается асимметричное, неравномерное и гетерохронное ретранслирование «текстов» культуры, вследствие чего именно личностью воплощается культура, как непрерывно трансформируемый способ или активная, подвижная форма овладения жизнью, вообще, как процесс информатизации жизни человека в качестве общественного индивида.

В этой связи требуется подчеркнуть, что явление информатизации на самом деле не может быть приватизировано современной эпохой в качестве специфической ее характеристики. Вместе с тем, именно в настоящее время становится, наконец, все более ясно, что непрерывное культурно-цивилизационное преобразование всей человеческой истории по существу является энергоинформационным. Военные конфликты всех времен также были в своей основе информационными войнами, с теми только осложнениями, что человеческие жизни замещали собой средства тотальной защиты энергоинформационных структур функционирования государства и общества.

Общей смысловой основой слов «информация», «трансляция» и «трансформация» является понятие «трансфер». Латинское «transfere» («переносу, перемещаю») адекватно тому пониманию, что трансфером предполагается небеспредметный перевод или перевод по сути дела, а также передача того содержания, которое обеспечивает взаимодействие и взаимопонимание посредством осознания существа коммуникации всеми ее участниками при условии адекватной регуляции и защиты движения информационных потоков.

Определением трансфера схватывается едва ли не вся совокупность явлений, представляющих качественно различные отношения активности, определяющие основные виды деятельности человека. Трансфер диалогичен, диалектичен по своему определению и предполагает, очевидно, диалектическое снятие одного содержания другим, в результате чего и то, и другое преобразуется и предстает в новом свете, как ясно осознаваемое, то есть понимаемое. Понимание, следовательно, как и осознание осуществляется посредством трансфера.

Быть в сознании – значит владеть его содержанием, его ценностями и смыслами, в которых оно явлено здесь и сейчас – обладать трансферальной способностью, характеризующей бодрственное, жизнеспособное, «по-стороннее» состояние человека. Осмысленность и трансферальность совместно обеспечивают активный, избирательный, самостоятельный и творческий характер сознания человека.

Быть в сознании в профессиональном отношении, – значит понимать существо дела, обладать проблемным зрением и средствами разрешения проблем; или, если это касается научно-практической деятельности, методологически адекватно осуществлять теоретический и эмпирический поиск истины, представляя, в особенности, адекватное определение ключевых понятий. Так, например, в данном контексте очень важно определить то, что понятие «функция», по существу, есть не что иное, как «деятельность», включающая в себя операции, действия и технологии. Идеальной, ведущей стороной (но не «частью») деятельности является активность, в качестве формы отношений управления или понимания этой деятельности.

Как обобщает Э.В. Ильенков, «идеальность» вообще (то есть идеальность вообще любого понимания как осмысленного овладения информацией) есть «форма вещи, но вне этой вещи, а именно, в деятельности человека, как форма этой деятельности». Конструктивный потенциал понимания единства форм активного отношения человека и видов его деятельности выражается в признании интегративного характера преемственной и непрерывной информатизации, или трансформации человеческой культуры. Из такого понимания следует, в частности, то, что различные виды функционирования деятельности или информации должны быть определяемы соответствующими формами, как способами их конституирования. Но эти же формы должны быть адекватны и задачам обеспечения безопасности деятельности, включая возможности комплексной ее защиты. В целом, ведущее значение имеют формы активности субъекта, то есть формы и технологии управления и защиты деятельности, так как они определяют способы овладения объекта субъектом, также как и механизмы установления субъектом коммуникативного взаимодействия с другими.

С этой точки зрения, именно формы защиты понимания и осуществления жизни человеком опережающим образом отображают возможные эволюционные изменения его целостности и деятельности. Взаимоотношение основных форм защиты информации и ведущих видов ее функционирования в связи с известными стратегиями человеческого взаимодействия может быть компактно представлено на декартовой системе координат, также как и на концентрической или линейной моделях, имея только в виду идею бинарного представления единого в классической науке:

- иерархия (приспособление);
- гетерархия (конкуренция);
- автономия (избегание);
- интеграция (сотрудничество).

При этом линии форм защиты и видов функционирования жизненно важной информации сдвинуты на одну фазу одна относительно другой, так что четвертая по счету форма защиты информации именно опережающим образом определяет первый из видов функционирования информации на каждом новом витке спирали развития человеческих ресурсов. Но неоправданные попытки интеграции информационных потоков субъектов с различными стратегиями могут привести к любому из четырех вариантов функционирования одного из партнеров, в силу все того же самого кардинального значения формы активности (и формы нравственности) по отношению к виду функционирования информации.

В целом, названия и порядок фаз устойчивого развития информационного пространства при условии комплексной его защиты являются следующими: конформат – конфликт – консенсус – консолидация. Понятно, например, что на первой фазе «оптимизация» или «модернизация» информации и вообще жизнедеятельности субъекта информацией может быть только иерархической, предельно однозначной и жесткой по отношению ко всему тому, что составляет «неформат». Форма управления и защиты информации предопределяет содержание, вид ее функционирования, когда акценты во взаимоотношении формы и содержания расставляются, исходя из внешних по отношению к содержанию, конкурирующих интересов субъектов исторического процесса.

ОПЫТ ПРОВЕДЕНИЯ АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Г.Г. Малюга, Г.Д. Томина,
Государственное предприятие «НИИ ТЗИ», г. Минск

Введение

Требования по проведению аттестации систем защиты информации (далее – СЗИ) в государственных информационных системах (далее – ИС), а также ИС, содержащих информацию, распространение и (или) предоставление которой ограничено, установлено законом Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации» (далее – Закон), порядок проведения аттестации определен Положением о порядке аттестации СЗИ, утвержденным Постановлением Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» (далее – Постановление № 675).

Законом государственная ИС определена как «информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц». ИС государственных органов Республики Беларусь согласно Закону подлежат отнесению к государственным ИС, для них обязательным является создание СЗИ с последующим проведением аттестации.

Деятельность по аттестации СЗИ координирует Оперативно-аналитический центр при Президенте Республики Беларусь в пределах его полномочий.

Аттестацию СЗИ проводят организации, имеющие соответствующие специальные разрешения (лицензии) Оперативно-аналитического центра при Президенте Республики Беларусь (далее – специализированные организации).

Владельцы государственных ИС, имеющие в своем составе подразделения по технической защите информации, вправе проводить аттестацию СЗИ, используемых при обработке информации, содержащейся в государственных ИС, владельцами которых они являются.

Поскольку процесс проведения аттестации требует высокой квалификации персонала в области защиты информации, а также опыта разработки автоматизированных систем и систем защиты информации в них, то для проведения аттестации СЗИ ИС чаще всего привлекаются специализированные организации.

Обеспечение процессов создания и аттестации систем защиты информации

Государственные ИС, а также ИС, содержащих информацию, распространение и (или) предоставление которой ограничено, порядок ввода в эксплуатацию которых регулируется Постановлением № 675, условно можно разделить на три группы:

I группа – ИС, которые введены в постоянную эксплуатацию и эксплуатировались до ввода Постановления № 675;

II группа – ИС, которые начали создаваться на момент введения Постановления № 675, а запланированный ввод в постоянную эксплуатацию выпал на время действия Постановления № 675;

III группа – ИС, для которых сроки создания и ввода в постоянную эксплуатацию спланированы с учетом действующего Постановления № 675.

Для эксплуатируемых ИС I группы потребовалось создание и аттестация СЗИ. Эти процессы включались в планы модернизации ИС на следующий год в рамках существующих возможностей по финансированию работ в государственных органах.

Для ИС II группы с утвержденным финансированием и установленным сроком ввода в постоянную эксплуатацию потребовалась срочная корректировка сроков этапов создания ИС в техническом задании, увеличение объема финансирования за счет включения в состав работ мероприятий по созданию и аттестации СЗИ, а также продление срока их ввода в постоянную эксплуатацию.

Для ИС I и II группы владелец ИС должен был решить вопрос определения и присвоения им класса типового объекта информатизации по СТБ 34.101.30.

При наличии в ИС необходимости обработки информации ограниченного распространения владелец должен был принять одно из следующих наиболее приемлемых решений:

1) исключить подключение к сети Интернет и возможность взаимодействия с другими (внешними) ИС, не имеющими аттестат соответствия класса Б2;

2) исключить в ИС обработку информации ограниченного распространения и присвоить ИС класс В3, позволяющий пользователям ИС работать с Интернет со своих рабочих мест и взаимодействовать с другими (внешними) ИС класса В3, имеющими аттестат соответствия;

3) разделить ИС на две изолированные физически системы: ИС класса Б2 и ИС класса В3, в случае необходимости работы с информацией ограниченного распространения и потребности подключения к Интернет или к другим (внешним) ИС. Перенос информации между ИС класса Б2 и ИС класса В3 проводить с использованием машинного носителя с соблюдением организационных мер с антивирусной защитой и контролем целостности переносимых данных.

После принятия решения по отнесению ИС I и II группы к классу типового объекта информатизации владельцу ИС необходимо было выполнить мероприятия по модернизации ИС в соответствии с изменением структуры вычислительной сети ИС. Для этого потребовалось принимать решения по внесению изменений (при необходимости) в:

– состав и структуру комплекса технических средств (КТС) ИС;

– организационную структуру ИС;

– структуру используемого программного обеспечения ИС;

– перечень используемых протоколов обмена информацией;

– общую функциональную схему ИС, включая схемы информационных потоков и режимы обработки информации;

– наличие и характер взаимодействия с другими (внешними) ИС или объектами;

– рабочую и эксплуатационную документацию ИС.

С учетом принятых решений по вышеперечисленным изменениям владельцу ИС требовалось определить необходимый объем финансирования и календарные сроки работ по модернизации или внесению изменений ИС, а

также заключить с исполнителем работ по созданию ИС договор или дополнительное соглашение на выполнение работ и уточнять сроки работ по модернизации или внесению изменений ИС.

Следует заметить, что владелец ИС, имеющий в своей организационной структуре подразделение по технической защите информации (или назначенных должностных лиц, ответственных за реализацию технических мер по защите информации), может создавать и эксплуатировать СЗИ собственными силами, в то время как аттестация СЗИ может проводиться только подразделением по технической защите информации владельца ИС. В случае отсутствия у владельца квалифицированного персонала в области защиты информации к созданию и аттестации СЗИ должны быть привлечены специализированные организации, при этом владелец ИС должен объявить тендер на проведение работ по созданию СЗИ и ее аттестации, а по результатам тендера владелец должен заключить договор на создание и аттестацию СЗИ, определив объем финансирования.

После завершения технического проекта на СЗИ в соответствии с ГОСТ 34.201-89 владелец должен закупить сертифицированные или прошедшие государственную экспертизу средства защиты информации, провести рабочее проектирование СЗИ и приемочные испытания СЗИ.

Аттестация СЗИ ИС на соответствие требованиям НПА и ТНПА в области защиты информации проводится после успешных приемочных испытаний ИС и СЗИ. Ввод в постоянную эксплуатацию ИС проводится после успешной аттестации СЗИ ИС и получения аттестата соответствия (заключение об отказе в выдаче аттестата соответствия).

Проблема выбора криптографических средств защиты информации

Положение о порядке организации криптографической защиты информации в государственных информационных системах, в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено (за исключением государственных секретов), а также в критически важных объектах информатизации (далее – Положение), утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 мая 2012 года № 46 (далее – Приказ № 46), внесло

дополнительные требования по криптографической защите информации.

Решение о криптографической защите информации принимается собственником (владельцем) ИС. При необходимости решения владельцем ИС задач обеспечения конфиденциальности, контроля целостности (неизменности) и подлинности информации в ИС должны применяться средства криптографической защиты информации (далее – СКЗИ). СКЗИ подлежат сертификации в Национальной системе подтверждения соответствия Республики Беларусь или государственной экспертизе на соответствие требованиям безопасности информации, содержащимся в ТНПА и документах, перечень которых приведен в приложении к Положению.

Для ИС класса А2 и Б2 необходимо использовать только программно-аппаратные (программно-технические) или аппаратные (технические) СКЗИ, удовлетворяющие требованиям пункта 11 Положения.

Белорусский рынок сертифицированных (прошедших государственную экспертизу) средств защиты информации имеет широкий выбор программных СКЗИ, а аппаратные и программно-аппаратные СКЗИ представлены очень скудно, что не может удовлетворить все потребности владельцев ИС на текущий момент, что значительно тормозит модернизацию эксплуатируемых ИС и ввод в действие вновь создаваемых ИС.

Таким образом, процесс аттестации СЗИ, использующих СКЗИ, в большинстве случаев не может быть проведен с успешным результатом.

Требуется срочное принятие мер органов государственного регулирования, так и от разработчиков СКЗИ по урегулированию проблемы.

При поэтапной модернизации средств защиты информации, в том числе СКЗИ, не потребуются повторная аттестация только в случае замены аппаратного или программно-аппаратного средства защиты информации на аналог или новую версию программного средства. Все остальные изменения потребуют корректировки ЗБ, эксплуатационной документации СЗИ, методики испытаний средств защиты информации в реальных условиях эксплуатации ИС, проведения испытаний новых средств защиты СЗИ, корректировки учетных форм ОРД СЗИ, а это все требует повторной аттестации.

СЕРТИФИКАЦИЯ ПРОДУКЦИИ В РАМКАХ ТАМОЖЕННОГО СОЮЗА

О.Ю. Кондрахин,

Государственное предприятие «НИИ ТЗИ», г. Минск

Решением Межгосударственного Совета Евразийского экономического сообщества (высший орган Таможенного союза) от 21.05.2010 № 38 с 01.07.2010 вступили в силу Соглашение о взаимном признании аккредитации органов по сертификации (оценке (подтверждению) соответствия) и испытательных лабораторий (центров), выполняющих работы по оценке (подтверждению) соответствия, и Соглашение об обращении продукции, подлежащей обязательной оценке (подтверждению) соответствия, на таможенной территории Таможенного союза.

В соответствии с вышеуказанными соглашениями Стороны взаимно признают аккредитацию органов по сертификации

(оценке (подтверждению) соответствия) и испытательных лабораторий (центров), выполняющих работы по оценке (подтверждению) соответствия, в национальных системах аккредитации государств Сторон, а также признают при подтверждении соответствия продукции, включенной в «Единый перечень продукции, подлежащей обязательной оценке (подтверждению) соответствия в рамках Таможенного союза с выдачей единых документов» и национальные перечни, протоколы испытаний продукции аккредитованных лабораторий.

Согласно требованиям ст. 5 Соглашения об обращении продукции, подлежащей обязательной оценке (подтверж-

дению) соответствия, на таможенной территории Таможенного союза при подтверждении соответствия продукции результаты испытаний продукции (протоколы испытаний), полученные в государстве одной Стороны, признаются органом по сертификации, включенным в Единый реестр, государством Стороны назначения, при соблюдении следующих условий:

- применение одинаковых или сопоставимых методов исследований (испытаний) и измерений продукции;
- проведение испытаний в испытательных лабораториях (центрах), включенных в Единый реестр.

Таким образом, для организации взаимодействия между испытательными лабораториями, в рамках признания результатов испытаний органами по сертификации Сторон, включенных в «Реестр органов по сертификации и испытательных лабораторий (центров) Таможенного союза, осуществляющих оценку соответствия продукции, включенной в Единый перечень продукции, подлежащей обязательной оценке (подтверждению) соответствия в рамках Таможенного союза с выдачей единых документов (Единый перечень продукции)» (далее – Реестр) в системе мероприятий программы Союзного государства можно рассмотреть реализацию следующих направлений работ:

- формирование единого плана стандартизации в области информационной безопасности государств-членов Таможенного союза;
- создание новых правил и процедур в области стандартизации;
- формирование Единого реестра органов по сертификации и испытательных лабораторий в области информационной безопасности;
- включение средств защиты информации, подлежащих оценке (подтверждению) соответствия в Единый перечень продукции Таможенного союза;
- аккредитацию органов по сертификации и испытательных лабораторий в Национальных органах по аккредитации (Испытательная лаборатория по требованиям безопасности

информации Государственного предприятия «НИИ ТЗИ» аккредитована и включена в Реестр);

- актуализация области аккредитации испытательных лабораторий под одинаковые или сопоставимые методы исследований (испытаний) применяемые Сторонами, либо, в случае отсутствия подобных методов – аккредитация в дополнительной области деятельности;

- установление и применение единых обязательных требований к продукции – средствам защиты информации;
- установление единых правил проведения работ по оценке соответствия;

- установление порядка применения мер технического регулирования в отношении третьих стран;

- принятие единых форм сертификатов соответствия и деклараций о соответствии;

- ведение Единого реестра выданных по единой форме сертификатов соответствия и деклараций о соответствии.

При этом, актуальными задачами остаются создание условий для обеспечения свободного обращения продукции (средств защиты информации) на таможенной территории, определение порядка ввоза на таможенную территорию и перемещения между территориями государств Сторон продукции, подлежащей обязательному подтверждению соответствия. Выработка единого подхода к процедурам подтверждения соответствия продукции требованиям технических регламентов с учетом опыта Европейского союза. Разработка межгосударственных стандартов на основе международных требований и технических регламентов.

Литература:

1. Соглашение о взаимном признании аккредитации органов по сертификации, решение Межгосударственного Совета Евразийского экономического сообщества и Соглашение об обращении продукции, подлежащей обязательной оценке (подтверждению) соответствия, на таможенной территории Таможенного союза от 21.05.2010 № 38.

МОДЕЛЬ ИНТЕГРАЦИИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ

М.Ю. Казеев,

Государственное предприятие «НИИ ТЗИ», г. Минск

На сегодняшний день, исходя из богатого опыта и мировых тенденций развития подходов в области информационной безопасности, можно выделить два основных направления государственного регулирования в данной области:

- создание уникальной самостоятельной национальной нормативно-правовой базы, регламентирующей вопросы организации, построения и контроля систем информационной безопасности;

- внедрение международной нормативно-правовой базы в качестве национальной базы, регламентирующей вопросы организации, построения и контроля систем информационной безопасности.

Стоит отметить, что выбор и реализация данных подходов полностью зависит от политики в области ин-

формационной безопасности, реализуемой государством, и обусловлен уровнем развития информатизации, как общества, так и государства в целом, опытом и профессионализмом государственных структур, ответственных за реализацию данной политики и другими основополагающими факторами.

Как правило, приверженность государства одному из вышеупомянутых подходов обеспечивает целостность и согласованность нормативного поля в области информационной безопасности, однако, при их интеграции могут возникать ситуации, сопряженные с такими явлениями, как избыточность, противоречивость и несогласованность.

На сегодняшний день в Республике Беларусь существуют два действующих подхода обеспечения информационной

безопасности, которые регламентируются следующими нормативно-правовыми актами соответственно [1, 2].

[1] регламентирует порядок защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено (далее – информационные системы). Согласно [1] для защиты информации в информационных системах создается система защиты информации (далее СЗИ), включающая комплекс организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Таким образом, обеспечение информационной безопасности информационной системы сводится к процессу создания СЗИ, который включает следующий комплекс мероприятий:

а) классификацию хранящихся и обрабатываемых в информационной системе сведений и разделение информации по категориям доступа;

б) анализ организационной структуры информационной системы, порядка организации вычислительных процессов и условий ее функционирования;

в) присвоение информационной системе класса типового объекта информатизации в соответствии с требованиями технических нормативных правовых актов в области защиты информации;

г) разработку или корректировку политики информационной безопасности;

д) разработку или корректировку задания по безопасности на информационную систему в соответствии с требованиями технических нормативных правовых актов в области защиты информации;

е) реализацию требований задания по безопасности в информационной системе;

ж) оценку соответствия СЗИ требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов, путем проведения мероприятий по аттестации СЗИ;

з) ввод информационной системы в эксплуатацию.

[2] регламентирует процесс разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (далее – СМИБ) организации. Согласно [2] для обеспечения информационной безопасности организации используется циклический процессный подход, включающий процессы:

а) plan (планирования);

б) do (создания);

в) check (проверки);

г) act (модификации).

В соответствии с [2] реализация данных процессов обеспечения информационной безопасности организации сводится к следующему комплексу основополагающих мероприятий:

1. Разработка СМИБ:

1.1. Определение области применения и границ распространения СМИБ;

1.2. Определение политики СМИБ;

1.3. Определение подходов к оценке рисков в организации;

1.4. Идентификация рисков;

1.5. Анализ и оценка рисков;

1.6. Идентификация и оценка вариантов обработки рисков;

1.7. Выбор целей и средств управления для обработки рисков;

1.8. Получение одобрения руководства по предлагаемым остаточным рискам;

1.9. Получение санкции руководства на внедрение и обеспечение функционирования СМИБ;

1.10. Разработка положения о применимости (существующих средств управления);

2. Внедрение и обеспечение функционирования СМИБ:

2.1. Разработка плана обработки рисков;

2.2. Реализация плана обработки рисков для достижения идентифицированных целей управления;

2.3. Внедрение средств управления;

2.4. Определение способов измерения результативности выбранных средств управления или групп средств управления;

3. Мониторинг и анализ СМИБ:

3.1. Реализация процедур мониторинга и анализа с применением специальных средства управления;

3.2. Регулярный анализ результативности СМИБ;

3.3. Измерение результативности средств управления с целью верификации соответствия требованиям безопасности;

3.4. Анализ оценки рисков, а также остаточных рисков и идентифицированных приемлемых уровней риска;

3.5. Проведение внутренних аудитов СМИБ;

3.6. Регулярный анализ СМИБ со стороны руководства;

3.7. Реализация процедур обновления планов в области безопасности;

3.8. Протоколирование действий и событий, которые могли повлиять на результативность или функционирование СМИБ;

4. Поддержка и улучшение СМИБ:

4.1. Внедрение идентифицированных улучшений в СМИБ;

4.2. Реализация корректирующих и предупреждающих действий;

4.3. Обеспечение обмена информацией о действиях и улучшениях со всеми заинтересованными сторонами;

4.4. Контроль соответствия вносимых улучшений поставленным целям СМИБ.

Таким образом, возникает вопрос о возможности применения данных подходов для создания систем информационной безопасности организации, информационная система которой подпадает под требования [1], и соответствующей требованиям [2]. Для ответа на данный вопрос необходимо рассмотреть, как могут соотноситься между собой мероприятия по созданию СЗИ и процессы СМИБ. Возможное наглядное представление данного соотношения приводится в таблице 1.

Проведя анализ полученного соотношения можно заключить, что каждому мероприятию, соответствующему [1], может соответствовать определенный процесс СМИБ, соответствующий [2]. Таким образом, несмотря на распространенное мнение о противоречивости и избыточности требований [1] и [2] в совокупности, процесс построения СЗИ информационной системы и процессы СМИБ могут быть интегрированы в единый процесс построения системы информационной безопасности, удовлетворяющий как [1], так и [2], путем выполнения требований соответствия и расширений (допущений), согласно таблицы 1.

Таблица 1 – Соотношение мероприятий по созданию СЗИ и процессов СМИБ

	СМИБ																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
--	------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Примечание: 1 – ввод информационной системы в эксплуатацию и ее сопровождение; 2 – выполнить процедуры мониторинга и анализа с применением специальных средства управления

Литература:

1. О некоторых вопросах защиты информации: Постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 675.

2. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: СТБ ISO/IEC 27001-2011. – Введ. 01.01.2012. – Минск: Госстандарт Республики Беларусь, 2011.– 36 с.

ОСОБЕННОСТИ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ В ОБНОВЛЕННОЙ РЕДАКЦИИ БАЗОВОГО СТАНДАРТА ОЦЕНКИ БЕЗОПАСНОСТИ

А.Б. Степанян, В.А. Дмитриев, Е.П. Максимович, В.К. Фисенко,
ОИПИ НАН Беларуси, г. Минск

Действующий стандарт СТБ 34.101.2-2004 «Информационные технологии безопасность. Критерии оценки безопасности информационных технологий – Часть 2: Функциональные требования безопасности» устанавливает совокупность функциональных требований, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать функциональные требования к объекту оценки (ОО), в том числе, как для продуктов, так и для систем.

Стандарт СТБ 34.101.2-2004 устанавливает:

- структуры класса, семейства и компонента функциональных требований безопасности продуктов и систем информационных технологий;
- функциональные требования безопасности (ФТБ), распределенные по классам, семействам и компонентам.

Как известно, СТБ 34.101.2-2004 разработан на основе международного стандарта ISO/IEC 15408-2:1999. Позже появились новые редакции стандарта ISO/IEC 15408-2:1999. Например, в 2005 году вышел стандарт ISO/IEC 15408-2:2005, в котором были введены некоторые изменения, например, новое семейство FMT_SMF «Определение функций управления». На основе стандарта ISO/IEC 15408-2:2005 в Республике Беларусь стандарт СТБ 34.101.2-2004 не модифицировался.

В 2008 году вышли новые редакции стандартов ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008, а в 2009 году – ISO/IEC 15408-1:2009. На основе этих версий стандартов было принято решение разработать новые версии стандартов СТБ 34.101.1-3.

В данном докладе излагаются основные изменения новой редакции стандарта СТБ 34.101.2-2004 с учетом ISO/IEC 15408-2:2008, который разработан в ГНУ «Объеди-

ненный институт проблем информатики Национальной академии наук Беларуси».

В новой редакции СТБ 34.101.2 все функциональные требования безопасности предусмотрены только для продуктов информационных технологий, т.е. система (имеется в виду информационная система), как информационная технология, в данном стандарте не рассматривается.

При этом примерами ОО могут быть:

- прикладная программа;
- операционная система;
- прикладная программа в сочетании с операционной системой;
- прикладная программа в сочетании с операционной системой и рабочей станцией;
- операционная система в сочетании с рабочей станцией;
- интегральная схема смарт-карты;
- локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства;
- приложение базы данных, за исключением программных средств удаленного клиента, обычно ассоциируемых с приложением базы данных.

Основные изменения в терминах СТБ 34.101.2:

1) Вместо термина «Комплекс средств безопасности объекта оценки» (КСБО) используется термин «Функциональные возможности безопасности ОО» (ФВБО) (TOE security functionality). Данный термин определяется следующим образом – объединенные функциональные возможности всего аппаратного, программного и программно-аппаратного обеспечения ОО, на которые необходимо базироваться для корректной реализации ФТБ.

Отметим, что аналогичный стандарт (на основе ISO/IEC 15408-2:2005) Российской Федерации «ГОСТ Р ИСО/

МЭК 15408-2-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности» используется термин «Функции безопасности объекта оценки» (ФБО).

2) Вместо термина «Политика безопасности объекта» (ПБО) используется термин «Функциональные требования безопасности» (ФТБ).

3) Заменен термин «Область действия комплекса средств безопасности» (ОДКСБ) в «Объект оценки» (ОО).

4) Все операции с ФТБ остались те же, только в некоторых операциях «Выбор» добавилась новая подоперация «выбор один из», т.е. из предлагаемого множества нужно выбирать только один элемент из множества.

В некоторых компонентах уточнены зависимости (исключены или добавлены новые, например, в FCS_COP.1 добавлена зависимость FDP_ITC.2 «Прием данных пользователя с атрибутами безопасности» и исключена зависимость FMT_MSA.2 «Безопасные атрибуты безопасности»).

Добавлены некоторые новые семейства и компоненты. В частности:

1) в классе FMT «Управление безопасностью», в семействе FMT_MSA «Управление атрибутами безопасности» добавлен компонент FMT_MSA.4 «Наследование значений атрибутами безопасности», который позволяет заданным ролям/политикам предписывать значения, которые наследуются атрибутами безопасности;

2) в классе FMT «Управление безопасностью» добавлено семейство FMT_SMF «Спецификация функций управления» (которое имеет единственный компонент – FMT_SMF.1). Это семейство позволяет определить функции управления, которые должны быть представлены в ОО;

3) в классе FTA «Доступ к объекту оценки», в семействе FTA_SSL «Блокирование сеанса» добавлен компонент FTA_SSL.4 «Завершение сеанса связи пользователем», который дает возможность пользователю завершить свой сеанс связи;

4) в классе FPT «Защита ФВБО» добавлено семейство FPT_TEE «Тестирование внешних сущностей», которое определяет требования для ФВБО для выполнения тестов для одной или более сущностей. При этом внешние сущности могут содержать приложения, запущенные в ОО, аппаратные или программные части, которые запускаются в подчинении ОО (платформы, операционные системы и т.д.) или приложения/блоки, связанные с ОО (система

обнаружения вторжения, межсетевые экраны, серверы регистрации, серверы времени).

Как видно из определения, семейство FPT_TEE является более общим, чем FPT_AMT «Тестирование абстрактной машины», из-за этого семейство FPT_AMT исключено из ФТБ.

Из состава ФТБ исключены следующие семейства, которые невозможно было четко определить в СТБ 34.101.2-2004:

1) Из класса FPT «Защита КСБО»:

– семейство FPT_RVM «Посредничество при обращениях», которое определяло требования по поддержке монитора обращений в состоянии постоянной готовности к предотвращению попыток нарушителей воздействовать на политики средства безопасности (ПСБ);

– семейство FPT_SEP «Разделение на области», которое содержало требования обеспечения гарантии наличия по крайней мере одной защищенной области для выполнения функций ФВБО, и что эта область защищена от внешнего вмешательства и воздействия (например, изменения кода или структур данных ФВБО) со стороны недоверенных субъектов.

Для оценки этих свойств ОО в состав класса «Разработка» гарантийных требований безопасности (ГТБ) включены требования для структурирования и представления ФВБО на различных уровнях и формах абстракции. В частности, требования к описанию архитектурно ориентированных характеристик разделения на области, самозащиты ФВБО и предотвращения обхода функциональных возможностей безопасности рассматриваются в семействах «Архитектура безопасности» (ADV_ARC) и «Внутренняя структура ФВБО» (ADV_INT);

Семейство, связанное с архитектурой «Архитектура безопасности» (ADV_ARC), включает требования и вопросы анализа ОО, базирующиеся на свойствах разбиения на области, самозащиты и невозможности обхода политики безопасности. Эти свойства относятся к ФТБ в том смысле, что не выполнение этих свойств, по всей вероятности, приведет к отказам механизмов реализации функциональных требований безопасности.

Дополнительная информация о таких свойствах архитектуры безопасности как самозащита, разделение на области и невозможность обхода, приводится в Приложении А в разделе А.1 «ADV_ARC: Дополнительные сведения об архитектурах безопасности».

НОВИЗНА И ОСОБЕННОСТИ МЕТОДОЛОГИЧЕСКОГО ПОДХОДА ОБНОВЛЕННОЙ ВЕРСИИ БАЗОВОГО СТАНДАРТА ОЦЕНКИ БЕЗОПАСНОСТИ

В.К. Фисенко, А.Б. Степанян, Е.П. Максимович, А.Ю. Квач,
ОИПИ НАН Беларуси, г. Минск

Введение

Прежде всего, рассмотрим новизну и особенности новой версии первой части «Введение и общая модель» ISO /IEC 15408-1:2009. Стандарт устанавливает основные понятия и принципы оценки безопасности информационных технологий (ИТ), а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ.

Целью настоящего доклада является краткое изложение новизны и особенностей новой версии первой части документа.

По-крупному новизна состоит в следующем:

- исключено понятие «Общие критерии»;
- расширена терминология, приведенная в первой и последующих частях стандарта;
- изменено наименование второй и третьей частей стандарта;

– изменена структура Задания по безопасности, Профиля защиты и пакета;

– конкретизированы концептуальные положения: объекта оценки, категории пользователей, контекста оценки и принятого подхода к представлению материала;

– конкретизированы понятия: актив, проблема безопасности, среда безопасности, корректность объекта оценки, оценка, зависимость, итерация, расширенные компоненты и др.

Кратко рассмотрим перечисленные новые понятия и изменения.

Исключение общего наименования ISO/IEC 15408-1,2,3 – общие критерии и уточнено понятие Объекта оценки

В предыдущих версиях ISO /IEC 15408 использовалось наименование международного стандарта «Общие критерии». В новых версиях такое наименование отсутствует. Это связано с тем, что в ранних версиях объектами оценки (ОО) выступали продукты и системы ИТ. ОО новой версии выступают лишь продукты ИТ.

ОО определяется, как набор программных, программно-аппаратных и/или аппаратных средств, возможно, сопровождаемых руководствами.

Хотя бывают случаи, что ОО представляет собой продукт ИТ, это не единственные случаи. ОО может быть продуктом ИТ, частью продукта ИТ, набором продуктов ИТ, уникальной технологией, которая может быть никогда не будет реализована в виде продукта, или сочетанием указанных вариантов.

Четкое соотношение между ОО и любыми продуктами ИТ является важным только в одном аспекте: оценку ОО, содержащего часть продукта ИТ, не следует ошибочно представлять, как оценку продукта ИТ, в целом.

Примерами ОО являются:

- прикладная программа;
- операционная система;
- локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства.

Термины и определения

Данный раздел является расширенным по отношению к терминам предыдущей серии и включает ряд новых терминов и определений, а именно:

- термины и определения, общие для всего стандарта СТБ 34.101.1,2,3-2013 (всего 84 термина);
- термины и определения, относящиеся к классу ADV «Разработка» (всего 26 терминов);
- термины и определения, относящиеся к классу AGD «Руководство пользователя» (всего 22 термина);
- термины и определения, относящиеся к классу AVA «Оценка уязвимостей» (всего 7 терминов);
- термины и определения, относящиеся к классу ACO «Составной объект».

Краткий обзор

В разделе представлены основные концептуальные положения: понятие категории пользователей, контекст оценки и принятый подход к дальнейшему представлению материала.

Остановимся на категории пользователей. Потребители, разработчики, эксперты уже известны. Интересна категория пользователей – прочие. Стандарт является справочным материалом для всех, кто интересуется вопросами безопас-

ности ИТ или несет ответственность за них. Среди них можно выделить, например, следующие группы:

– лица, ответственные за техническое состояние оборудования, и сотрудники служб безопасности, ответственные за определение и выполнение политики и требований безопасности организации в области ИТ;

– аудиторы как внутренние, так и внешние, ответственные за оценку адекватности безопасности ИТ – решения (которое может состоять из ОО или включать ОО) и др.

Теперь о контексте оценки. Для достижения большей сравнимости результатов оценок их следует проводить в рамках полномочной системы оценки, которая устанавливает стандарты, контролирует качество оценок и определяет нормы, которыми необходимо руководствоваться организациям, проводящим оценку, и самим экспертам.

Системы оценки и процессы сертификации находятся в ведении органов оценки, управляющих системами и процессами оценки, и не входят в область действия СТБ 34.101.1,2,3.

Общая модель

В этом разделе представлены общие понятия, включая контекст использования этих понятий, и подход к их применению. Краткое описание этих понятий приведено ниже.

Активы – это сущности, представляющие ценность для кого-либо. Но так как ценность – это весьма субъективное понятие, то почти все, что угодно, может рассматриваться в качестве активов.

Среда, в которой размещаются эти активы, называется средой функционирования.

Безопасность связана с защитой активов. Для того чтобы уменьшить риски для активов, реализуются контрмеры. Надо иметь в виду, что:

- контрмеры являются достаточными: если контрмеры выполняют то, что заявлено, то угрозам, направленным на активы, обеспечивается противостояние;
- контрмеры являются корректными: контрмеры выполняют то, что заявлено.

Следующим понятием является корректность ОО.

Для определения корректности ОО могут выполняться различные виды деятельности, такие как:

- тестирование ОО;
- исследование различных проектных представлений ОО;
- исследование физической безопасности среды разработки ОО.

Если ГТБ удовлетворяются, то существует гарантия корректности ОО и, таким образом, меньше вероятность, что ОО содержит уязвимости, которые могут быть использованы нарушителем.

Среда функционирования также может быть некорректно спроектирована и реализована и может, таким образом, содержать ошибки, которые ведут к уязвимостям. Посредством использования этих уязвимостей нарушители могут причинить ущерб и/или несанкционированно использовать активы. Среда функционирования является на 100 % корректным отражением задач безопасности для среды функционирования.

Оценка. Стандарт признает два типа оценки: оценка ЗБ/ОО и оценка ПЗ. Оценка ЗБ/ОО проходит в два этапа:

- а) оценка ЗБ: на этом этапе определяют достаточность ОО и среды функционирования;

б) оценка ОО: на этом этапе определяют корректность ОО. Оценка ОО не включает оценку корректности среды функционирования.

Результатом процесса оценки ОО будет:

– либо утверждение, что не все ФТБ удовлетворены, и поэтому не достигнут заданный уровень гарантии к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ;

– либо утверждение, что все ФТБ удовлетворены, и поэтому достигнут заданный уровень гарантии к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ.

Взаимосвязь между Профилем защиты, Заданием по безопасности и объектом оценки

В то время как ЗБ всегда описывает конкретный ОО ПЗ предназначен для описания типа ОО. Поэтому один и тот же ПЗ можно использовать в качестве шаблона для множества различных ЗБ, которые будут использоваться в различных оценках.

Обычно ЗБ описывает требования для ОО и его формирует разработчик ОО, в то время как ПЗ описывает общие требования для некоторого типа ОО и поэтому обычно разрабатывается:

– сообществом пользователей, стремящихся прийти к консенсусу относительно требований для данного типа ОО;

– разработчиком ОО или группой разработчиков подобных ОО, желающих установить минимальный базис для конкретного типа ОО и др.

ПЗ определяет допустимый тип соответствия ЗБ профилю защиты. То есть, в ПЗ устанавливают, какие типы соответствия являются допустимыми для ЗБ.

Если в ЗБ заявляют о соответствии нескольким ПЗ, то оно должно соответствовать каждому из этих ПЗ в такой форме, как это предписано в этом ПЗ. Это подразумевает, что ЗБ может строго соответствовать одним ПЗ и демонстрируемо соответствовать другим ПЗ.

Определение проблемы безопасности: обоснование соответствия в ЗБ должно продемонстрировать, что определение проблемы безопасности в ЗБ является эквивалентным (или более ограничительным), по отношению к определению проблемы безопасности в ПЗ. Это означает, что:

– ОО, который бы отвечал определению проблемы безопасности в ЗБ, также отвечал бы определению проблемы безопасности в ПЗ;

– все среды функционирования, которые отвечали бы определению проблемы безопасности в ПЗ, также отвечали бы определению проблемы безопасности в ЗБ.

Если определено строгое соответствие ПЗ, то применяют следующие требования:

а) Определение проблемы безопасности: ЗБ должно

включать определение проблемы безопасности из ПЗ, может определять дополнительные угрозы и ПБОР, но не может определять дополнительные предположения;

б) задачи безопасности: ЗБ:

– должно включать все задачи безопасности для ОО из ПЗ, но может определять дополнительные задачи безопасности для ОО;

– должно включать все задачи безопасности для среды функционирования (за одним исключением, указанным в следующем пункте данного перечисления), но не может определять дополнительные задачи безопасности для среды функционирования;

– может определять, что определенные задачи для среды функционирования из ПЗ являются задачами безопасности для ОО в ЗБ. Это называется переназначением задачи безопасности. Если задача безопасности переназначена для ОО, то обоснование задач безопасности должно четко показать, какое предположение или часть предположения больше не требуется;

с) требования безопасности: ЗБ должно включать все ФТБ и ГТБ из ПЗ, но может определять дополнительные или иерархические, более строгие ФТБ и ГТБ. Выполнение операций в ЗБ должно быть согласовано с выполнением операций в ПЗ; либо выполнение операций в ЗБ будет таким же, как и в ПЗ, либо приведет к более ограничивающим требованиям (применяют правила уточнения).

Если определено «демонстрируемое соответствие» профилям защиты, то применяют следующие требования:

– ЗБ должно включать обоснование того, почему ЗБ рассматривается как «эквивалентное или более ограничительное» по отношению к ПЗ;

– демонстрируемое соответствие позволяет разработчику ПЗ описать общую проблему безопасности, которая должна быть решена, и обеспечить общее руководство по требованиям, необходимым для ее решения, с пониманием того, что, вероятно, существует более чем один способ ее решения.

Таким образом, новая версия дает возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциональным возможностям безопасности продуктов ИТ и к мерам гарантии, применяемым к этим продуктам ИТ при оценке безопасности. Данные продукты ИТ могут быть реализованы в виде аппаратного, программно-аппаратного или программного обеспечения. В процессе оценки достигают определенный уровень уверенности в том, что функциональные возможности безопасности таких продуктов ИТ, а также меры гарантии, предпринятые по отношению к таким продуктам ИТ, отвечают предъявляемым требованиям.

СТРУКТУРА, ПРАВИЛА И РЕКОМЕНДАЦИИ ПО РАЗРАБОТКЕ ЗАДАНИЯ ПО БЕЗОПАСНОСТИ ОБЪЕКТА ОЦЕНКИ

**В.К. Фисенко, А.Б. Степанян, Е.П. Максимович, А.Ю. Квач,
ОИПИ НАН Беларуси, г. Минск**

В настоящее время в рамках НИР «Аттестат» готовится к введению в Республике Беларусь новой версии государственного стандарта, так называемого «Общие критерии». Уже на данном этапе разработки стандарта можно заявить, что новая версия стандарта изложена более понятно и содержит ряд новых положений. В настоящем докладе

речь будет идти о содержании новой версии Задания по безопасности.

Введение ЗБ

В разделе «Введение ЗБ» описывают ОО в повествовательной форме на трех уровнях абстракции:

Первый уровень: ссылка на ЗБ и ссылка на ОО, обеспечивающие идентификационные материалы для ЗБ и ОО, на который ссылается ЗБ, а именно:

- ссылка на ЗБ: наименования ЗБ, версия, разработчик и дата выпуска;
- ссылка на ОО: наименования разработчика, наименования ОО и номер версии ОО.

Правила:

- если ОО сформирован на основе одного или более известных продуктов, то допускается отразить это в ссылке на ОО путем указания наименований этих продуктов;
- являются недопустимыми случаи, когда основные части ОО или функциональные возможности безопасности не были рассмотрены в процессе оценки, но в ссылке на ОО это не отражено.

Некоторые пояснения:

- ссылка на ОО не обязательно может быть уникальной, если один и тот же ОО оценен несколько раз, например, по инициативе различных потребителей этого ОО, а для него может существовать несколько ЗБ;
- ссылка на ЗБ и ссылка на ОО облегчают индексацию и ссылку на ЗБ и ОО и их включение в состав сводной информации списков оцененных ОО/продуктов.

Второй уровень: аннотация ОО, в которой кратко описывается ОО.

Структура: порядок использования ОО, основные характеристики безопасности ОО, идентификация типа ОО, идентификация типа аппаратных средств/программного обеспечения/программно-аппаратных средств, не входящие в ОО, но требуемые для ОО.

Некоторые пояснения:

- описание использования и основных характеристик безопасности ОО предназначено, чтобы дать общее представление о возможностях ОО с точки зрения безопасности и о том, для чего можно использовать ОО в контексте безопасности. Это должно быть написано для (потенциальных) потребителей ОО;
- в аннотации ОО идентифицируют общий тип ОО, такой как: межсетевой экран, шлюз виртуальной частной сети, смарт-карта, интранет, веб-сервер, система управления базами данных, вебсервер и система управления базами данных, ЛВС, ЛВС с веб-сервером и системой управления базой данных и др.;
- возможна ситуация, когда ОО не может быть легко отнесен к имеющемуся типу, при которой приемлемым является указание на то, что ОО не отнесен ни к одному типу;
- требуется идентифицировать соответствующие, не входящие в ОО, аппаратные средства/программное обеспечение и/или программно-аппаратные средства. Полная и абсолютно детальная идентификация дополнительных аппаратных средств/программного обеспечения и/или программно-аппаратных средств не требуется, но при этом необходима полнота и детализация идентификации, достаточная для определения потенциальными потребителями основных аппаратных средств, программного обеспечения и/или программно-аппаратных средств, необходимых для использования ОО.

Третий уровень: описание ОО, в котором более подробно описывается ОО.

Структура:

- физические границы ОО: список всех аппаратных, программно-аппаратных, программных частей и руководства, которые составляют ОО (подробное описание);

- логические границы ОО: логические характеристики безопасности, обеспечиваемые ОО.

Некоторые пояснения рекомендации:

- описание ОО должно обеспечить оценщикам и потенциальным потребителям общее понимание возможностей безопасности ОО с большей детализацией, чем в аннотации ОО. Описание ОО можно также использовать для описания более широкого прикладного контекста, для которого ОО будет подходящим;
- важная роль физических и логических границ заключается в том, что они описывают ОО способом, не оставляющим неясностей в том, входит ли определенная часть или характеристика в ОО или не входит. Это особенно важно, когда ОО интегрирован с сущностями, не входящими в ОО, и не может быть легко выделен из них.

Утверждения о соответствии (ASE_CCL)

Структура. Соответствие ЗБ описывается на трех уровнях:

Первый уровень: соответствие ЗБ государственному стандарту СТБ 34.101.1,2,3: используемые СТБ 34.101.1,2,3, наличие в ЗБ расширенных компонентов безопасности, отсутствие в ЗБ расширенных компонентов безопасности

Второй уровень: соответствие профилям защиты: перечень в ЗБ профилей защиты, по отношению к которым требуется соответствие.

Третий уровень: соответствие пакетам: перечисление в ЗБ пакетов, по отношению к которым требуется соответствие.

Определение проблемы безопасности

Проблема безопасности включает: угрозы, политики безопасности организации, предположения.

Представляются угрозы, которым должен противостоять ОО, его среда функционирования или их сочетание.

Примеры источников угроз – хакеры, пользователи, компьютерные процессы и инциденты.

Примеры угроз:

- системный администратор, нарушающий приватность пользователя;
- пользователь Интернета, прослушивающий трафик конфиденциального электронного обмена.

Представляются ПБО, которые должны быть реализованы ОО, его средой функционирования или их сочетанием.

Примеры ПБО:

- все продукты, которые используются государственными организациями, должны соответствовать национальным стандартам по генерации пароля и криптографии;
- только пользователям с привилегиями системного администратора и допуском секретного отдела должно быть разрешено управление файл-сервером.

Представляются предположения, которые сделаны по отношению к среде функционирования ОО для обеспечения функциональных возможностей безопасности. Предположения могут быть по отношению к физическим аспектам, персоналу и внешней связности в среде функционирования.

Следует отметить, что в течение оценки эти предположения считаются верными: они в любом случае не проверяются.

4 Задачи безопасности (ASE_OBJ)

Роли задач по безопасности:

- роль первая: предоставить на естественном языке высокоуровневое описание решения проблемы.

Задачи безопасности состоят из совокупности коротких и четких утверждений без чрезмерно больших подробностей, которые формируют высокоуровневое решение проблемы безопасности. Уровень абстракции задач безопасности должен быть таким, чтобы они были ясными и понятными для хорошо осведомленных потенциальных потребителей ОО.

– роль вторая: разделить данное решение на две части, отражающие, что различные сущности решают свою часть проблемы;

Проблема решается двумя частями задач безопасности: задачами безопасности для ОО и задачами безопасности для среды функционирования. Это означает, что данные части решения обеспечиваются двумя различными сущностями: ОО и средой функционирования.

Задача безопасности для ОО включает совокупность задач, которые должны быть достигнуты ОО, чтобы решить свою часть проблемы.

Примеры задач безопасности для ОО:

– ОО должен обеспечивать конфиденциальность содержания всех файлов, передаваемых между ним и сервером;
– ОО должен выполнять идентификацию и аутентификацию всех пользователей до предоставления им доступа к сервису передачи информации, предоставляемого ОО.

Задачи безопасности для среды функционирования включают совокупность утверждений, описывающих задачи, которые должны быть достигнуты средой функционирования.

Примеры задач безопасности для среды функционирования:

– в среде функционирования должно быть обеспечено, чтобы все пользователи ОО были соответствующим образом обучены до того, как им будет разрешено работать с ОО;
– среда функционирования ОО должна ограничить физический доступ к ОО, разрешая такой доступ только персоналу, выполняющему функции администраторов, и персоналу технической поддержки в сопровождении администраторов.

– роль третья: продемонстрировать, что эти части решения формируют полное решение проблемы.

Для демонстрации необходимо:

1. Провести прослеживание (на этапе обоснования задач безопасности), какие задачи безопасности направлены на какие угрозы, ПБОР и предположения.

Прослеживание обеспечивает:

а) отсутствие избыточных задач: каждая задача безопасности сопоставлена, по крайней мере, с одной угрозой, ПБОР или предположением;

б) полнота: для каждой угрозы, ПБОР и предположения имеется, по крайней мере, одна задача безопасности, сопоставленная с ними;

в) корректность сопоставления: предположения всегда делаются по отношению к среде функционирования, а задачи безопасности для ОО не сопоставляются с предположениями.

Примечание: Несколько задач безопасности могут быть сопоставлены с одной и той же угрозой, указывая на то, что сочетание этих задач безопасности направлено на противостояние данной угрозе. Подобное утверждение справедливо для ПБОР и предположений.

2. Показать (на этапе обоснования задач безопасности) путем совокупности логических обоснований, что все угро-

зы, ПБОР и предположения надлежащим образом учтены в задачах безопасности.

Обоснование задач безопасности демонстрирует, что сопоставление является надлежащим: все определенные угрозы, ПБОР и предположения учтены (то есть, угрозам обеспечено противостояние, ПБОР осуществлена, предположения реализованы, если все задачи безопасности, сопоставленные с конкретной угрозой, ПБОР или предположением, достигнуты).

Данная демонстрация содержит результаты анализа эффекта от достижения соответствующих задач безопасности по противостоянию угрозам, осуществлению ПБОР и реализации предположений и приводит к заключению, что это действительно так.

Примечание: Противостояние угрозе не обязательно означает устранение угрозы, а может означать достаточное уменьшение этой угрозы или достаточное смягчение последствий реализации этой угрозы.

Примеры устранения угрозы:

– устранение возможностей со стороны источника угрозы выполнять нежелательное действие;

– перемещение, изменение или защита актива таким образом, что нежелательное действие становится более не применимым к нему;

– устранение источника угрозы (например, отключение от сети ПЭВМ, которые часто «рушат» эту сеть).

Примеры уменьшения угрозы:

– ограничение способности источника угрозы по выполнению нежелательных действий;

– ограничение возможности выполнить нежелательное действие источником угрозы;

– уменьшение вероятности успешного результата, выполненного нежелательного действия;

– сокращение мотивации источника угрозы выполнить нежелательное действие путем сдерживания;

– требование от источника угрозы большей компетентности или больших ресурсов.

Примеры смягчения последствий реализации угрозы:

– частое создание резервных копий актива;

– приобретение дополнительных копий актива;

– страхование актива;

– обеспечение своевременного обнаружения успешных нежелательных действий, чтобы предпринять соответствующие ответные действия.

Примечание: Основываясь на задачах безопасности и обосновании задач безопасности, может быть сделано следующее заключение: если все задачи безопасности достигнуты, то проблема безопасности, определенная в соответствии с ASE_SPD, решена: всем угрозам обеспечено противостояние, все ПБОР осуществлены и все предположения реализованы.

Определение расширенных компонентов (ASE_ECD)

В некоторых случаях, в ЗБ могут быть требования, которые не основаны на компонентах из СТБ 34.101.2 или СТБ 34.101.3. В этом случае, новые компоненты (расширенные компоненты) должны быть определены, и такое определение следует сделать в разделе ЗБ «Определение расширенных компонентов». Это должно быть сделано способом, подобным существующим компонентам СТБ 34.101.2,3: четким, однозначным, использовать обозначе-

ние, способ выражения и уровень детализации, подобные существующим компонентам СТБ 34.101.2,3.

Требования безопасности (ASE_REQ) Функциональные требования безопасности Предварительные пояснения

1. ФТБ являются результатом преобразования задач безопасности для ОО путем их представления на некотором стандартизированном языке. Перевод задач безопасности с естественного языка на стандартизированный способствует более точному описанию функциональных возможностей ОО. Стандартизированный язык обеспечивает использование единой терминологии и понятий при изложении требований безопасности, что обеспечивает проведение сравнения нескольких ЗБ.

2. Не требуется перевод на стандартизированный язык задач безопасности для среды функционирования, так как среда функционирования не оценивается и поэтому не требует описания, направленного на ее оценку.

Способы преобразования задач безопасности в требования безопасности:

- первый способ: использование четкого «языка», т.е. совокупности компонентов, определенных в СТБ 34.101.2;
- второй способ: путем использования операций: назначение, выбор, итерация и уточнение, которые позволяют модифицировать ФТБ с целью обеспечения более точного учета задач безопасности для ОО;
- третий способ: путем определения зависимостей – механизм, который поддерживает более полное преобразование задач безопасности для ОО в ФТБ.

Взаимосвязь между ФТБ и задачами безопасности:

Первая взаимосвязь: прослеживание ФТБ к задачам безопасности для ОО, чем обеспечивается:

- отсутствие избыточных ФТБ: каждое ФТБ сопоставлено, по крайней мере, с одной задачей безопасности;
- полнота по отношению к задачам безопасности для ОО: для каждой задачи безопасности для ОО имеется, по крайней мере, одно ФТБ, сопоставленное с ней.

Несколько ФТБ могут быть сопоставлены с одной и той же задачей безопасности для ОО, указывая на то, что сочетание этих требований безопасности удовлетворяет данную задачу безопасности для ОО.

Вторая взаимосвязь: предоставление логического обоснования для сопоставления: сопоставление является надлежащим: если все ФТБ, сопоставленные с конкретной задачей безопасности для ОО, удовлетворены, то эта задача безопасности для ОО достигнута.

В случаях, когда ФТБ являются очень близкими к изложению задач безопасности для ОО, демонстрация может быть очень простой.

Гарантийные требования безопасности

ГТБ – описание того, каким образом должен быть оценен ОО. В данном описании используется стандартизированный язык по следующим причинам:

- чтобы обеспечить точное описание того, каким образом ОО должен быть оценен. Использование стандартизированного языка способствует точному описанию и исключению неоднозначности;
- чтобы обеспечить сопоставление двух ЗБ. Стандартизированный язык обеспечивает использование единой терми-

нологии и понятий при изложении требований безопасности, что обеспечивает проведение сравнения нескольких ЗБ.

Стандартизированный язык определяется как совокупность компонентов, определенных в СТБ 34.101.3. Преобразование задач безопасности в ГТБ осуществляется:

- путем использования операций: назначение, выбор, итерация и уточнение, которые позволяют модифицировать ГТБ с целью обеспечения более точного учета задач безопасности для ОО.

- путем определения зависимостей – механизм, который поддерживает более полное преобразование задач безопасности для ОО в ФТБ.

ГТБ и обоснование требований безопасности

ЗБ также содержит обоснование требований безопасности, которое содержит аргументы, позволяющие считать конкретную совокупность ГТБ надлежащей. Каких-либо конкретных требований к такому обоснованию не предъявляется. Задача этого обоснования заключается в том, чтобы обеспечить пользователям ЗБ понимание причины выбора конкретной совокупности ГТБ.

Примером несогласованности является ситуация, когда в «Описании проблемы безопасности» присутствуют угрозы, источник которых (нарушитель) обладает достаточными возможностями, а в совокупность ГТБ включен младший компонент из семейства AVA_VAN или вообще не включен никакой компонент из данного семейства.

Выводы по требованиям безопасности: если все ФТБ и ГТБ удовлетворены и все задачи безопасности для среды функционирования достигнуты, то имеется гарантия к тому, что проблема безопасности, определенная в соответствии с ASE_SPD, решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы. Объем приобретенной гарантии определяется ГТБ, а достаточность этого объема гарантии определяется пояснением выбора ГТБ.

Общая спецификация ОО (ASE_TSS)

Задача данного раздела – предоставить потенциальным потребителям ОО описание того, каким образом ОО удовлетворяет все ФТБ. В разделе следует привести описание основных технических механизмов, которые с этой задачей использует ОО. Уровень детализации данного описания должен быть достаточным, чтобы позволить потенциальным потребителям понять основной облик и реализацию ОО.

Например, если ОО является ПК, подключенным к Интернет, и ФТБ включают компонент FIA_UAU.1 для определения аутентификации, то в краткой спецификации ОО следует указать, каким образом выполняется аутентификация: посредством пароля, токена, сканирования радужной оболочки глаза и т.д.

Может быть также приведен больший объем информации, такой, например, как указание применимых стандартов, используемых в ОО для удовлетворения ФТБ, или более детальное описание.

Литература:

1. СТБ 34.101.1. – 2013 (ИСО/МЭК 15408-1:2009) Информационная технология. – Методы и средства безопасности. – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель.

К ВОПРОСУ О ЧЕЛОВЕЧЕСКОМ ФАКТОРЕ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.И. Иванченко, Е.А. Свирский,
БГУ, г. Минск

Главной отличительной чертой современного этапа развития цивилизации являются ее информатизация, которая порождает высокие темпы обновления научных знаний, и, как следствие, технологий и технических устройств и систем, применяемых не только на производстве, но и в быту и в сфере досуга человека. Темпы обновления знаний существенно опережают возможности развития человеческого интеллекта.

Все чаще и чаще традиционная образовательная система становится не способной обеспечить выпускникам долговременную гарантию занятости, поскольку высокие темпы обновления знаний требуют постоянной переподготовки. Наиболее ярко это проявляется в инновационных или вновь ставших на инновационный путь развития отраслях деятельности общества. Очевидно, знания обновляются по степенному закону, а человеческий интеллект – по линейному, поэтому человек обречен на пожизненную учебу. Учеба и работа все теснее переплетаются и учеба становится пожизненным занятием.

Информатизация общества приводит к возникновению различных потенциальных проблем, связанных с нарастающей виртуализацией жизни. Открытость информационных пространств делает возможным несанкционированное вмешательство в функционирование информационных систем предприятий и государственных структур и проникновение в частную жизнь граждан. Кроме этого, обществу придется столкнуться с глубокой и трудно реализуемой опасностью, которая заключается в большом расслоении социума по знаниям.

Необходимо отметить, что в настоящее время происходит трансформация подходов к обеспечению информационной безопасности, которая заключается в смене парадигмы методов и средств защиты информации с технических на социогуманитарные (на первый план выходит человеческий фактор – человек становится составной частью информационной системы). Также следует отметить, что и роль человека в процессах информатизации общества также меняется, возрастает его влияние, как источника деструктивных действий, так и

фактора положительного воздействия на информационные системы в целом и обеспечение их безопасности в частности.

Это повышает роль нормативно-правового обеспечения, административных процедур и уровня профессиональной подготовки. В современных условиях постоянно усиливается воздействие на человека в системе с использованием методов социальной инженерии, а также методов контактного воздействия. В связи с этим, должны постоянно совершенствоваться методы повышения компетентности всех участников информационных отношений, их психологической устойчивости и созидательной мотивации.

В условиях высоких темпов обновления знаний и всевозрастающего их объема традиционное образование и самообразование не обеспечивают должного эффекта. На повестку дня встает вопрос выработки новых форм управления образованием в информационных высокотехнологичных сферах и создание эффективной инфраструктуры поддержки процессов обеспечения информационной безопасности.

Эта инфраструктура должна включать такие институты как правового обеспечения, технического нормирования, консалтинга в области информационной безопасности, оценки уровня информационной безопасности (включая аудит и управление рисками), менеджмента инцидентов информационной безопасности. Конкретная реализация такой инфраструктуры возможна с использованием идеи консорциума компетенций, включающего в себя центры реагирования на информационные инциденты, аудиторские фирмы, учреждения образования, научные организации, технический комитет по стандартизации в области защиты информации, органы, формирующие правовое поле в области информационных отношений, и т.п.

Такая инфраструктура должна, не вдаваясь в подробности, обеспечивать решение следующей задачи: оказывать компетентную помощь в создании и эксплуатации систем менеджмента информационной безопасности.

ПОДПИСКА-2013

Подписку на журнал «Электроника инфо» можно оформить в отделении связи по месту жительства с любого месяца.

ПОДПИСКА В БЕЛАРУСИ: «Белпочта» (подписной индекс – 00822).

ПОДПИСКА В РОССИИ: «Роспечать» (подписной индекс – 00822),

«АРЗИ – Почта России» (подписной индекс – 91654).

Читатели также могут подписаться по национальным каталогам: агентств «МК-Периодика», «Информнаука», «Интерпочта-2003» и «Урал-Пресс»; «Пресса» (Украина).

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

ТЕХНОЛОГИЧЕСКОЕ И НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ ТРАНСГРАНИЧНОГО ЭЛЕКТРОННОГО ЮРИДИЧЕСКИ-ЗНАЧИМОГО ДОКУМЕНТООБОРОТА

**С.А. Кирюшкин,
ООО «Газинформсервис»**

В законодательствах стран Единого экономического пространства (ЕЭП), как и в законодательствах большинства современных государств, где есть нормы связанные с электронным документооборотом, обеспечение юридической силы, как свойства электронных документов, базируется на гарантиях аутентичности и целостности документов. При этом, в основном¹, для обеспечения свойств аутентичности и целостности электронных документов используются криптографические методы, а правовые основы закладываются в международном и национальном законодательстве. Поэтому для организации трансграничного защищенного электронного юридическизначимого взаимодействия может потребоваться согласование между странами-участниками отличий правового регулирования (например, требований к условиям применения криптографических средств) и отличий в средствах и способах обеспечения заданных значений защищенности.

Для организации защищенного электронного документооборота в Беларуси, России и Казахстане, в соответствии с рядом национальных нормативно-правовых актов, используются криптографические средства. При этом, все указанные страны развивают собственную криптографию, имеют собственные стандарты криптографических алгоритмов, используемых для создания и проверки ЭП (ЭЦП) и собственные реализации данных алгоритмов (средства электронной подписи и их аналоги²). В общем случае, эти решения между собой не совместимы, т.е. электронный документ, подписанный ЭЦП на основе криптографических стандартов Республики Беларусь, не может быть проверен при помощи средств ЭЦП Республики Казахстан и российских средств ЭП. Аналогично и в случае с электронным документом, под-

писанным на основе Российских и Казахских средств криптографической защиты информации (СКЗИ).

Наиболее очевидным решением в этой ситуации, казалось бы, является использование общего, единого для ЕЭП криптографического стандарта для процедур электронной подписи (рисунок 1).

В пользу этого подхода говорит наличие криптографических стандартов СНГ – ГОСТ 34.310-2002. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования». Но такой подход противоречит национальным законодательствам, которые определяют необходимость использования сертифицированных по национальным стандартам средств электронной подписи, а так же не позволяет гармонизировать правовую основу применения электронной подписи в разных странах (а отличия существенные, начиная с терминов, заканчивая смысловым содержанием аналогов собственноручной подписи). По этим причинам вышеуказанные стандарты СНГ не имеют широкого применения и не могут быть использованы для решения задачи трансграничных госзакупок в Таможенном Союзе.

Другим очевидным решением, казалось бы, должен стать подход на основе импорта/экспорта средств электронной подписи (СКЗИ) партнеров, взаимный обмен ими, для оснащения национальных ЭТП и поставщиков госзаказа (рисунок 2).

Но этот вариант имеет большое количество организационных и технических сложностей, и кроме того, не разрешает весь перечень проблем. Прежде всего, средства электронной подписи являются шифровальными (криптографическими) средствами, а их экспорт и импорт имеет ряд существенных ограничений, затрудняющих реализацию данного варианта. В соответствии с «Положением о порядке ввоза на таможенную территорию таможенного союза и вывоза с таможенной территории таможенного союза шифровальных (криптографических) средств»:

«Ввоз и вывоз шифровальных средств осуществляется на основании разовых лицензий, выдаваемых уполномоченным органом государства-участника Таможенного союза, на территории которого зарегистрирован заявитель».

¹Есть исключения, в частности Федеральный закон РФ № 63-ФЗ от 06.04.2011 предусматривает возможность использования некриптографической простой электронной подписи, которая в данном материале рассматриваться не будет, как неприменимая для рассматриваемых прикладных задач.

²В основе стандартов стран ЕЭП лежат общие подходы, но в настоящее время национальные реализации «навстречу» не совместимы.

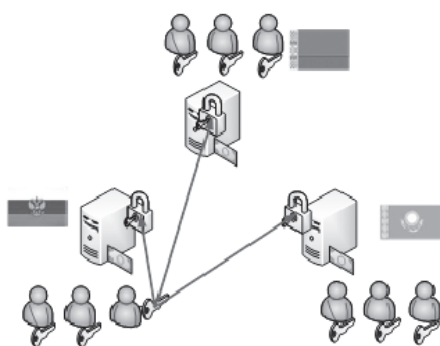


Рисунок 1 – Взаимодействие поставщиков с ЭТП ЕЭП на основе единого криптографического стандарта

Кроме того, ряд вопросов, связанных с использованием средств электронной подписи, требует их периодического обслуживания провайдером сертификационных услуг (например, удостоверяющими центрами), которые функционируют в соответствии с требованиями национальных законодательств и получение таких сервисов не в стране присутствия затруднено (например, изготовление квалифицированного сертификата ключа проверки электронной подписи иностранцу). Даже при решении задачи ввоза-вывоза средств электронной подписи для конкретной информационной системы, при масштабировании системы организационные проблемы возникают вновь, так как они требуют поэтапного учета этих средств, и каждый случай ввоза или вывоза требует оформления разовой лицензии.

К техническим особенностям данного варианта следует отнести так же необходимость оснащения всех ЭТП и всех поставщиков полным набором средств электронной подписи, что в настоящее время, кроме организационных затруднений, осложняется и отсутствием совместимости, при работе на одном средстве вычислительной техники наиболее распространенных в странах Таможенного союза СКЗИ.

К правовым недостаткам данного варианта следует отнести то, что в этом случае сторонам не предоставляется

возможность получения документального подтверждения правомерности применения сертификата ключа проверки подписи для подписания конкретного типа документов в соответствии с законодательством страны происхождения электронного документа. В результате, каждый из контрагентов должен принимать решение о доверии электронному документу, не имея на это достаточных правовых оснований.

Таким образом, вариант, основанный на вывозе и ввозе СКЗИ, не является технологичным и неприменим для массового использования, для развивающихся информационных систем и для информационных систем предполагающих наличие четких правовых условий применения электронных документов, к которым электронные торговые площадки и процедуры госзаказа относятся в полной мере.

Для реализации защищенного трансграничного электронного юридическизначимого документооборота на основе криптографических средств целесообразно использовать иные подходы, позволяющие реализовать адекватные (по обеим сторонам границы) уровни криптографической защиты информационных потоков и достаточные правовые основания для признания юридической силы электронных документов, т.е. методы, обеспеченные достаточной нормативной базой.

За годы, прошедшие с момента постановки данного вопроса на повестку дня в Российской Федерации (как правило, здесь приводится 2006 год, когда в рамках Федеральной целевой программы «Электронная Россия» был создан узел международного взаимодействия Общероссийского государственного информационного центра), данный вопрос был проанализирован экспертами разных стран, объединенными в различных международных форматах – ЕврАзЭС, КТС (ЕврАзЭК), ШОС, РСС, АТЭС и др. В результате этой многолетней работы были выработаны три базовых принципа:

- для создания «пространства доверия» на основе технологий информационной безопасности и в строгом соответствии с нормами международного и национального права, необходимо чтобы каждая из взаимодействующих сторон оставалась в своем национальном правовом поле;
- необходимо чтобы каждая из взаимодействующих сторон использовала собственные национальные криптографические стандарты;
- решение вопросов гармонизации технологий криптографической защиты и юридическизначимого оформления «пространства доверия» должно быть делегировано специализированным операторам, функционирующим по принципу Доверенной третьей стороны (ДТС)³.

Схема взаимодействия сторон при реализации этих базовых принципов представлена на рисунке 3.

Данная схема, соответствующая ей технология, а так же правовые и организационные аспекты ее применения будут раскрыты в докладе и освещены в аналитической записке МОО «АЗИ» опубликованной по адресам:

<http://www.gosbook.ru/node/66513>

<http://www.gaz-is.ru/files/analit-zapiska.pdf>

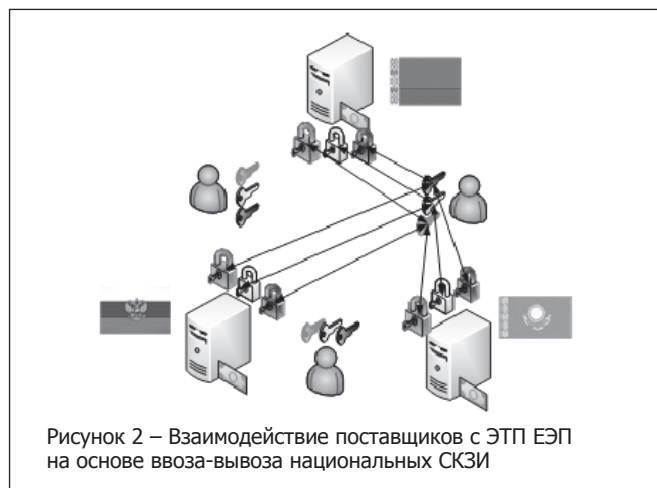


Рисунок 2 – Взаимодействие поставщиков с ЭТП ЕЭП на основе ввоза-вывоза национальных СКЗИ



Рисунок 3 – Взаимодействие поставщиков с ЭТП ЕЭП на основе сервисов валидации электронных документов с помощью ДТС

³ Доверенная третья сторона (ДТС) – это организация или представитель организации, который оказывает одну или несколько услуг безопасности, и является доверенным для других субъектов относительно действий, связанных с этими услугами безопасности (ITU IT Recommendation X.842. Information technology – Security Techniques – Guidelines for the use and management of trusted third party services).

ВОПРОСЫ ОРГАНИЗАЦИИ ТРАНСГРАНИЧНОГО ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ И ОКАЗАНИЯ ЭЛЕКТРОННЫХ УСЛУГ

Г.Д. Томина, Д.А. Комликов, А.В. Юрьева,
Государственное предприятие «НИИ ТЗИ», г. Минск

Введение

Основная проблема организации трансграничного обмена электронными документами (далее – ЭД) и оказания электронных услуг (далее – ЭУ) состоит в создании доверенной инфраструктуры, содержащей центры доверенных сервисов, используемых информационными системами (далее – ИС), юридическими и физическими лицами при трансграничном взаимодействии. При этом доверенные сервисы не должны зависеть от используемых средств электронной цифровой подписи (далее – ЭЦП) или национального законодательства и стандартов в области ЭЦП.

Техническая концепция организаций доверенной третьей стороны (далее – ДТС) изложена в международных рекомендациях X.842, X.843, уточнена в ETSI TS 101733, которые определяют требования к перечню доверенных сервисов, а также к использованию, управлению и услугам ДТС по поддержке приложений ЭЦП и предполагает наличие национального центра (или центров) ДТС.

Совокупность систем доверенных сервисов ДТС и доверенных удостоверяющих центров (далее – УЦ) должна составить основу национального пространства доверия (сегмента доверия) государства.

Организация трансграничного взаимодействия для оказания ЭУ и ЭД между юридическими и физическими лицами различных государств предполагает объединение национальных сегментов доверия в единое пространство доверия. При этом принципы организации, форматы, интерфейсы и протоколы используемые в национальных сегментах доверия, не должны подвергаться корректировке. Следовательно, существующие национальные законодательства и стандарты в области ЭЦП и пути их развития не будут подвергаться диктату и навязыванию чужих, т. н. унифицированных стандартов ЭЦП. Каждый из национальных центров ДТС должен быть аккредитован в своей стране в соответствии с национальным законодательством и получить полномочия на оказание ЭУ доверенной стороны в национальном сегменте и выдачу по результатам услуги электронных квитанций, подписанных ЭЦП ДТС.

Практически во многих национальных инфраструктурах открытых ключей подписи на сегодняшний день используются форматы сертификатов, соответствующие X.509, а службы электронного нотариата оказывают услуги по удостоверению обладанием информацией с или без ее предоставления сервису и (или) проверки действительности ЭЦП на текущий момент времени, и (или) проверки действительности сертификата по X.509 по протоколу DVCS, в соответствии с RFC 3029, выработки квитанций со штампом времени по RFC 3161, проверки действительности сертификата с помощью протокола OCSP по RFC 2560.

При трансграничном взаимодействии совокупность взаимосвязанных национальных ДТС необходима для «перезаверения» трансграничных сообщений. Фактически, для двух национальных пространств доверия, в которых

создается и будет использоваться ЭУ или ЭД, национальные ДТС должны выполнять роль моста доверия, в котором квитанция ДТС, подписанная страной отправителя, проверяется ДТС страны получателя квитанции, заверяющей квитанцию своей ЭЦП.

Проблемы организации трансграничного обмена и пути их решения

Следует заметить, что для обеспечения полноценного трансграничного обмена ЭД недостаточно наличия в качестве инструмента цифрового сертификата по X.509 V.3. Т. к., во-первых, не все реквизиты, которые однозначно бы идентифицировали юридическое лицо, можно разместить в сертификате. Во-вторых, отдельную проблему составляет апостиль ЭД – нотариальное заверение перевода официального документа на другой язык для признания официальных документов установленного образца при межгосударственном обмене.

Теоретически модель (архитектура и основные компоненты) единого межгосударственного пространства доверия на сегодняшний день не определена: иерархическая, браузерная или сетевая. Развитие электронного бизнеса и ЭУ между юридическими лицами государств упорно продвигает общество в сторону сетевой модели, когда потребности бизнес-сообществ потребуют присутствия на рынке ЭУ множества национальных и региональных центров ДТС.

Пример технического решения по организации ДТС приведен в концепции «Интегрированная информационная система внешней и взаимной торговли таможенного союза». Данное решение одобрено на межгосударственном уровне и реализуется в Казахстане, Республике Беларусь (далее – РБ), Российской Федерации (далее – РФ) и может быть применено не только для государственных и межгосударственных нужд, но и для бизнеса.

Основной задачей центров ДТС при трансграничном обмене является проведение проверочных процедур по:

- проверке действительности ЭЦП на электронном сообщении (документе);
- проверке действительности сертификата;
- выработке штампа времени, связанного с проверкой, и отправке квитанции, подписанной ЭЦП центра ДТС.

Последняя процедура позволяет продлить срок действия алгоритма и ключа подписи и обеспечить действительность исходной ЭЦП на длительное время, что особенно важно при ведении электронных архивов.

Однако это только техническая сторона организации взаимодействия. Для придания юридической значимости трансграничного взаимодействия центров ДТС необходимо принять свод нормативных правовых, национальных и межгосударственных актов (далее – НПА), определяющих:

- на национальном уровне – порядок аккредитации центров ДТС, для получения полномочий по проверке действительности сертификата и ЭЦП под документом и по

выдаче квалифицированной справки-квитанции о результатах проверки, подписанной ЭЦП центра ДТС; порядок подтверждения подлинности иностранной ЭЦП; порядок сертификации технических средств ЭЦП и услуг ДТС;

– на межгосударственном уровне – соглашение о признании юридической силы квалифицированных справок-квитанций и ЭЦП национальных центров ДТС; договорные отношения между центрами ДТС стран, подписавших соглашение.

Принятие национальных и межгосударственных НПА позволит при возникновении спорных ситуаций получить юридически значимые доказательства, что конкретный национальный центр ДТС проверил и подтвердил законность и действительность ЭЦП на ЭД и несет юридическую (и в том числе финансовую) ответственность за результаты.

Еще одной важной проблемой обеспечения трансграничного взаимодействия является предоставление технической возможности по экстренному признанию ЭД недействительным (важно при декларировании перемещения грузов, выдачи санитарных разрешений и т. д.). Механизмы экстренного отзыва ЭД с действительной ЭЦП на сегодняшний день не стандартизованы и реализуются различными способами, например, механизм отзыва ЭЦП ЭД, предложенный ООО «Топ-кросс» (РФ). Национальные центры ДТС должны уметь выдавать квалифицированные справки-квитанции на отзыв ЭД.

Второй пример – подтверждение ДТС регистрации и ведения идентификаторов объектов, что позволяет регистрировать и публиковать описание структур информационных блоков с целью идентификации объектов в ИС, например, перемещение товаров, помеченных RFID-идентификаторами.

Актуальной является проблема идентификации и аутентификации взаимодействующих сторон. Сегодня аутентификация пользователя производится с использованием сертификатов, выдаваемых УЦ, и протоколов TLS, Kerberos и RADIUS (EAP-TLS). В одном из ведомств РФ в качестве идентификатора госслужащего применили OID его компьютера, что при иерархической структуре (уровень сельсовета) может оказаться проблемой.

Целесообразной представляется идея консорциума W3C о цифровом удостоверении единого формата XML, выдаваемой центром ДТС на основании его сертификата (выданного УЦ) для идентификации в конкретной ИС. Единый формат обеспечивает независимость цифрового удостоверения от конкретных механизмов аутентификации и позволит не только переносить дополнительную информацию, необходимую для новых сервисов, но и использовать информацию из цифрового удостоверения для придания юридической значимости ЭД, заверенному ЭЦП.

Техническим решением по реализации цифрового удостоверения может являться электронная пластиковая карта или аппаратный идентификатор, хранящие как личный ключ подписи владельца-пользователя, который подтверждает правомерность обладания сертификатом, так и цифровое удостоверение, выданное центром ДТС.

Согласно НПА РБ [1], все криптографические операции должны быть реализованы аппаратным, аппаратно-программным способом и соответствовать [2]. Криптографические операции выработки и проверки подписи должны быть реализованы со стороны пользователя

на «борту» электронной пластиковой карты или аппаратного идентификатора, а со стороны центра ДТС – в аппаратном или аппаратно-программном криптографическом комплексе, что повысит уровень доверия взаимодействующих сторон.

Заключение

В то же время, начиная с середины октября 2013 года, в соответствии с первой частью пункта 4 [3] в государственных ИС (в том числе в государственных ДТС) криптографическая защита информации будет осуществляться только в части обеспечения целостности и подлинности электронных документов.

Требования к применению программно-аппаратных и технических средств криптографической защиты информации будут распространяться только на служебную информацию ограниченного распространения. Таким образом, на критически важных объектах информации, а также в ИС, обрабатывающих информацию, распространение и (или) предоставление которой ограничено (за исключением государственных секретов и служебной информации ограниченного распространения), личные ключи подписи пользователей можно будет использовать программным способом, что особенно чревато в системах оказания электронных услуг по приемке таких электронных документов как, например, декларации таможенного груза, электронных медицинских карточек, актов гражданского состояния и пр.

При организации технических и криптографических мер защиты в ДТС вышеуказанным способом уровень доверия к такой системе со стороны пользователей будет незначительным.

Для обеспечения надлежащего уровня защиты компонентов (ДТС и УЦ) национальной инфраструктуры открытых ключей необходимо до ввода в действие [3] привести, как указано в Указе Президента Республики Беларусь от 16.04.2013 № 196, законодательство в соответствие. С учетом того, что в государственных ИС при обработке информации, распространение и (или) предоставление которой ограничено, должны применяться аппаратные, аппаратно-программные средства защиты информации.

Литература:

1. Положение о порядке организации криптографической защиты информации в государственных информационных системах, а также в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 мая 2012 года № 46 «О некоторых мерах по реализации Указа Президента Республики Беларусь от 8 ноября 2011 года № 515».

2. Перечень технических нормативных правовых актов и документов, в которых определены требования к средствам криптографической защиты информации и на соответствие которым осуществляется сертификация и государственная экспертиза (Приложение к [1]).

3. Положение о технической и криптографической защите информации в Республике Беларусь, утвержденное Указом Президента Республики Беларусь от 16 апреля 2013 года № 196.

К ВОПРОСУ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЯХ

С.А. Брутчиков, Г.К. Резников, Ю.Г. Резников,
ОДО «ВирусБлокАда»

Мировая практика показывает, что важнейшей проблемой, стоящей перед руководством и службой безопасности предприятий и организаций, в том числе государственных, в настоящее время, является проблема внутренних угроз информационной безопасности.

Очевидно, что внутренний злоумышленник, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями об информационной системе, может нанести гораздо больший ущерб, чем нарушитель, взламывающий такую систему через Интернет. Так, по различным оценкам, от 50 % до 80 % атак, направленных на получение информации ограниченного распространения, начинается из локальной сети предприятий и организаций (интрасети).

Особенную актуальность проблема защиты от внутренних угроз приобрела в связи с появлением и повсеместным распространением мобильных накопителей информации, подключаемых через USB-порты: flash-диски, винчестеры с USB-интерфейсом и т. д. Внутренний злоумышленник может практически незаметно пронести на территорию большинства предприятий компактный носитель большого объема. Если не предпринимать специальных мер по блокировке USB-портов, удалению информации, не требующейся для дальнейшего использования, в том числе следов ее обработки, злоумышленник может, используя свой легальный доступ к информации, скопировать на такой носитель всю интересующую его или его заказчиков информацию.

Отсутствие контроля действий пользователя и журнала аудита действий пользователя позволяет злоумышленнику остаться безнаказанным.

Как правило, внешние электронные носители используются не столько для длительного хранения информации, сколько для ее доставки на ПЭВМ с целью дальнейшей обработки. На такие носители злоумышленник может легко записать специальную вредоносную программу. Отсутствие проверки данных на наличие вредоносных программ и межсетевое экранирование позволяют злоумышленнику не только инфицировать ПЭВМ или корпоративную сеть, но и получить, в том числе по сети, с помощью вышеупомянутой вредоносной программы требуемую ему информацию.

Последние тенденции в развитии вредоносного ПО показывают, что наибольшую популярность у злоумышленников получают так называемые руткит-технологии, используемые для защиты от обнаружения и удаления вредоносных программ.

Промежуток времени между первым появлением вредоносной программы в «живой природе» и ее попаданием в антивирусные базы может составлять как несколько часов для большинства вредоносных программ, так и несколько месяцев. По сообщениям западных источников, червь Stuxnet, который первыми в мире нашли сотрудники ОДО «ВирусБлокАда» в 2010 г. с помощью разработанного на предприятии антируткита Vba32, успел до своего обнаружения повлиять на выполнение иранской ядерной программы.

Однако до сих пор на рынке средств защиты информа-

ции отсутствуют программные средства, обеспечивающие комплекс следующих услуг:

- контроль действий пользователя при работе с информацией на ПЭВМ;
- удаление информации, не требующейся для дальнейшего использования, в том числе, следов ее обработки;
- ограничение и контроль доступа пользователей к внешним устройствам;
- ведение аудита действий пользователя при работе с информацией, функционирования прикладного и системного ПО с возможностью просмотра и редактирования списка объектов и устройств в электронных журналах только администратором безопасности;
- осуществление проверки данных (в т.ч. поступающих или отправляемых с ПЭВМ) на наличие вредоносных программ (в реальном масштабе времени и по запросу пользователя/администратора);
- реализация функции межсетевого экранирования.

Кроме того, не разработаны программные средства, являющиеся полноценным инструментом для поиска аномалий операционных систем, причиной которых является присутствие в системе вредоносных программ.

В настоящее время по ГНТП «Защита информации-2» разрабатывается программный комплекс, являющийся комплексным решением, направленным на обеспечение целостности и доступности информации в информационных системах государственных организаций.

Разрабатываемый программный комплекс обеспечивает выполнение следующих основных функций:

- работоспособность, как в локальном, так и сетевом варианте использования;
- централизованное управление всеми программными модулями и управление программными комплексами по сети;
- защиту ПЭВМ от вредоносного ПО;
- защиту от несанкционированного доступа к информации;
- межсетевое экранирование;
- удаление информации, не требующейся для дальнейшего использования, в том числе следов его обработки, в ручном и автоматическом режимах;
- контроль целостности конфигурации СВТ и установленного на нем программного обеспечения;
- ведение журналов аудита доступа пользователей к информации, функционирования прикладного и системного ПО;
- контроль целостности файлов комплекса с реализацией функции восстановления с единого центра управления в случае выявленного нарушения;
- контроль и управление перечнем программных процессов, функционирующих на ПЭВМ для каждого пользователя;
- постоянный автоматический, либо по запросу анализ обрабатываемой информации на наличие вредоносных программ в соответствии с заданными администратором условиями;

– непрерывный контроль за действиями пользователя при работе с информацией (доступ, запись, чтение, копирование информации, вывод на печать и т.д.), состояния защиты системы для своевременного обнаружения нарушений политики безопасности системы и действий вредоносных программ с возможностью уведомления администратора при возникновении критических ситуаций;

– контроль и фильтрацию проходящих через изделие сетевых пакетов, (IP v.4/IP v.6) в соответствии с заданными правилами (сетевые адреса получателя и отправителя, используемый протокол передачи данных, порт), и принятие на основе интерпретируемых правил соответствующих решений;

– выставление приоритета на потребление ресурсов ОС при выполнении фоновых заданий комплекса, объединение защищаемых объектов в группы и подгруппы для применения к ним отдельных политик и заданий, контроль работы комплекса, состояния защищаемых объектов и отображение их состояния;

– уведомление администратора о критических событиях, возникающих при работе комплекса (с возможностью выбора уровня подробности протоколирования), о регистрации события, ведении, хранении и статистической обработке отчетов о результатах работы комплекса;

– просмотр и редактирование списка защищаемых объектов и устройств только администратором;

– назначение периодических и разовых заданий объектам по управлению клиентской частью ПО;

– хранение в центральном журнале аудита событий безопасности и результатов заданий администратора;

– контроль и ограничение доступа (доступ, запись, чтение) к следующим видам устройств:

– USB-устройства (flash-накопители, внешние жесткие диски, цифровые камеры и аудиоплееры, карманные компьютеры; локальные и сетевые принтеры);

– контроллеры беспроводных сетей (Wi-Fi, Bluetooth, IrDA);

– сетевые карты и модемы, дисководы, CD и DVD-приводы, накопители на жестких магнитных дисках;

4) внешние порты LPT, COM и IEEE 1394 и другие устройства, имеющие в ОС символическое имя.

Журналы аудита комплекса содержат:

а) события безопасности комплекса;

б) данные по работе модулей комплекса;

в) информацию о выданных заданиях и их результатах;

г) данные об инцидентах и нештатных ситуациях, связанных с работой ПО;

д) данные о всех успешных и не успешных действиях пользователей при обращении к устройствам и информации в соответствии с требованиями по контролю.

В рамках той же государственной научно-технической программы для обнаружения неизвестных вредоносных программ, использующих руткит-технологии, разрабатывается инструмент (программное средство) для поиска аномалий операционной системы. Данный инструмент позволяет специалисту, работающему с ним, проводить анализ найденных аномалий. По результатам проведенного анализа специалист имеет возможность обнаружить и обезвредить вызвавшую данную аномалию вредоносную программу или передать ее для дальнейшего анализа и вставки в антивирусную базу.

Основные технические характеристики программного средства:

– поиск в операционной системе аномалий, появившихся в результате воздействия вредоносного программного обеспечения и иных видов угроз;

– сбор статистики о состоянии системы и ее передача на анализ администраторам безопасности;

– обеспечение функциями удаления вредоносных программ, вызывающих в операционной системе аномалии (по возможности).

Наличие вышеописанных комплекса и программного средства, являющегося инструментом для поиска вредоносных программ по аномалиям в операционной системе, позволит улучшить процесс обеспечения бесперебойной работы и предотвратить утечки информации, вызванных внутренним злоумышленником, а также функционированием вредоносных программ в информационных системах государственных организаций.

ПРИМЕНЕНИЕ СРЕДСТВ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В РАЗЛИЧНЫХ СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Д.Ю. Счастный,
ОКБ САПР, г. Москва

Технологии биометрического распознавания являются уникальными с точки зрения построения систем защиты информации (СЗИ). С одной стороны, по биометрическим параметрам можно однозначно идентифицировать человека (пользователя) – предъявляемые и оцениваемые параметры (отпечаток пальца, сосудистое русло, динамика почерка) позволяют системам защиты информации точно определить пользователя системы. С другой стороны, те же самые биометрические параметры могут выступать и в качестве аутентифицирующей пользователя информации – предъявив тот же самый палец или руку, пользователь однозначно подтверждает обладание некоторой уникальной информацией, которую «знает» только он. В настоящее вре-

мя биометрические технологии существенно подешевели и упростились с точки зрения применения в СЗИ – сканеры отпечатка пальца стоят десятки долларов, есть SDK для различных ОС. Попробуем разобраться в этой технологии более подробно с тем, чтобы понять, как ее можно применять именно в контексте СЗИ.

Суть применения биометрических технологий можно описать следующим образом: пользователь предъявляет свой параметр, сканер его считывает, производится сравнение с эталоном и с некоторой долей вероятности возвращается результат – соответствует ли предъявленный параметр эталону или нет. В описанной последовательности действия можно выделить несколько ключевых моментов,

которые являются критическими с точки зрения защиты информации: процесс получения параметра, процесс получения эталона, процесс сравнения, процесс предъявления результата. Не вызывает сомнения тот факт, что конечный результат будет признаваться сторонним приложением (в том числе и СЗИ) достоверным только в том случае, если каждый из этих процессов не будет изменен и если каждый из них будет оперировать аутентичными надежными данными и взаимодействовать с другими процессами по защищенным каналам.

В реальности, не все процедуры взаимодействия и получения данных защищаются технологически. Часть процедур защищается организационными мерами.

Встраивание в СЗИ процедур работы с биометрическими технологиями производится через интерфейсы, специфици-

рованные для каждой конкретной практической реализации технологии. В настоящее время наиболее распространены следующие реализации биометрических технологий:

- «все в одном» – в одном приборе объединены все сущности (считыватель, верификатор, работа с эталоном);

- «эталон передается снаружи» – прибор считывает биометрический параметр и верифицирует его с переданным в него эталоном;

- «эталон в базе» – прибор считывает биометрический параметр и передает его в верификатор, функционирующий в ОС, для поиска соответствующего эталона в базе эталонов.

Каждая из реализаций имеет свои особенности при встраивании их в СЗИ и эти особенности обязательно нужно учитывать как разработчикам, так и эксплуататорам СЗИ для адекватной оценки решения в целом.

ОБЛАЧНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО РУКОПИСНЫМ ПАРОЛЯМ «SIGNTOLOGIN»

П.С. Ложников,
ООО «Научно-технический центр «КАСИБ»

На сегодняшний день, использование возможностей глобальной сети Интернет в любой отрасли экономики приобрело стратегическое значение. За последние годы наметилась тенденция интенсивного переноса бизнес-процессов большинства компаний в облачные ресурсы сети Интернет. Наиболее популярные Google- и Apple-инфраструктуры используются для распространения мобильных бизнес-приложений, являющихся дополнительным или основным каналом продаж для многих отраслей бизнеса. Сегодня на рынке услуг и розничной торговли есть выигрышная стратегия: чтобы завоевать клиента, нужно «прийти» к нему в мобильное устройство. Функциональность таких приложений будет только увеличиваться в условиях глобальной конкуренции. Таким образом, количество мобильных приложений и ресурсов сети Интернет, предназначенных для удаленного взаимодействия типа «продавец-покупатель», «банк-клиент», «партнер-партнер» и др. будет стремительно расти. На сегодняшний день, этот рост выявляет необходимость надежной аутентификации удаленных пользователей.

По результатам глобальных исследований информационной безопасности в отчете Global State of Information Security Survey 2012 года на третьем месте среди угроз безопасности для облачных вычислений стоит угроза несанкционированного доступа пользователей на сайт компании. По данным технических отчетов Information Security Breaches Survey 2010 она была признана одной из самых опасных для бизнеса угроз информационной безопасности, мировые потери от которой приблизились к 1 трлн. долл. в год [1]. Приостановить или хотя бы уменьшить прирост таких потерь является актуальной задачей, решение которой значительно отстает от запросов в информационной сфере.

К настоящему времени широко распространена стандартная парольная аутентификация с использованием пары «логин/пароль». Количество паролей, которые современный человек вынужден запоминать, постоянно увеличивается. С точки зрения информационной безопас-

ности эффективность такой аутентификации будет только снижаться. Пользователи, не задумываясь, позволяют сохранять (запоминать) пароли браузерам и мобильным приложениям на персональных устройствах доступа к сети Интернет. Доступным решением этой проблемы стало применение двухэтапной аутентификации, реализованной, в подавляющем большинстве, с помощью мобильных телефонов. После успешной парольной аутентификации пользователю передается одноразовый пароль (в виде SMS) на ранее зарегистрированный мобильный телефон. Сегодня, так производят аутентификацию своих клиентов большинство банковских Интернет-сервисов, Интернет-магазинов, социальных сетей.

Но здесь необходимо учитывать тенденцию расширения функциональности современных мобильных устройств связи. Они становятся одновременно средством сотовой связи и доступа к сети Интернет. Это порождает огромную проблему информационной безопасности и сводит на нет набирающую популярность двухэтапную аутентификацию с помощью одноразовых sms-паролей (подтверждений). В случае отчуждения такого мобильного устройства от хозяина, процедура аутентификации может быть выполнена без его ведома.

Таким образом, сегодня возникает потребность в доступных для массового применения технологий аутентификации, неуязвимых к отчуждению идентификатора от владельца. С 2004 года именно доступные технологии биометрической аутентификации исследовались и разрабатывались в Научно-техническом центре «КАСИБ» (г. Омск). Реалистичнее всех выглядит технология аутентификации пользователя по динамике написания подписи или фиксированного рукописного пароля. Данная технология относится к области динамической биометрии. Еще 5-6 лет назад этот способ аутентификации требовал покупки дополнительного оборудования – графического планшета (дигитайзера) со световым пером. Эволюция мобильных устройств за последние годы в сторону ис-

пользования сенсорных экранов ввода, позволила сделать эту технологию максимально доступной. В конце 2012 года Научно-технический центр «КАСИБ» выпустил Beta-версию облачного сервиса «SignToLogin» (<http://signtologin.com>), реализующего аутентификацию пользователей по динамике написания рукописных паролей, как услугу.

Процедура аутентификации сводится к тому, что для каждого удаленного пользователя сначала должен быть создан эталон рукописного пароля. Процесс создания эталона сводится к последовательному вводу 10-ти реализаций рукописного пароля на сенсорном экране мобильного планшета (возможно с использованием стилуса), что может занять в среднем 3 минуты. Пользователь должен написать своим обычным почерком рукописное слово. После ввода необходимого количества реализаций, выполняется их статистическая обработка для получения признаков, необходимых в дальнейшем для аутентификации динамических характеристик написания рукописного пароля пользователя [2]. Как правило, это только функции скорости курсора в плоскости сенсорного экрана. Но если пользователь расписывается световым пером, чувствительным к нажатию на плоскость графического планшета, то будет использоваться еще и функция давления. Это повысит надежность аутентификации. Облачный сервис «SignToLogin» формирует эталонные значения всех необходимых характеристик пользователя и «запоминает» их.

Во время процедуры аутентификации введенная реализация рукописного пароля будет обработана по такому же принципу, что и реализации, вошедшие в эталон. В режиме аутентификации обработанная реализация сравнивается с эталонными значениями с помощью специальных алгоритмов и методов, которые делают сервис «SignToLogin» максимально удобным для пользователя. Введенные реализации рукописного слова (подписи) автоматически масштабируются и при этом не чувствительны к поворотам в плоскости экрана. В случае успешной аутентификации пользователя, введенная реализация рукописного слова добавляется в эталон, вытесняя из него самую позднюю реализацию. Таким образом, эталон рукописного пароля всегда обновляется и становится не чувствительным к изменениям почерка пользователя.

Учитывая, что система «SignToLogin» представляет собой облачную услугу аутентификации, необходимо обеспечить безопасность облачных вычислений данного сервиса. Система имеет распределенную архитектуру, все вычисления, связанные с аутентификацией пользователей и регистрацией пользовательских эталонов производятся на защищенном сервере. Организации, нуждающиеся в дополнительной аутентификации своих удаленных партнеров, проходят процедуру регистрации в системе (рисунок 1). Для каждой компании-клиента генерируется уникальный «Application ID» и секретный ключ, комбинация которых

The screenshot displays the SignToLogin beta web application. The top navigation bar includes links for Dashboard, How it works, Documentation, Pricing, Help, and a Logout button for 'TestName'. The breadcrumb trail shows 'Home / Companies / Companies Name'. The main content area is titled 'Companies Name' and features a sidebar with links to Profile, Devices, Companies, and Notifications. The main panel has tabs for Info, Account, Users, and Billing. Under the 'Account' tab, there is a 'Public Key' input field and a 'Generate public key' button. Below this, instructions state: 'To add signtologin form on your website just copy widget code placed below and paste it on your login page.' This is followed by the 'Application id: 108' and 'Secret key: d62307fb38c9ff90b63727fdf316dacc'. At the bottom, a 'Widget code:' section contains the following HTML/JavaScript code:

```
<script src="//signtologin.com/js/api.js"></script>
<script>initAPI(108);</script>

<div id="stl-auth"></div>
```

Рисунок 1 – Регистрация компании в облачной системе «SignToLogin», реализующей аутентификацию пользователей по динамике написания рукописных паролей

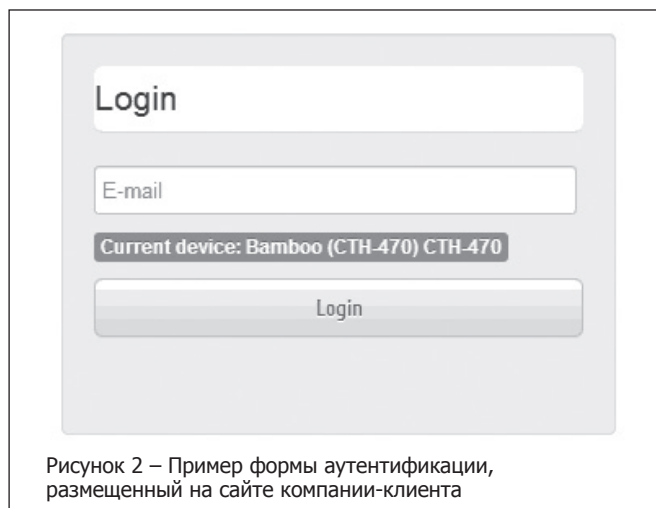


Рисунок 2 – Пример формы аутентификации, размещенный на сайте компании-клиента

будет использоваться для шифрования результатов аутентификации пользователей, возвращаемых сервером «SignToLogin». Система также генерирует специальный HTML-код формы аутентификации, который должен быть размещен на Интернет-ресурсе или встроен в бизнес-приложение компании-клиента (рисунок 2).

Далее компания-клиент может рассылать приглашения пользователям для их регистрации в системе «SignToLogin» с привязкой к своему профилю. Для большей надежности аутентификации, например, удаленных сотрудников, можно организовать их очную регистрацию в присутствии сотрудников соответствующей службы безопасности.

С целью защиты от атак на «прослушивание» соединения между пользователем и сервером «SignToLogin» во время процедуры аутентификации используется протокол HTTPS. Уникальность технологии аутентификации по ру-

кописным паролям заключается в том, что пользователь не может написать одинаковые слова с точностью до пикселя. Эта особенность данной технологии делает ее неуязвимой к атакам с помощью муляжей биометрических идентификаторов.

Практическое применение выше описанного сервиса аутентификации целесообразно в комплексе со стандартной парольной аутентификацией. Как и любая другая биометрическая технология, она возвращает вероятностный результат, который может дать дополнительную информацию о пользователе в спорных ситуациях. В настоящее время коллективом Научно-технического центра «КАСИБ» разрабатывается расширенный комплект средств разработки (SDK) для его использования в мобильных Android- и iOS-приложениях компаний-клиентов. В первую очередь, разрабатываемый SDK будет интересен для облачных систем документооборота, так как в этой сфере подпись является традиционным средством заверения личности. Помимо информации о том, с какой вероятностью рукописную подпись на документе поставил ваш удаленный партнер, можно будет получать сведения о дате и месте подписания документа, а также о наличии внесенных изменений в подписываемый документ.

Литература:

1. Епифанцев Б.Н., Ложников П.С., Сулавко А.Е., Борисов Р.В. Комплексированная система идентификации личности по динамике подсознательных движений // БИТ. – 2011. № 4. – С. 97–102.
2. Pavel Lozhnikov, Oksana Chernikova. Handwriting dynamics as a means of authentication / ICTST 2011: 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates. – P. 176–179.

НЕКОТОРЫЕ ПРОГРАММНО-АППАРАТНЫЕ РЕШЕНИЯ ЗАДАЧИ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В МАССОВЫХ ТЕХНОЛОГИЯХ

Ю.В. Виланский,

Институт современных знаний имени А.М. Широкова

Аутентификация пользователей электронных систем является важнейшим элементом обеспечения информационной безопасности. Как известно, аутентификаторы можно условно разделить на категории, основанные на знании (пароли, пин-коды), владении (электронные ключи, карточки с магнитной полосой и т.д.), неотъемлемых свойствах субъекта (отпечаток пальца, радужная оболочка глаза и т.д.) или на комбинации различных факторов вышеупомянутых категорий. Использование нескольких факторов для аутентификации увеличивает надежность процесса.

Обычная схема взаимодействия пользователя с системой, реализующей некоторую массовую информационную технологию, приведена на рисунке 1. Одним из тонких моментов, связанных с обеспечением взаимодействия пользователя с информационной системой, является необходимость реализации восстановления аутентификационных данных в случае их утраты легальным пользователем.

Самые «дешевые» способы аутентификации обеспечиваются на основе использования пользовательских паролей. К сожалению, такие схемы являются и самыми уязвимыми либо из-за легкости подбора пароля (при использовании

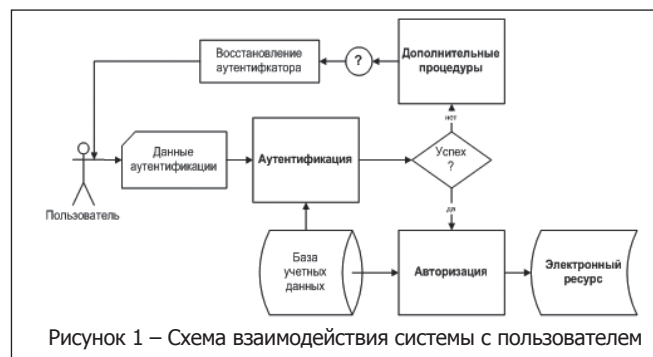


Рисунок 1 – Схема взаимодействия системы с пользователем

«слабых» паролей), либо из-за человеческого фактора (при использовании «сильных» паролей). Слабости такой аутентификации привели к широкому распространению программно-аппаратных решений. Наиболее надежные решения реализуются на основе получения неотъемлемых характеристик субъекта. Однако такие решения требуют дорогостоящих организационных и технических мероприятий и возможности их внедрения достаточно ограничены. В реальных массовых электронных технологиях наиболее распространенным способом является аутентификация, основанная на пользовательских паролях. Наиболее компромиссным вариантом, обеспечивающим реализацию надежных схем аутентификации, в настоящее время является использование аутентификации на основе паролей (пин-кодов) и так называемых различных электронных ключей. Особенностью таких устройств обычно является наличие некоторой защищенной области для хранения сертификатов и криптографических ключей (см., например [1, 2]). При использовании таких устройств требуется установка на пользовательскую систему специального программного обеспечения, что связано с необходимостью проведения дополнительных мероприятий и не всегда возможно.

Основой для всех схем аутентификации является обладание субъекта неким уникальным объектом или знанием. В случае использования электронного ключа это само устройство с секретным ключом в защищенной памяти и пин-код (пароль, известный пользователю), подтверждающий права доступа к этой памяти. С точки зрения ОС, любое устройство – это лишь набор специфицированных интерфейсов и данных. Аппаратная особенность наблюдается ОС, как особенность интерфейса или данных. Такую особенность можно создать (и создают, в том числе и злоумышленники) искусственно.

Если возможно получить гарантированный, неподдельный уникальный идентификатор устройства, то используя криптографические механизмы можно обеспечить защищенное хранение секретных ключей, используя обычные USB-накопители (USB-диски). Такие механизмы могут включать в себя пороговые схемы разделения секрета (ПСПС), симметричные (СШ) и ассиметричные (АШ) шифрсистемы и функции хеширования ([3, 4]). USB-диски имеют ряд достоинств. Они дешевы, широко распространены, поддерживаются большинством систем. Являясь носителями данных, они позволяют разместить в своей памяти специализированное программное обеспечение для работы под управлением различных операционных систем на разнообразных аппаратных платформах. USB-диски имеют ряд идентифицирующих их характеристик, позволяющих выполнить привязку программного обеспечения к конкретному устройству.

Для использования USB-диска в качестве электронного ключа, естественно записать на него данные, по сути, являющиеся секретными ключами и/или мастер-ключами. Хранение таких данных допускается только в зашифрованном виде. При потере USB-диска с такими ключами (как, впрочем, и при потере обычного электронного ключа) теряется доступ к соответствующему пользовательскому ресурсу.

Схемы ПСПС позволяют разделить секрет между авторизованным подмножеством пользователей. Применение этих схем, в совокупности с другими механизмами безопасности позволяет обеспечить как конфиденциальность криптографических ключей, так и возможность восстановления данных совместно разрешенным пользователем и поставщиком

устройства выполнив «привязку» этих данных к USB-диску. На рисунке 2 показан вариант инициализации устройства. Посредством криптографического генератора (ГСЧ) создают мастер-ключ (МКЕУ). С помощью ПСПС мастер-ключ делится на доли. При этом идентификатором для доли, связанной с USB-диском, является значение некоторой функции от параметров устройства (SUID).

В результате на устройство записывается информация (SAD0), которая содержит долю, соответствующую SUID и оставшиеся доли, необходимые для восстановления данных МКЕУ. При этом необходимо обеспечить невозможность восстановления конкретных параметров устройства по известному значению SUID. Если это условие выполнено, то значение SUID неизвестно, когда устройство отсутствует и может быть вычислено при его наличии. Таким образом, можно обеспечить выполнения принципа невозможности «обхода» средств защиты данных [5, С. 315]. Другие данные, нужные для восстановления МКЕУ санкционированным пользователем (на рисунке – PDATA), при необходимости помещаются в специальное хранилище. Естественно, такая схема требует использования пароля пользователя, что необходимо и при использовании аппаратных USB-ключей. Аналогичной процедурой можно «привязать» USB-диск к специальному ПО и аппаратным средствам.

Использование USB-дисков позволяет реализовывать многофакторные схемы аутентификации, основанные на пользовательских паролях, данных, записанных на USB-диске и характеристиках устройства (или устройств). Такие ключи можно использовать в корпоративных системах, как для аутентификации, так и для сопоставления с разрешенными для работы компьютерными системами. Другим вариантом использования является возможность эксплуатации устройства на «чужих» компьютерах для безопасного доступа к удаленным пользовательским ресурсам.

Можно выделить следующие объекты, которые должны использоваться для аутентификации с использованием USB-устройства.

Разделяемый секрет – двоичная случайная строка заданной длины (зависит от параметров системы), генерируемая поставщиком продукта, выборки из этой строки могут использоваться в различных целях. Основным ее назначением является обеспечение, совместно с паролем пользователя, конфиденциальности мастер-ключа при отсутствии соответствующего USB-устройства хранения данных и возможность восстановления аутентификационных данных пользователя

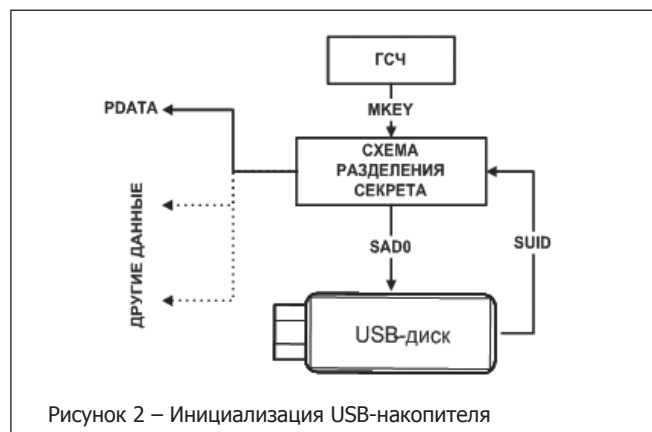


Рисунок 2 – Инициализация USB-накопителя

в случае выхода из строя USB-устройства. Он может использоваться для шифрования мастер-ключа, в том числе и в оперативной памяти, и шифрования данных (метаданных) на USB-носителе.

Мастер-ключ – случайная двоичная строка. Желательно, чтобы он не был известен поставщику продукта. Используется для обеспечения конфиденциальности данных пользователя на внешних компьютерных системах, как ключ для алгоритма шифрования и разделения данных MV2.

Идентификатор USB-устройства – набор данных, однозначно идентифицирующий устройство. Используется для вычисления идентификатора при восстановлении разделяемого секрета. Назначение – обеспечить аутентификацию USB-устройства.

Преобразованный пароль пользователя – результат преобразования пользовательского пароля программным обеспечением. Используется для аутентификации пользователя и обеспечения конфиденциальности мастер-ключа. Не хранится в системе.

Можно выделить следующие механизмы безопасности, которыми должно обладать программное обеспечение, реализующие аутентификатор на USB-накопителе.

Схемы разделения секрета – для обеспечения конфиденциальности разделяемого секрета. Обеспечивает привязку данных в сейфе к конкретному устройству.

Криптографический(ие) алгоритм(ы) симметричного шифрования – для обеспечения безопасного хранения мастер-ключа и данных, и метаданных пользователя.

Криптографические функция хеширования – для идентификации защищенных пользовательских файлов и проверки подлинности USB-устройства. Также могут использоваться при генерации случайных значений.

Литература:

1. «Аладдин Р.Д.»: [электронный ресурс]. – 2012. – Режим доступа: <http://www.aladdin-rd.ru/catalog/etoken/>. – Дата доступа: 22.03.2012.

2. Рутокен С.: [электронный ресурс]. – 2012. – Режим доступа: <http://www.rutoken.ru/products/all/rutoken-s/>. – Дата доступа: 22.03.2012.

3. Алферов, А.П. Основы криптографии. / А.П. Алферов [и др.] – М.: Гелиос АРВ, 2002. – 480 с.

4. Мао, Венбо. Современная криптография: теория и практика. / Венбо Мао. – М.: Издательский дом «Вильямс», 2005. – 768 с.

5. Кузнецов Н.А. Информационная безопасность систем организационного управления. Теоретические основы / Н.А. Кузнецов и др.; [под ред. акад. Н.А. Кузнецова, д.т.н. В.В. Кульбы], в 2 т. М. Наука, 2006. Т. 1. – 2006. – 495 с.

ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА В ИНТЕГРИРОВАННЫХ СИСТЕМАХ МЕНЕДЖМЕНТА ПОСРЕДСТВОМ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

И.И. Лившиц,

Департамент базовых услуг и аутсорсинга, г. Санкт-Петербург

Аннотация

В статье рассмотрены подходы к решению проблем обеспечения непрерывности бизнеса (Business Continuity) в интегрированных системах менеджмента (ИСМ) посредством проведения систематических аудитов информационной безопасности (ИБ) в соответствии с требованиями ряда международных стандартов. Актуальность данной работы вызвана рядом факторов, к наиболее значимым можно отнести постоянное появление новых угроз ИБ, критическую зависимость бизнеса от ИТ и возрастающую техническую сложность проведения оценок (аудитов) уровня защищенности ИТ-инфраструктуры.

В качестве методической базы применяются международные стандарты: ISO/IEC 27001:2005 – определяет требования к системам менеджмента информационной безопасности (СМИБ) [2], ISO 22301:2012 – определяет требования к системам менеджмента непрерывности бизнеса (СМНБ) [6], PAS 99:2012 определяет требования к ИСМ, ISO/IEC 20000-1:2011 – определяет требования к системам управления услугами (СУУ) [4] и ISO 9001:2008 – определяет требования к системам менеджмента качества (СМК) [1].

Новые угрозы

В последнее время активно проявляются новые типы угроз, негативное воздействие которых (impact) чрезвычайно опасно для ИТ-инфраструктуры и бизнеса в целом.

Угрозы неконтролируемого оборота корпоративной информации. Согласно результатам исследования Symantec, половина сотрудников, уволенных за последние 12 месяцев, продолжает хранить ценную конфиденциальную информацию с прошлой работы, а 40% из них планируют пользоваться этой информацией на своем будущем рабочем месте. Также 62% считают приемлемым перенос рабочих документов на личные компьютеры (планшеты, смартфоны). При этом 56% работников не считают преступлением использовать конфиденциальную информацию конкурента.

Угрозы техногенных катастроф. По материалам «Мегафона», после наводнения в Крымске летом 2012 г., когда часть базовых станций была выведена из строя, возникла сильная нагрузка на сети. По инициативе Роскомнадзора операторами «большой тройки» было достигнуто соглашение о межсетевом роуминге при аварийных ситуациях. При инциденте с Челябинским метеоритом в 2013 г. были выведены из строя 65 базовых станций GSM (12,9%) и 180

базовых станций UMTS (36,6%). В результате другие операторы приняли колоссальную нагрузку: в сети «ВымпелКома» нагрузка возросла в 20 раз, в сети МТС нагрузка выросла в 8–10 раз.

Социальные сети. По данным международного исследования «Лаборатории Касперского», проводившегося среди компаний, корпоративная сеть которых насчитывает менее 250 компьютеров, около 49 % представителей «малого и среднего экономического сектора» рассматривают социальные сети в качестве главного источника угроз ИБ.

Проблемы обеспечения непрерывности бизнеса ИСМ

Известно, что ИСМ подразумевает внедрение и обеспечение соответствия требованиям двух и более систем менеджмента, например, СМНБ + СУУ + СМИБ (см. PAS 99-2012). Применительно к целям данной публикации основной фокус будет обращен на проблему обеспечения непрерывности, что достаточно подробно может быть изучено (и в известной степени – оценено) на соответствие известным требованиям. Например, для СМИБ проблема обеспечения непрерывности бизнеса отражена в стандарте ISO/IEC 27001:2005 [2] в разделе A.14 «Business Continuity Management», в стандарте ISO 22301:2012 применительно к СМНБ [6] установлены требования «Business continuity» (пункт 6.2) и «Business continuity strategy» (пункт 8.3), применительно к СУУ в стандарте [4] установлены требования «Service continuity and availability management» (пункт 6.3). На практике предложены и реализованы различные модели и методы решения проблем обеспечения непрерывности бизнеса ИСМ [7], но единой методики анализа выбора вариантов (множества альтернатив) для оценки соответствия требованиям бизнеса не сформировано.

Отчасти эти проблемы являются сложно разрешимыми в силу неустоявшейся практики менеджмента рисков, т.к. в СМК (стандарты серии 9000) вообще нет таких требований, а подавляющее большинство ИСМ включают в себя «базовую» СМК. Такое «ограничение» не позволяет провести обстоятельный анализ требований ИСМ и сформировать адекватный выбор эффективных средств обеспечения ИБ (security controls). Следующим известным противоречием является проблема «конвертации» полученной оценки уровня информационной безопасности (например, по известной «триаде безопасности» п. 3.4 [2] или ее расширению по «подотчетности», «неотказуемости» или «надежности») в официальный сертификат. Постановка задачи по формированию системы оценки уровня непрерывности (например, в терминах «целевого стандарта» СМНБ или ИСМ) не предполагает автоматического прохождения какой-либо внешней оценки с целью «гарантированного» получения официального сертификата (например, на соответствие требованиям ISO/IEC).

Таблица 1 – Выборка недоступности сервисов ведомств

ФОИВ	Сумма времен недоступности всех сервисов ведомства за неделю	Доля времени недоступности сервиса за период
МВД	197:39:29	32,9%
ФССП	175:16:04	29,2%
ГИБДД	116:45:06	19,5%
ФСС	92:38:31	15,4%
Росалкогольрегулирование	81:01:09	13,5%
Росздравнадзор	54:34:27	9,1%
Росреестр	30:13:42	5,0%

Следующей известной проблемой справедливо считают ограниченность ресурсов при проведении различных типов аудитов (как внутренних, так и внешних). Известно, что аудит базируется на «выборочном принципе» оценки, т.е. «если несоответствия не найдены, это не значит, что их нет». Очевидно, что бизнес, в силу экономических факторов не может позволить затраты, превышающие доходы; более того, с учетом жестких реалий экономики XXI века бизнес стремится оптимизировать любые расходы, за исключением минимального выполнения обязательных требований «регуляторов».

Примеры многих известных компаний только подтверждают этот принцип – абсолютно неуязвимых систем не бывает, следовательно, ни одна методика оценки не способна автоматически гарантировать абсолютную надежность для бизнеса по любому набору критериев [7]. В качестве актуального примера рассмотрим известные публичные данные по оценке доступности ресурсов федеральных ведомств РФ (по данным Snews). В таблице 1 отражены данные по оценке сервисов федеральных ведомств (с метрикой недоступности > 5%).

Походы к решению проблемы обеспечения непрерывности бизнеса

На примере рассмотренных выше угроз и ряда противоречий покажем несколько примеров практического решения проблемы обеспечения непрерывности ИСМ в процессе проведения аудитов ИБ. Прежде всего, еще раз примем во внимание классическую «триаду безопасности» [2] – «конфиденциальность», «целостность» и «доступность». Для примера ИСМ в составе СУУ, СМИБ и СМНБ возможно определить «базис», на фундаменте которого будет выполняться анализ требований ИСМ – это соглашение об уровне сервиса (SLA). Строго говоря, в модели СМИБ [7] могут быть предложены произвольное количество альтернатив (например, стандартов ISO) и факторов (например, средств обеспечения ИБ), но требования рассмотренных выше стандартов применительно к проблеме обеспечения непрерывности бизнеса могут быть инкорпорированы в единую сущность – SLA, что значительно облегчает процесс аудита ИСМ.

Рассмотрим далее несколько реальных аудиторских свидетельств (в точной терминологии ISO 19011:2011), касающихся проблемы обеспечения непрерывности бизнеса и позволяющих выполнять «аудиторский след» по основным стандартам (рассмотренным выше).

1. В организации разработан типовой шаблон SLA (он идентифицирован как документ в СУУ), в то же время этот шаблон несколько лет не обновляется, реальные услуги описываются в SLA произвольной формы, нет соответствия по кодам (идентификаторам) услуг, не определен состав и/или метрики услуг. При изучении в процессе аудита ряда

Таблица 2 – Соотношение требований стандартов по ситуациям на аудите

Ситуация на аудите	Требования СУУ	Требования СМИБ	Требования СМНБ	Требования ИСМ
Ситуация 1	4.3.2	4.3.2	7.5.3	7.5
Ситуация 2	8.1	5.2.1	7.3	7.3
Ситуация 3	6.1	4.2.3	4.2.2	4.2

претензий от заказчика выяснилось, что все указанные нарушения SLA, в конечном счете, влияют непосредственно на доступность сервисов для бизнеса организации.

2. В организации несколько действующих SLA не содержат спецификации критичных (значимых) инцидентов, схем/схемы эскалаций и/или коммуникаций, регламента развертывания критичных (значимых) релизов. При изучении в процессе аудита просрочек сроков решения инцидентов, выяснилось, что в каждом случае наблюдались хаотичные действия персонала различных линий поддержки, что, в конечном итоге, влияло непосредственно на доступность сервисов для бизнеса организации.

3. В организации один из SLA не согласован в установленном порядке: договор с клиентом есть, SLA, как часть договора, есть, но реальная отчетность по предоставляемым услугам формируется на основании инструкции (...отработки данных телеметрии...), подготовленной несколько лет назад и подписанной только с одной стороны. При изучении в процессе аудита показателей SLA / CSI выяснилось, что заказчик каждый месяц формировал оценку CSI за нарушения регламентов по инструкции, о которой никто из представителей организации не знал. В конечном итоге, реальные оценки доступности сервиса были существенно занижены – что приводило ежемесячно к финансовым потерям для организации провайдера.

Обобщенное представление нарушений (в терминологии аудита – «несоответствия») требований стандартов для рассмотренных ситуаций аудитов представлено в таблице 2.

Таким образом, в качестве одного из «корневых» методов для решения проблем обеспечения непрерывности бизнеса в ИСМ можно предложить экспертизу (оценку) SLA. Эта оценка (в процессе независимого аудита) является частным случаем анализа контрактных требований СМИБ [2], СМНБ [6] и прямого требования СУУ [4, 5]. Общий вывод – неудовлетворительное (по отношению к бизнесу) соглашение SLA приводит напрямую к неправильному соотношению активов, к непродуманным (нерезультативным) схемам восстановления деятельности (в том числе, схемы эскалации в случае критичных инцидентов), что, в конечном итоге, приводит к серьезным системным рискам для бизнеса.

Управления рисками в процессе обеспечения непрерывности бизнеса

Применительно к ИСМ минимально следующие риски необходимо принять во внимание:

- некорректное определение критичных бизнес-процессов для бизнеса (или выделение слишком большого числа таких процессов, что повышает затраты и снижает экономическую эффективность системы менеджмента);
- некорректное определение активов, подлежащих защите (например, перечня конфигурационных единиц (КЕ), относящихся к конкретному сервису), что необоснованно повышает затраты и время закрытия инцидентов (обращений);

– неосведомленность о ценности нематериальных активов (НМА), например, лицензий на ПО, что значительно увеличивает риски срыва SLA по причине отсутствия необходимых КЭ, их доступности (например, эталонных образов дисков) и подключения необходимых линий поддержки (Oracle, SAP, Microsoft) при необходимости.

Формального исполнения процедур аудита (например, внутреннего аудита ИБ), что может определять либо некомпетентность клиент/сервис менеджеров, либо умысел в оценке финансовых параметров бизнеса;

Непринятие во внимание требований обеспечения непрерывности бизнеса (например, в соответствии с требованиями Федеральных законов: «О связи», «О транспортной безопасности», «Об электронной подписи», «О персональных данных»).

Выводы

Применение предложенных подходов к решению проблем обеспечения непрерывности бизнеса в ИСМ посредством аудита ИБ в соответствии с требованиями международных стандартов позволит:

Сократить финансовые последствия рисков благодаря оптимизации системы внутренних аудитов, администрирования средств обеспечения ИБ и проведения периодической оценки со стороны руководства;

Сформировать универсальный подход к управлению бизнес-рисками и создать «вертикальную» модель рисков ИСМ, адекватную бизнес-процессам в организации;

Сократить число формальных требований благодаря единому унифицированному набору четко документированных и необходимых процессов ИСМ.

Литература:

1. ISO 9001:2008 «Системы менеджмента качества. Требования».
2. ISO/IEC 27001:2005 «Информационная технология. Методы защиты. Системы менеджмента информационной безопасности. Требования».
3. ISO/IEC 27002:2005 «Информационная технология. Методы защиты. Практическое руководство по системам менеджмента информационной безопасности».
4. ISO/IEC 20000-1:2011 «Information technology – Service management – Part 1: Service management system requirements».
5. ISO/IEC 20000-2:2012 «Information technology – Service management – Part 2: Guidance on the application of service management systems».
6. ISO 22301:2012 «Societal security – Business continuity management systems – Requirements».
7. Лившиц И.И. Методы оценки защищенности систем менеджмента информационной безопасности, разработанных в соответствии с требованиями международного стандарта ISO/IEC 27001:2005: Автореф. дис. канд. техн. наук. – Санкт-Петербург, 2012. – 20 с.

КОМПЛЕКСНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ ДЛЯ РЕШЕНИЯ ОПЕРАТИВНЫХ ПРОИЗВОДСТВЕННЫХ ЗАДАЧ В РЕАЛЬНОМ СЕКТОРЕ ЭКОНОМИКИ

**С.П. Калютчик,
Центр защиты информации
Белорусской железной дороги**

Основными аспектами, влияющими на разработку, создание и обеспечение функционирования инфраструктур открытых ключей (ИОК) являются:

- характеристики и особенности производственных процессов (технологических задач), для решения которых создается ИОК;
- нормативно-правовая база, в которой предполагается функционирование ИОК;
- характер взаимодействия со смежными информационными технологиями;
- среда функционирования объектов ИОК, уровень требований по безопасности и пр.

Наиболее характерными особенностями по вышеуказанным позициям среди отраслей реального сектора экономики обладает ИОК железнодорожного транспорта общего пользования.

Рассмотрим особенности организации комплексной системы управления открытыми ключами на примере ИОК Белорусской железной дороги.

В соответствии с Законом Республики Беларусь «О железнодорожном транспорте» от 06.01.1999 № 237-З, Уставом государственного объединения «Белорусская железная дорога» (постановление СМ Республики Беларусь от 10.01.2009 № 19), Белорусская железная дорога монополично оказывает услуги по перевозке грузов и пассажиров железнодорожным транспортом общего пользования на принципах обязательности, при этом являясь предприятием непрерывного функционирования и объектом повышенной опасности. Эти ключевые моменты положены в основу технологических процессов, посредством которых обеспечивается перевозка грузов и пассажиров, и, следовательно, оказывают прямое влияние на характеристики информационно-телекоммуникационных ресурсов, применяемых для интенсификации техпроцессов железнодорожного транспорта.

Таким образом, с точки зрения функциональности ИОК Белорусской железной дороги направлена на:

- организацию применения всех основных возможностей технологии открытых ключей (выработка ЭЦП, создание защищенных цифровых каналов, идентификация и аутентификация);
- обеспечение непрерывного решения производственных задач железнодорожного транспорта с реализацией функционала ИОК в режиме on-line.

Являясь объединением государственных юридических лиц, Белорусская железная дорога в полной мере реализует требования законодательства, регламентирующего техническую и (или) криптографическую защиту информации. В частности, организационно-правовые, технические и технологические принципы построения ИОК Белорусской железной дороги основаны на:

– Законе Республики Беларусь «Об электронном документе и электронной цифровой подписи» от 28.12.2009 № 113-З;

– Указе Президента Республики Беларусь от 01.09.2010 № 450 «О лицензировании отдельных видов деятельности»;

– технических нормативных правовых актах Республики Беларусь, регулирующих процедуры выработки и проверки ЭЦП, шифрования и контроля целостности, форматы сертификатов, списков отозванных сертификатов и т.д.

Реализация требований вышеуказанных актов законодательства потребовала значительных усилий как на этапе создания, так и в процессе функционирования ИОК Белорусской железной дороги. Однако данная позиция для железной дороги является принципиальной, поскольку обеспечивает высокий уровень надежности технологических процессов железнодорожного транспорта, в которых применяется функционал ИОК, а также служит основой разрешения претензионных вопросов, связанных с применением технологий открытых ключей.

Взаимодействие ИОК Белорусской железной дороги со смежными информационными технологиями по характеру, условиям и особенностям можно разделить на три направления:

- взаимодействие с ведомственными информационными системами;
- взаимодействие с информационными системами субъектов правового поля Республики Беларусь;
- взаимодействие с информационными системами иных государств.

Взаимодействие с информационными системами, применяемыми в производственной деятельности железнодорожного транспорта является наиболее объемным и оперативным. Вместе с тем, данное взаимодействие в наибольшей степени поддается регламентации в силу единой организационно-информационной среды и наличия достаточных механизмов внутриведомственного регулирования.

Взаимодействие ИОК Белорусской железной дороги с частными информационными системами субъектов правового поля Республики Беларусь в настоящее время практически не ведется, что является прямым следствием отсутствия единого технического и технологического государственного центра и, соответственно, наличия большого количества не взаимодействующих ведомственных систем управления открытыми ключами. В этой связи, Белорусская железная дорога считает крайне необходимым полноценное функционирование Государственной системы управления открытыми ключами Республики Беларусь (ГосСУОК) с аккредитацией корневых удостоверяющих центров ведомственных ИОК в ГосСУОК.

Взаимодействие ИОК Белорусской железной дороги с информационными системами иных государств представляет собой один из наиболее злободневных и, вместе с тем, наиболее неурегулированных вопросов. В силу геополитического положения, являясь транзитной железной дорогой, расположенной на пересечении двух основных трансъевропейских транспортных коридоров, Белорусская железная дорога крайне тесно взаимосвязана как с железными дорогами сопредельных государств, так и практически со всеми ведущими железнодорожными администрациями евроазиатского региона.

Учитывая общемировые требования интенсификации и оптимизации транспортных услуг, ведущие железнодорожные администрации в качестве одного из основных средств решения данной задачи выбирают перевод международных грузовых железнодорожных перевозок на электронные перевозочные документы посредством WEB-технологий, что, в свою очередь, прямо связано с использованием возможностей технологий открытых ключей. В частности, указанные вопросы являются предметом рассмотрения на уровне Организации сотрудничества железных дорог (ОСЖД), ведущей международной железнодорожной организации, объединяющей железнодорожные администрации и организации 27 стран Европы и Азии.

В этой связи, можно с удовлетворением констатировать, что железнодорожные ведомства Беларуси и России первыми и единственными на евроазиатском полигоне международных железнодорожных перевозок перешли к осуществлению международных железнодорожных перевозок грузов на основе юридически значимых электронных перевозочных документов. Для этого пришлось решить комплекс взаимосвязанных организационных, технических и технологических проблем, среди которых одной из основных являлась проблема проверки ЭЦП, выработанной в ином правовом поле, а, следовательно, проблема взаимодействия ИОК Белорусской железной дороги и ОАО «Российские железные дороги».

Очевидным путем решения задачи взаимодействия ИОК Белорусской железной дороги с ИОК другого государства является реализация ст. 30 Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи», однако, насколько нам известно, механизма практического воплощения этой статьи не существует, в связи с чем, Белорусская железная дорога, по согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь, была вынуждена во взаимодействии с российскими коллегами разрабатывать собственные принципы технического и технологического взаимодействия систем управления открытыми ключами железных дорог, которые в настоящее время успешно функционируют в тестовом режиме при осуществлении грузовых железнодорожных перевозок на основе электронных документов между Белорусской и Октябрьской железными дорогами.

Основными факторами влияния на функционирование ИОК Белорусской железной дороги со стороны среды функционирования являются:

- территориальная распределенность корпоративной информационной системы Белорусской железной дороги;
- наличие в составе информационно-телекоммуникационных ресурсов железнодорожного транспорта критически важных объектов информатизации (КВОИ).

С последним фактором тесно связаны требования по безопасности ИОК железнодорожного транспорта, которые

отличаются в сторону ужесточения по сравнению с требованиями, предъявляемыми к ИОК общего назначения. При решении этой задачи зачастую приходится сталкиваться с необходимостью учета взаимоисключающих факторов.

Например: ИОК Белорусской железной дороги, тесно связанная с решением оперативных транспортных задач для открытого множества потенциальных пользователей (клиентов железнодорожного транспорта) должна обеспечивать непрерывное качественное взаимодействие с сетями передачи данных общего пользования. Вместе с тем применение средств ЭЦП, шифрования, аутентификации и идентификации в информационных задачах управления перевозками, финансовых задачах, в КВОИ влечет требования усиления защищенности и, как следствие, локализации по телекоммуникационным аспектам.

В этой связи, следует отметить, что сдерживающим обстоятельством для окончательной конкретизации норм обеспечения безопасности ИОК Белорусской железной дороги является отсутствие сформированной законодательной базы функционирования КВОИ.

Таким образом, система управления открытыми ключами Белорусской железной дороги является комплексной, мультифункциональной, специализированной, рассчитанной на перспективу развития в составе единой государственной системы во взаимодействии со смежными информационными системами как в составе правового пространства Республики Беларусь, так и вне его.

**Качество и компетентность
в мире печатных плат**

ОАО «Минский часовой завод»

ВАШ НАДЕЖНЫЙ ИЗГОТОВИТЕЛЬ ПЕЧАТНЫХ ПЛАТ

220095, г. Минск,
пр. Независимости, 95,
т./ф. +375 (17) 280-49-55
моб. +375 (29) 750-45-50
bogdashich@mail.ru

Типы плат

- дпп, мпп (до 24 слоев) любого класса точности
- Гибкие печатные платы
- Платы для ВЧ/СВЧ
- Платы на алюминиевой подложке
- Платы для смарт-карт

Возможности

- Проектирование плат
- Технологическая поддержка
- Покрyтия: HASL, иммерсионное золото, иммерсионное олово, ПОС, NI-B
- Формирование контура любой формы
- Материалы: FR-4, Rogers, Duroid, алюминий, лавсан

Качество

- Сертификат соответствия ВУ/112 05.01.0030030

Срок изготовления от 2 дней до двух недель

СОЗДАНИЕ КРУПНОМАСШТАБНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЕДИНОЙ ГОСУДАРСТВЕННОЙ СИСТЕМЫ РЕГИСТРАЦИИ И УЧЕТА ПРАВОНАРУШЕНИЙ

Н.М. Бобович,
Академия МВД Республики Беларусь

Единая государственная система регистрации и учета правонарушений (ЕГСРУП) органов внутренних дел – это совокупность информационных подсистем на базе программных, компьютерных и коммуникационных комплексов, обеспечивающих оперативный обмен сообщениями и данными оперативно-розыскного, справочного и административно-управленческого характера между подразделениями органов внутренних дел.

ЕГСРУП функционирует в интересах всех отраслевых служб ОВД и предоставляет возможность оперативного информационного взаимодействия как в системе ОВД, так и с правоохранительными органами, государственными учреждениями, министерствами и ведомствами Республики Беларусь, а также с правоохранительными органами других государств.

Основой ЕГСРУП ОВД является территориально-распределенная компьютерная сеть, построенная в соответствии с идеологией открытых систем.

Использование идеологии открытых систем для построения ЕГСРУП и системы защиты информации в ней предполагает применение разработанных в эталонной модели взаимодействия открытых систем (ЭМ ВОС) общего описания архитектуры безопасности, служб безопасности информации и соответствующих им механизмов обеспечения безопасности. Для этих целей в эталонной модели используются службы безопасности и механизмы обеспечения безопасности. Реализация каждой службы безопасности осуществляется с помощью набора протоколов, использующих соответствующие механизмы обеспечения безопасности. При этом каждый из протоколов, по существу, представляет собой алгоритм, точное выполнение которого объектами ЕГСРУП гарантирует реализацию соответствующего уровня защиты информации.

Для поддержания заданного уровня защищенности система защиты информации (СЗИ) должна выбрать конкретный протокол. При этом в рамках выбранного протокола имеется возможность изменять уровень защищенности, выполняя, например, для службы идентификации парных логических объектов следующие действия: смена пароля, переход на новые главные ключи абонентов, переход на новый сеансовый ключ, выполнение процедуры двухсторонней идентификации во время сеанса и т.д.

Очевидным недостатком такой архитектуры безопасности является то, что предлагаемые протоколы обладают различной стойкостью против воздействий дестабилизирующих факторов (нарушителя), а их реализация в системе защиты информации требует различных материальных затрат.

Система защиты информации, построенная по принципам ЭМ ВОС, является сложной системой. Поэтому оценка эффективности такой системы является задачей многокритериального оценивания.

Для ее решения возможны следующие два подхода:

- сведение множества частных показателей к некоторому единственному интегральному показателю;
- использование методов теории многокритериального выбора и принятия решений (при наличии значительного числа частных показателей эффективности, имеющих приблизительно одинаковую важность).

Поскольку целью функционирования системы защиты информации является поддержание заданного уровня защищенности ЕГСРУП, то используемые для оценки ее эффективности показатели должны характеризовать динамические свойства системы защиты информации и позволять сравнивать различные структуры системы защиты информации. Наилучшим образом этим требованиям отвечают показатели эффективности вероятностно-временного характера, которые в общем случае имеют смысл функций распределения:

- вероятность преодоления системы защиты информации P_n за время T_n ;
- вероятность доставки единицы информации (например, пакета данных) от абонента к абоненту P_d за время T_d ;
- аппаратная сложность S .

Значения показателей P_n , T_n , P_d и T_d могут быть определены с помощью имитационного моделирования или аналитически.

Показатель аппаратной сложности S может быть определен, например, как количество типовых модулей в системе защиты информации. Однако такой подход к оценке аппаратной сложности применим только при сравнении однотипных структур систем защиты информации.

При анализе структур различных типов, различающихся, например, количеством и распределением механизмов защиты, получение аналитического выражения для показателя S практически невозможно. Это связано со значительным различием типов механизмов защиты информации, с множеством способов их практической реализации и, следовательно, с невозможностью сведения их аппаратной избыточности к общей единице измерения. Поэтому целесообразно в этом случае рассматривать S как качественный показатель, а для его оценки использовать методы теории нечетких множеств. При этом количественные показатели P_n , T_n , P_d и T_d также могут рассматриваться как нечеткие при условии что для них определены максимальные и минимальные допустимые значения.

ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИИ В СФЕРЕ КУЛЬТУРЫ КАК КОМПЛЕКСНАЯ ПРОБЛЕМА

**Д.В. Кондратьев,
АНО «Центр поддержки общественных инициатив и социального партнерства «Экклезия»,
С.Т. Петров, журнал «Цифровое наследие»,
А.А. Тарасов, РГГУ, г. Москва**

Культурное наследие всегда служило важнейшим показателем развития цивилизации, являлось важным материальным активом государства. Перевод объектов культурного наследия в цифровую форму порождает новый социокультурный и технологический феномен – «цифровое наследие», которое не только существенно расширяет возможности по обеспечению целостности и доступности культурного наследия, но и порождает ряд серьезных проблем [1]. Цифровое наследие служит в значительной мере «проводником культуры» внутри страны и за рубежом. По состоянию цифрового наследия судят и об общем уровне развития информационного общества в стране. Обеспечение информационной безопасности в сфере культуры становится одним из основных факторов сохранения и доступа к ценностям культуры, успешного формирования цифровых информационных массивов и соответствующей инфраструктуры.

Вместе с тем, в настоящее время отсутствует должное понимание необходимости и особенностей защиты информации во всей гуманитарной сфере, где доля закрытой информации в общем объеме информационных ресурсов в современном обществе весьма мала. Хотя проблемы целостности и доступности «культурной информации», а по отдельным информационным системам и конфиденциальности требуют самого пристального внимания.

Традиционные системы сохранения культурного наследия основаны, в том числе, на бумажно-компьютерных системах учета, физической охране объектов культуры (здания и сооружения, предметы, документы и пр.), иногда осуществляемой специальными подразделениями МВД, регламентами деятельности в чрезвычайных ситуациях, финансовыми мерами (страхование). При таком подходе объект культуры рассматривается исключительно как материальный предмет, требующий защиты, прежде всего, в силу его высокой стоимости, а также оцениваемый по иным, гораздо менее четким, часто конъюнктурным критериям «общественной ценности». При этом, основными угрозами объекту культуры являются угрозы, связанные с неблагоприятными воздействиями внешней среды, хищением и подменой, акты вандализма. «За скобками» безопасности оказывается информационная природа объектов культуры, их «смыслообразующая» ценность, а также практически все вопросы информационной безопасности формируемых информационных массивов, включая учетные системы, информационная безопасность автоматизированных систем учреждений культуры и их сайтов и пр. Меры информационной безопасности должны обеспечивать защиту

«информационной составляющей» всего жизненного цикла объекта культуры – от создания произведения искусства до бессрочного хранения.

Мировое сообщество осознало важность сохранения цифрового наследия и угрозы, связанные с его утратой. Это нашло отражение в «Хартии по сохранению цифрового наследия», принятой ЮНЕСКО в 2003 г. [2]. К сожалению, понятие «цифровое наследие Российской Федерации» и вопросы обеспечения его безопасности, пока не нашли должного отражения как в научно-практических исследованиях, так и в документах федерального и ведомственного уровня. Основная правовая проблема цифрового наследия определяется тем, что цифровые образы объектов, отнесенных к культурному достоянию народов России, сами не являются объектами такого достояния. Поэтому к ним и к обеспечению их безопасности относятся как к нечто второстепенному, факультативному. Само музейное, библиотечное и архивное сообщество также пока еще не достаточно готово к обсуждению поставленных проблем, особенно в области информационной безопасности.

На наш взгляд, именно «человеческий фактор» является сдерживающим для формирования, освоения и обеспечения безопасности цифрового наследия. Однако, в повестке дня – проектирование и создание «умного музея» [3], в котором интегрированы все информационные подсистемы, а посетители могут вступать в диалог с «умными экспонатами». Освоение и популяризация цифрового наследия начинает постепенно переходить к «одухотворенным аватарам» [4].

Но не меньшие угрозы для культуры могут исходить от «цифровой эйфории», повальной замены и утраты проверенных временем аналоговых носителей и технологий. Это связано как с тем, что многие вопросы миграции цифровых данных все еще остаются открытыми, так и с малой изученностью ограничений аналого-цифровых и цифро-аналоговых преобразований.

Именно в сфере культуры формируется значительная часть потребностей, а также технических требований, связанных с оцифровкой информации (документы, книги, произведения искусства), ее бессрочным хранением в неизменном виде, а также конфиденциальности информации, связанной как с обеспечением авторских прав, так и непосредственно с безопасностью функционирования учреждений культуры.

Достижение весьма высоких контрольных значений показателей развития информационного общества на период до 2015 года, определенные в «Стратегии развития информационного общества в Российской Федерации» [5]

и соответствующих показателей Государственной программы «Информационное общество (2011-2020 годы)» требуют самых серьезных усилий со стороны десятков тысяч учреждений культуры, федеральных и муниципальных органов исполнительной власти, гражданского общества. Уже созданные и создаваемые в рамках программы «Информационное общество», иных программ и проектов гигантские информационные ресурсы и информационная инфраструктура требуют адекватных мер по обеспечению информационной безопасности в целях обеспечения сохранности и доступности формируемого цифрового наследия России.

Среди первоочередных задач, решаемых в области информационной безопасности в сфере культуры можно выделить следующие:

- разработка концептуальных документов в области информационной безопасности культуры и ее нормативно-правовой базы;
- обеспечение безопасности цифрового наследия Российской Федерации, включая целостность и безопасность создаваемой инфраструктуры;
- обеспечение доступности цифрового наследия;
- обеспечение конфиденциальности информации, связанной с авторским правом, а также в области безопасности самих объектов культуры.

Направление информационной безопасности культуры задается в «Доктрине информационной безопасности Российской Федерации» следующей формулировкой: «Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства» [6]. Среди видов угроз в Доктрине упоминается «дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы». На этой основе можно попытаться построить концептуальные документы по обеспечению информационной безопасности в сфере культуры.

Для восприятия культуры, одним из важнейших является целостность отдельных собраний и культурного наследия как единой системы. Угроза утраты целостности объектов культуры связана, в том числе, с реформированием собраний архивов, музеев, библиотек. Одним из наиболее известных примеров может служить преобразование Румянцевского музея в Государственную библиотеку им. В.И. Ленина. В результате, коллекции Румянцевского музея оказались в сотнях учреждений бывшего СССР или были частично утрачены. Виртуальная реконструкция утраченных и реформированных собраний является важным и, по сути, единственным способом воссоздания их целостности.

Целостность культурного наследия пока относится к интуитивным понятиям. Цифровое наследие России плохо

систематизировано и разрознено. Отчасти, это объясняется и архаичностью систем государственного учета культурных ценностей. Пока о целостности цифрового наследия приходится говорить только в порядке постановки задачи. Одним из способов решения проблемы целостности цифрового наследия России, могло бы стать создание распределенного (резервируемого) катастрофоустойчивого хранилища с единой системой управления. Пока даже отдельные учреждения культуры национального уровня не всегда могут обеспечить целостность своих цифровых собраний. Однако трудности создания единого информационного хранилища связано в значительной мере с низким уровнем доверия учреждений культуры к любому из возможных операторов данного хранилища. Вместе с тем, в настоящее время подавляющее количество информационных ресурсов учреждений культуры хранится в единственном экземпляре в самих объектах культуры и их сохранность не регламентируется никакими ведомственными или внутренними документами. Таким образом, в случае чрезвычайных ситуаций под угрозой одновременно оказываются как сами предметы хранения, так и их цифровые образы.

Обеспечение доступности объектов культуры является одним из основных смыслов и целей деятельности культуры. Практика фактического сокрытия предметов культуры в запасниках или спецхранах оказала негативное влияние на культуру России и страну в целом. Доступ к создаваемым цифровым образам объектов культуры в настоящее время зачастую неправомерно ограничивается с помощью организационных и/или технических средств. Это ведет к искусственному сужению культурного пространства России, наносит вред ее международному престижу. Обеспечение доступности цифровых образов объектов культуры и их описаний является составляющей частью комплексной защиты информации в сфере культуры.

Доступность цифрового наследия зачастую носит формальный характер и ограничивается отдельными учреждениями культуры размещением на своих сайтах цифровых изображений недостаточного качества, введением ограничений на скорость доступа и количество скачиваний, процедурами выборки информации из баз данных и т.д. Попытки создания общероссийских порталов в области культурного наследия, истории, туризма оборачиваются весьма большими затратами и не приносят пока должного эффекта с точки зрения интеграции информации и посещаемости.

Неправомерные ограничения в доступе к цифровому наследию связаны и с деятельностью зарубежных компаний, обеспечивающих оцифровку наших культурных ценностей, а затем берущих под финансовый и иной контроль распространение данной информации (например, архив Коминтерна или книжное наследие старообрядцев). С другой стороны, правомерно ограниченная информация (мы не говорим о целесообразности), например, из библиотеки диссертаций РГБ, непрерывно «утекает» в коммерческие структуры.

Проблемы и перспективы межгосударственного информационного сотрудничества в сфере культуры связаны, в том числе, с развитием системы контроля за перемещением культурных ценностей, а также созданием целостных виртуальных собраний, объектов, относящихся к одной национальной культуре, но находящихся под разной государственной юрисдикцией.

Передовые, флагманские учреждения культуры развитых стран не боятся брать на себя инициативы в цифровой сфере, казалось бы, не имеющие прямого отношения к их традиционной деятельности. Так, Библиотека Конгресса США стала учреждением, обеспечивающим хранение архива сообщений Twitter. Сам Twitter начал предоставлять услуги по возможности генерации сообщений после смерти владельца аккаунта (аналог «одухотворенного аватара»). Таким образом, государственная библиотека выступает гарантом целостности и доступности огромного массива частных сообщений, а Интернет-компания, по сути, расширяет и модифицирует социокультурное поле памяти.

В России отсутствует система головных учреждений культуры, способных наряду с функциями хранения и собирания, выполнять общеотраслевые задачи системного проектирования, анализа и прогнозирования, как это осуществляется, например, в ЦНИИ Машиностроения Роскосмоса (который, кстати, является и хранилищем общеотраслевого архива, а также собирается организовать музей всего военно-промышленного комплекса). Нет также организации, комплексно решающей задачи, связанные с обеспечением информационной безопасности сферы отечественной культуры.

В тех случаях, когда государство не может эффективно решать проблемы доступа к цифровой информации (например, в силу причин, связанных с авторским правом), эти проблемы решают сообщества частных лиц и сетевые структуры. Так, русскоязычный сервис rutracker.org обеспечивает доступ многих миллионов пользователей к более чем миллиону единиц хранения, общим объемом около 2 петабайт. Это в разы превышает объемы оцифрованной

информации всех российских учреждений культуры вместе взятых. При этом, качество собственных оцифровок, осуществляемых по определенным регламентам, как правило, выше, чем в большинстве государственных учреждениях культуры, а сохранность и доступность обеспечивается самой организацией пиринговой сети. Тем самым, при формировании цифрового наследия следует учитывать интересы и возможности гражданского общества, в том числе и в вопросах информационной безопасности.

Итак, информационная безопасность сферы культуры является проблемой, на которую пока не обращали должного внимания, но без ее решения невозможно обеспечить сохранение и доступность культурного наследия, как в традиционной, так и цифровой форме.

Литература:

1. Наши задачи в переходный период от аналогового к цифровому наследию // Цифровое наследие. – 2009, № 1, С. 23–25.
2. Хартия о сохранении цифрового наследия [Электронный ресурс]: – Режим доступа: http://www.ifapcom.ru/files/Documents/digital_heritage_preserv.pdf
3. Ненашев А.Н. Музей в измерении 5 D // Музей. – 2013. – № 5, С. 5–12.
4. Расторгуев С.П., Литвиненко М.В. Аватаризация – Санкт-Петербург: 2011. – 310 с.
5. Стратегия развития информационного общества в Российской Федерации [Электронный ресурс]: – Режим доступа: <http://www.scrf.gov.ru/documents/6/90.html>. – М., 2008.
6. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: <http://www.scrf.gov.ru/documents/6/5.html> – М., 2003.

МОДЕРНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ПО СПЕЦИАЛЬНОСТИ «ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ» В УСЛОВИЯХ ПЕРЕХОДА НА ЧЕТЫРЕХЛЕТНЕЕ ОБУЧЕНИЕ

М.П. Батура, Л.М. Лыньков, Т.В. Борботько,
БГУИР, г. Минск

Специальность «Защита информации в телекоммуникациях» в Белорусском государственном университете информатики и радиоэлектроники (БГУИР) была открыта в 2004 г. Особенностью подготовки специалистов по указанной специальности является то, что обучение реализуется по двум направлениям: первое – проектирование и эксплуатация телекоммуникационных систем и сетей, и второе – создание и сопровождение систем защиты информации. В соответствии с чем, молодому специалисту присваиваются следующие квалификации: «специалист по защите информации», «инженер по телекоммуникациям».

Образовательный стандарт специальности «Защита информации в телекоммуникациях», рассчитанный на пятилетнее обучение специалистов, включал в себя три цикла: социально-гуманитарных, естественно-научных и общепрофессиональных, и специальных дисциплин. В цикле специальных дисциплин внимание уделялось обучению

студентов по следующим направлениям защиты информации: нормативно-правовое обеспечение информационной безопасности, инженерно-техническая защита объектов от несанкционированного доступа, защита информации от утечки по техническим каналам, криптографическая защита информации, обеспечение безопасности информационных систем и особенности использования систем и средств защиты информации в телекоммуникациях и банковской сфере.

С учетом развития современных средств информационного обмена и специфики применения информационных систем в жизни общества одним из актуальных направлений обеспечения информационной безопасности является защита персональных данных и другой информации, относящейся к категории ограниченного распространения. Ее обработка и хранение реализуются с помощью информационных систем, состоящих из банков данных, где обеспечивается хранение сведений, аппаратно-программных комплексов и

информационной технологии, позволяющих получать доступ к данным и выполнять их обработку. Взаимодействие между компонентами таких систем реализуется посредством телекоммуникационных систем, которые так же используются злоумышленниками для несанкционированного доступа к таким ресурсам, включая методы социальной инженерии.

Во внедряемой с 2013 года новой системе получения высшего образования по схеме 4+2 на первой ступени, в новом стандарте специальности «Защита информации в телекоммуникациях», цикл специальных дисциплин дополнен новыми предметами: «Защита операционных систем и

программного обеспечения» и «Социально-психологические аспекты информационной безопасности», которые с учетом ранее введенных дисциплин позволяют дать студенту знания по основам обеспечения защиты информации в информационных системах с учетом современного уровня угроз информационной безопасности.

На первой ступени высшего образования молодой специалист может продолжить обучение в магистратуре по специальности «Методы и системы защиты информации, информационная безопасность» для получения углубленных знаний по информационной безопасности.

О СИСТЕМЕ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Е.А. Свирский,
БГУ, г. Минск**

За последние три десятилетия информация приобрела статус одного из важнейших ресурсов, определяющих политический, экономический, научно-технический и оборонительный потенциал стран. Процессы информатизации наполнили все сферы жизни общества новыми качествами, придали им оперативность, гибкость и динамичность. Проблемы информационного обеспечения всех сфер деятельности по своей значимости и актуальности стали выходить на первое место любого общества, опережая остальные процессы, которые, еще недавно, считались одними из главных. Информационные технологии в настоящее время насквозь пронизывают всю жизнь общества, они являются определяющими условиями эффективной деятельности людей и всеобщего прогресса.

В то же время, процессы информатизации общества, которые активно протекают все это время, породили новую глобальную социотехнологическую проблему – проблему информационной безопасности человека и общества. Суть этой проблемы состоит в том, что информационная сфера в значительной мере определяет многие важнейшие интересы человека, общества, государства, да и всей мировой цивилизации. Поэтому деструктивные воздействия на информационную сферу со стороны внешних или же внутренних источников, независимо целенаправленные они или непреднамеренные, представляют собой угрозы для безопасности человека и общества. Мировая экономика ежегодно несет убытки от воздействий на информационную сферу, исчисляемые сотнями миллиардов долларов.

Глобальная сеть Интернет стала не только популярным средством обмена информацией, но и инструментом несанкционированного доступа к государственным секретам и деньгам, хранимым в банках. В последнее время число подобных случаев во всем мире быстро растет. Степень защиты информации во многом зависит от уровня квалификации специалистов, обеспечивающих защиту информации, а также от общей культуры владения продуктами информационных технологий и осведомленности в вопросах информационной безопасности всех пользователей информационных технологий.

Основные проблемы, связанные с обеспечением защиты информационных ресурсов, являются следствием недостаточной компетентности сотрудников (руководителей, исполнителей, пользователей) в вопросах обеспечения информационной безопасности. По данным западных исследований, порядка 80-90% нарушений информационной безопасности компаний связано с деятельностью собственных сотрудников. Причем, более 80% инцидентов, в которых виновны сотрудники, происходят в результате неумышленных действий. Причины неумышленных действий – это и невнимательность сотрудников к правилам и требованиям обеспечения информационной безопасности, и нежелание выполнять требования запретительно-ограничительного характера, а иногда и просто незнание сотрудниками этих правил и требований. В итоге, перед специалистами, отвечающими за информационную безопасность, возникает понятная, но довольно непростая задача: как добиться того, чтобы сотрудники более внимательно относились к защите информационных ресурсов, выполняли необходимые правила, и требования, не вызывая у них при этом негативного отношения.

Очевидно, что одним из решений данной задачи является создание системы непрерывного повышения осведомленности общества в области информационной безопасности. Эта система, в силу всеобъемлющей роли информации в жизни общества, должна охватывать все слои общества. Непрерывность связана с необходимостью информировать общество о проблемах информационной безопасности в силу постоянного обновления знаний и, естественно, технологий, которые могут, как сами иметь уязвимости, так и выявлять и использовать уязвимости в продуктах информационных технологий, появившихся на рынке значительно раньше.

Проблема повышения осведомленности в области информационной безопасности – это не только забота руководства конкретных компаний, организаций и учреждений. Сегодня это уже проблема государственного уровня, например, обеспечение информационной безопасности критически важных объектов. Все более массовое внедрение информационных технологий в государственное управление и управление экономической жизнью страны требует огромных финансовых затрат и недопустимо, чтобы здесь государство несло убытки.

Решение проблемы повышения осведомленности в области информационной безопасности необходимо решать, например, как проблему электрической безопасности практически на подсознательном уровне, что можно делать, а что нельзя, потому что это может привести к катастрофическим последствиям.

В основу должна быть положена постоянная профилактическая работа со всем населением страны. Работу по формированию мировоззрения по проблемам информационной безопасности надо начинать со школы с начальных классов, когда у учеников появляются мобильные телефоны и компьютеры. Профилактическая работа с учащимися средних школ, системы профессионально-технического, среднего специального и высшего образования должна вестись постоянно, а не по принципу месячников. Очевидно, чтобы проводимая работа по повышению осведомленности в области информационной безопасности была эффективной, Министерство образования должно разработать циклы лекций для учащихся начальных, средних и выпускных классов по информационной безопасности. В данном случае, очевидно, необходимо начинать с обсуждения рисков попасться на мошенничество и, как следствие, причинить материальный ущерб семье при пользовании мобильными устройствами и компьютерами в информационно-коммуникационных сетях в начальных классах и заканчивать уголовной ответственностью при противоправном использовании мобильных устройств и компьютерной техники в старших классах.

В состав коллективов по разработке материалов циклов лекций должны входить педагоги, специалисты по информа-

ционным технологиям, юристы и психологи. Лекции необходимо строить не по запретительному принципу, а учитывая возрастную психологию учеников подводить их к самостоятельному осознанию выполнения определенных требований и ограничений при работе, прежде всего, с мобильными информационными системами. Основная цель, учитывая подростковую протестную реакцию на обязательность выполнения действий запретительно-ограничительного характера, не назойливо сформировать и закрепить систему знаний в области информационной безопасности, сформировать информационно-правовую культуру обращения с продуктами информационных технологий.

В организациях и учреждениях должны разрабатываться собственные программы внутренней осведомленности персонала. Эти программы могут быть привязаны к должностным обязанностям сотрудников. Специалисты же по защите информации обязаны проходить курсы повышения квалификации с достаточно частой периодичностью и, возможно, курсы переподготовки кадров с более длительной периодичностью, например, один раз в 10-15 лет.

При организации системы повышения осведомленности общества в сфере информационной безопасности необходимо перенимать опыт зарубежных стран, где эти процессы зарекомендовали себя с положительной стороны. Так, по примеру некоторых высокоразвитых стран, необходимо создать сайт, целями которого будут являться информирование об угрозах информационной безопасности и повышение осведомленности в вопросах обеспечения информационной безопасности, как простых людей, так и технических специалистов.

О ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ АЭС

Э.П. Крюкова,

Государственное предприятие «НИИ ТЗИ», г. Минск

Опыт эксплуатации АЭС в условиях перехода на новые, компьютерные технологии показывает, что недостатки в управлении безопасностью и многочисленные ошибки человека могут привести к событиям с существенной значимостью для безопасности. Основные недостатки в действиях человека и управлении безопасностью можно описать через следующие события:

- недостаточное взаимодействие и усиление роли и обязанностей;
- отсутствие адекватной жесткой верификации;
- недостаточный анализ изменяющихся условий для тестирования;
- недостатки в планировании работ и управлении человеческими ресурсами;
- самоуспокоенность и самонадеянность в процессах верификации на всех стадиях подготовки и исполнения;
- недостаточная технологическая подготовка, недостатки в предпусковом инструктаже и оценке после проведения операции;
- многочисленные нарушения рабочих инструкций и процедур;

– недостатки в проектах и эксплуатационной документации.

Главным компонентом в событиях, связанных с нарушением безопасности (47 %), является человеческая ошибка (эксплуатация, обслуживание, обеспечение качества). При отключении реактора, заправляемого топливом, ошибка человека оказывает главное влияние (автоматизация в меньшей степени). 28 % событий вызваны организационными факторами и планированием, такими как неадекватные процедуры, обучение, управление и т.д., и только 5 % событий непосредственно приписываются отказу компонента/оборудования [1].

Многочисленные исследования и отчеты идентифицировали человеческую ошибку как причину номер один нарушений правил безопасности. Оценки влияния ошибок человека, связанных с нарушением правил безопасности, достигают величины 63–80 % [2]. Как только произошел отказ и началось восстановление КС, ошибка человека может сыграть разрушительную роль при восстановлении данных. Отмечается, что 30% всей потери данных – результат человеческой ошибки, и только 15 % – от злоумышленного

воздействия (компьютерное вирусное повреждение – 6 % плюс кража с использованием компьютера – 9 %) [3]. Эти ошибки могут быть активными ошибками, которые происходят в ходе процесса восстановления, или скрытыми ошибками, которые следуют из предыдущего процесса архивирования или резервирования.

Результаты анализа безопасности, проводимого на Украине и в Российской Федерации, идентифицировали ошибки операторов, как максимальный вклад в нарушение безопасности АЭС. Основное средство сокращения вероятности ошибок состоит в обучении полной области действий на специализированных имитаторах.

Наиболее существенные корректирующие действия по повышению безопасности АЭС предлагаются для улучшения соотношения ролей и обязанностей, а также для повышения внимания работающих и руководства к основным правилам эксплуатации и безопасности в ходе работ по обслуживанию. Дальнейшие корректирующие действия включают модификацию проекта и эксплуатационной документации, особое значение придается использованию автономных инструментальных средств и усовершенствование передачи данных в технологических процессах, а также улучшению качества контроля процессов. В последние годы, из-за изменений в деловой среде, управление и организационный фактор становятся более важными, оказывая влияние на эффективность работы отдельного человека. Изменения в управлении в организации могут оказать существенное влияние на ядерную безопасность.

В связи с вышесказанным, особую актуальность получает проблема подготовки кадров для атомной энергетики. Эта система базируется на принципах допуска к самостоятельной работе по управлению атомной станцией (управленческий и инженерный персонал), к эксплуатации и ремонту оборудования (оперативный и ремонтный персонал) только подготовленного и аттестованного персонала.

Для работы на ключевых должностях Белорусской АЭС планируется привлечь около 70 зарубежных специалистов, обладающих опытом работы на АЭС. В соответствии с генеральным контрактом на строительство АЭС в Беларуси подготовка эксплуатационного персонала АЭС будет осуществляться российской стороной и проводиться как в Беларуси, так и на строящихся и действующих АЭС в России [4].

Предполагается, что состав персонала для белорусской АЭС будет назначаться, исходя из структуры, установленной нормативными документами России [5].

К персоналу, обеспечивающему нормальную эксплуатацию оборудования, систем и сооружений АЭС, относятся [6]:

- работники по обеспечению ядерной безопасности, радиационной безопасности пожарной безопасности, общей техники безопасности, всех вспомогательных технических услуг, нормальной работы систем теплоснабжения и подземных коммуникаций, нормальной работы систем вентиляции и кондиционирования, азотом, кислородом, гелием, сухим и влажным воздухом различных давлений;

- работники технической инспекции, по анализу надежности работы оборудования АЭС, режима и охраны, по подготовке кадров, по обращению с топливом и его хранению, по обращению с твердыми, жидкими и газообразными отходами, осуществляющие химический и радиохимический контроль, осуществляющие наблюдение за гидротехническими и другими сооружениями, а также зданиями, осуществляющие

наладку и испытания оборудования атомной станции, по проведению периодической дезактивации оборудования и производственных помещений атомной станции, осуществляющие ведомственную поверку средств измерений.

Единый квалификационный справочник (ЕКС) должностей руководителей, специалистов и служащих России в общем виде описывает обязанности персонала АЭС, полномочия которого касаются использования средств автоматизации [7]. В соответствии с ЕКС к персоналу, связанному с эксплуатацией компьютерных систем АЭС, можно отнести:

- начальника отдела автоматизированных систем управления;

- начальника самостоятельного научно-технического отдела (бюро, группы) по комплексной защите информации технологическими процессами;

- начальника ЭВМ;

- руководителя аналитической группы подразделения по комплексной защите информации;

- руководителя группы подразделения по комплексной защите информации;

- администратора баз данных;

- администратора вычислительной сети;

- администратора информационной безопасности вычислительной сети;

- инженера-конструктора-системотехника;

- инженера-конструктора-схемотехника;

- инженера по автоматизированным системам управления технологическими процессами;

- инженера по инженерно-техническим средствам физической защиты:

- инженера-системного программиста;

- инженера электросвязи;

- прибориста цеха;

- техника по автоматизированным системам управления технологическими процессами (техник-конструктор-системотехник).

Анализ содержания их должностных обязанностей показывает, что они, во многом, перекрываются, что не позволяет четко разграничить ответственность каждого за компьютерную безопасность АЭС в соответствии с рекомендациями МАГАТЭ.

Новое направление в обеспечении безопасности АЭС, связанное с противодействием кибернетическими угрозам, требует новых подходов к подготовке персонала, ответственного за функционирование компьютерных систем контроля и управления, относящихся к безопасности АЭС, и четкому распределению его обязанностей в этой области. Это направление уже нашло отражение в серии руководств МАГАТЭ по безопасности АЭС. В развитие этих руководств разрабатываются соответствующие стандарты МЭК, основное внимание которых акцентируется на проблеме обеспечения качества устройств, систем и компонентов АЭС, важных для безопасности, на всех стадиях их жизненного цикла: начиная с концепции, далее проектирование, изготовление, эксплуатация и вывод из нее. В настоящее время эти стандарты вводятся в Республике Беларусь.

Программа проверки качества АЭС должна включать формальные процедуры и правила определения требований к квалификации исполнителя любого задания, которое может потенциально повлиять на качество работы или

безопасность оборудования АЭС. Эти требования включают необходимые знания, полученные через образование, программы начального и непрерывного обучения, и записи о квалификации.

Ключевым пунктом программы обеспечения качества функционирования АЭС является компетентность персонала, работающего по контрактам, которая должна быть оценена через проверку существующей или запрашиваемой документации и отчетов, таких как: сертификаты, дипломы, отчеты о работе, краткие биографии, результаты оценок, отчеты об аналогичных работах, выполненных на другой АЭС и т.д.

Принципы подтверждения компетентности персонала критически важных компьютерных систем, работающего по контрактам, исходят из общей политики обеспечения качества и безопасности АЭС и из нормативных требований. Основным принципом обеспечения компетентности персонала – специалисты должны быть соответствующим образом оценены прежде, чем выполнить работу. Соответственно, компетентность персонала, работающего по контракту, должна быть формально оценена и зарегистрирована. Конечная ответственность за обеспечение качества всех работ, выполняемых на АЭС остается за эксплуатирующей организацией АЭС.

Оценка формальной квалификации персонала должна выполняться для гарантии, что любой конкретный работающий имеет необходимые способности выполнять свои задачи. В связи с этим, эксплуатирующей организацией должны быть разработаны необходимые процедуры по обеспечению качества или руководства, устанавливающие надлежащие профили специалистов, соответствующие потребностям АЭС.

В настоящее время персонал щитов управления АЭС фактически во всех странах с первых шагов проходит обучение на имитаторах щитов и продолжает обучение, причем более 90 % обучаются на специальных имитаторах оборудования. Для новых предприятий доступен специальный имитатор щита, моделирующий всю область управления реактором, даже на шаге ввода АЭС в действие. В работу щенда при обучении включаются и операции вне щита управления (например, дистанционные пульты отключения, аварийные дизельные генераторы).

МАГАТЭ рекомендует следующий список сценариев, выполняемых на имитаторе (для реакторов типа PWR, BWR) [8]:

1. Запуски оборудования или реактора, включающие диапазон, при котором заметна обратная связь реактивности от повышения температуры ядерного источника и установлена степень нагрева.
2. Отключение оборудования.
3. Ручное управление паровыми генераторами или подачей воды или и то и другое во время запуска, и во время остановки.
4. Борирование или ослабление раствора во время механизированной операции.
5. Существенные (свыше 10 %) изменения мощности при ручном управлении стержнем или потоком рециркуляции.
6. Изменение мощности реактора на 10 процентов или выше.
7. Потеря хладагента, включая:
 - существенные утечки из PWR парогенератора;
 - внутренний и внешний первичный объем;

– большой или маленький, включая определение степени утечки;

– реагирование насыщенного реактора на хладагент (PWR).

8. Потеря вентиляции приборов (при моделировании специфики установки).

9. Потеря электроэнергии (или ухудшение характеристик источника энергии).

10. Потеря потока хладагента/ естественной циркуляции в активной зоне реактора.

11. Потеря подачи воды (в нормальном или аварийном режиме).

12. Потеря технической воды, если требуется для безопасности.

13. Потеря хладагента для отвода тепла ядерного распада.

14. Потеря компонента системы охлаждения или хладагента для отдельного компонента.

15. Потеря нормальной подачи воды или отказа системы нормальной подачи воды.

16. Потеря вакуума конденсатора.

17. Потеря канала системы защиты.

18. Ошибочная настройка управляющего стержня или стержней (или сжигания стержней).

19. Невозможность ввести в действие управляющий стержень.

20. Условия, требующие использования аварийного борирования или резервной системы контроля жидкости.

21. Разрушение топливной оболочки, вызывающее высокую активность хладагента или отходящих газов реактора.

22. Отключение турбины или генератора.

23. Нарушение функций системы автоматического управления, который влияет на реактивность.

24. Нарушение функций системы контроля давления/ объема хладагента для реактора.

25. Отключение реактора.

26. Разрыв основного паропровода (внутренней или внешней защитной оболочки).

27. Отказы приборов (например, приборов реактора).

28. Ожидаемый переходный процесс с отказом для быстрого отключения реактора (ATWS).

29. Множественные отказы системы безопасности.

30. Отказы сигнализатора во время и нормального, и аварийного процессов изменения.

За всеми этими сценариями стоят не только недостатки в проекте АЭС, но и нарушение функционирования компьютерных систем контроля и управления, относящихся к безопасности, и ошибки персонала, от которого требуется обеспечение надежной работы этих систем или действия по управлению вручную при их отказах, если это допустимо по условиям эксплуатации. Последнее требует особо четкого знания инструкций и грамотных реакций человека на нестандартные ситуации, что следует учитывать как положительное влияние действий человека на обеспечение безопасности АЭС. Будучи звеном компьютерной системы, оператор может стать преградой, предотвращающей отказ системы или ее компрометацию, что еще раз говорит о необходимости обеспечения его подготовленности и наличия практического опыта для работы с такими системами.

Ежегодно четыре белорусских вуза – БГУ, БНТУ, БГУИР и Международный государственный экологический универ-

ситет имени А.Д. Сахарова – будут готовить около 220 специалистов в области ядерной энергетики – по управлению АЭС (управление и инженерный персонал), эксплуатации и ремонту оборудования (оперативные и ремонтные рабочие). Министерство образования планирует обеспечить системный подход к подготовке персонала. Министерство основывается на документах Международного агентства по атомной энергии (МАГАТЭ) и лучшей международной практике. В стране будет налажена непрерывная и гибкая система подготовки сотрудников в соответствии с этапами строительства АЭС, пуска АЭС в эксплуатацию и дальнейшей эксплуатации. Схема подготовки кадров – профотбор, базовая подготовка (5-5,5 года) в отечественных вузах, специальная подготовка (0,5-3 года) за рубежом. Планируется также создать учебно-тренировочный центр АЭС [9]. При подготовке кадров должны учитываться требования МАГАТЭ к персоналу АЭС, а также использование национального и мирового опыта подготовки персонала для критически важных приложений.

Опыт решения задач обеспечения безопасности в области атомной энергетики целесообразно распространить на компьютерные системы управления другими критически важными инфраструктурами.

Литература:

1. Nuclear Power Plant operating experience from the IAEA/NEA international reporting system for operating experience

2005–2008/IAEA6. – VIENNA, 2010.

2. IAEA-TECDOC-1411. Use of control room simulators for training of nuclear power plant personnel – 2004.

3. Certification magazine:online: Study Shows Human Error Behind Most IT Security Breaches». – 2004 (Исследование показывает ошибку человека в основе большинства брешей в ИТ безопасности).

4. http://www.belta.by/ru/all_news/economics/Beloruskiju-AES-budut-sovmestno-obsluzhivat-beloruskie-i-inostrannye-spetsialisty_i_628412.html.

5. Министерство здравоохранения и социального развития российской федерации. Приказ от 3 октября 2005 г. № 614 «Об утверждении тарифно-квалификационных характеристик профессий рабочих атомных электростанций.

6. Основные положения по подбору, подготовке, допуску к работе и контролю в процессе эксплуатации персонала атомных станций (ОПКП АЭС -90). – Москва, 2000.

7. Приложение к Приказу Министерства здравоохранения и социального развития Российской Федерации от 10 декабря 2009 г. N 977. Единый квалификационный справочник должностей руководителей, специалистов и служащих. Раздел «Квалификационные характеристики должностей работников организаций атомной энергетики».

8. IAEA-TECDOC-1411. Use of control room simulators for training of nuclear power plant personnel 2004

9. <http://www.nestor.minsk.by/sn/2008/35/sn83504.html>.

НОВОСТИ от «Вектор технологий»

СЕРВОПРИВОДЫ

Технологии не стоят на месте и для повышения производительности труда и улучшения его качества требуются новые, максимально эффективные решения для автоматизации технологического оборудования.

Яркий пример современного высокотехнологичного устройства для автоматизации – сервоприводы. Они представляют собой системы привода, которые способны гарантировать высокоточные процессы движения и реализовать их хорошую повторяемость в самом широком диапазоне регулирования скорости. По сути, любой современный сервопривод – это высокотехнологичная ступень электропривода.

Для чего нужны сервоприводы?

Сегодня тенденция к активному внедрению данных устройств объясняется высокими требованиями к производительности технологического оборудования и улучшению качества продукции на выходе. Использование сервоприводов позволяет реализовать высокочастотное регулирование скорости крутящего момента и вращения вала, а также произвести точное позиционирование с максимально высокой повторяемостью подвижных элементов оборудования.

Сервоприводы незаменимы в самых различных отраслях промышленности, ведь они позволяют выполнять широчайший спектр операций, таких, как высокоточное перемещение частей и деталей на линиях сборки, перемещение роботов и манипуляторов, упаковка и многое другое.

Сервоприводы серии Sigma 5

Ни один специалист не откажется от сервопривода, который не нуждается в сложной настройке. Именно такой и является новинка от корпорации Yaskawa – компактный высококачественный сервопривод Sigma 5.

Это оборудование имеет удобное и интуитивно понятное в использовании программное обеспечение, что позволило сократить время на его ввод в эксплуатацию, а также максимально увеличить эффект от его использования.

Семейство сервоприводов этой серии отличается целым рядом весомых преимуществ, основными из которых являются:

- возможность получать доступ к приводам через одно соединение;
- наличие встроенной шины позиционного управления;
- практически полное отсутствие задержек;
- сокращение механических вибраций;
- высокое качество и надежность;
- быстрое позиционирование;
- простота в эксплуатации;
- плавное управление;
- высокая точность;
- эргономичность.

У Вас высокие требования к сервоприводам? Sigma 5 даст Вам все и даже больше того, что можно ожидать от подобного оборудования!

Vec-tech.by

ЗАКРЫТИЕ КОНФЕРЕНЦИИ

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО АССОЦИАЦИИ ЗАЩИТЫ
ИНФОРМАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Н. Зубков,
«Авангард ПРО»

В последние годы МОО «АЗИ» придает важное значение направлению, связанному с международным сотрудничеством в области ИБ. В основе этого лежат следующие факторы.

Во-первых, современный этап развития ИТ характеризуется постоянным ростом угроз безопасности их использования. При этом киберпреступность давно уже приобрела международный трансграничный характер. В этой связи и противодействие этим опасностям тоже должно осуществляться на международной основе.

С другой стороны, в настоящее время наиболее успешно развивающийся крупный бизнес во многом связан на взаимодействии бизнес-структур разных стран. В этом случае использование ИТ субъектами бизнеса происходит в различных нормативных полях, что требует обсуждения и согласования порядка трансграничного обмена деловой информацией.

Можно выделить 3 уровня международного сотрудничества в области ИБ. Первый, высший уровень – это взаимодействие на уровне государственных структур. Здесь Россия занимает одну из лидирующих позиций, являясь инициатором обсуждения вопросов ИБ на международных форумах государств. Результатом, в частности, стало включение вопросов ИБ, как важной области информационного сотрудничества, в ряд резолюций ООН.

В качестве нижнего уровня международного сотрудничества в области ИБ мы рассматриваем взаимодействие на уровне B2B, что в настоящее время активно востребовано, в частности, в ТЭК и банковском секторе.

На примере МОО «АЗИ», я хотел бы остановиться на некотором среднем уровне взаимодействия, который условно можно отнести к уровню «народной дипломатии».

Остановлюсь на некоторых примерах.

Первый пример. Наша ассоциация с самого начала активно участвует в организации и проведении международных конференций, которые ежегодно проводятся в Гармиш-Партенкирхене (Германия). На данной конференции одной из главных составляющих является обсуждение вопросов противодействия кибертерроризму и обеспечения безопасности использования интернета. На этой конференции присутствуют специалисты и эксперты таких стран как Австрия, Германия, США, КНР, Россия и др.

Важно отметить, что ряд участников, являясь госслужащими, не имеют полномочий выражать официальную точку зрения государства, а выражают «личную» точку зрения. И происходит обмен «личными» позициями, которые в дальнейшем учитываются на более высоких уровнях. Это и есть один из примеров «народной дипломатии».

Традиционно, Ассоциации поручается ведение в рамках Форума совместно с представителями США (что важно!) Круглого стола по частно-государственному партнерству в сфере противодействия кибертерроризму.

В качестве другого положительного примера я хотел бы привести результаты работы Ассоциации по выводу Российских достижений в области разработки и применения РК1-технологий на международный уровень. В частности, в 2011 году на Десятой сессии РК1-Forum в г. Санкт-Петербурге между МОО «АЗИ» и членом международного комитета Unizeto и всеукраинской ассоциацией был подписан трехсторонний меморандум о взаимодействии и взаимной поддержке в развитии этих технологий и обмене опытом и достижениями в этой сфере.

Действительный меморандум работает. По его мотивам, в частности, российская делегация приняла активное участие в двух мероприятиях на Украине (РК1-форум Украина, E-government).

Меморандум открыт к присоединению к нему представителей других стран.

Одной из главных задач Ассоциации является продвижение российских разработок в области ИБ на международный рынок. В этой связи следует упомянуть проект, поддерживаемый и продвигаемый Ассоциацией по организации Международной выставки «Ехро».

Еще одной немаловажной задачей Ассоциации является организация обмена международным опытом и лучшими практиками в области разработки и создания СЗИ. В обеспечение этой задачи Ассоциация поддерживает и продвигает проект международной выставки «Infobez». В рамках которой Ассоциации удалось привлечь к участию в выставке одного из мировых лидеров в области создания СКЗИ швейцарскую компанию «Crypto AG».

Вполне понятно, и это я вставил в заключительную часть доклада, что Ассоциация уделяет, если не самое главное, то очень важное внимание развитию отношений в рамках Союзного государства, СНГ и ОДКБ.

В частности Ассоциация готова откликнуться на любые инициативы в этой области со стороны уполномоченных структур указанных объединений.

При этом положительным примером может являться активная работа Ассоциации по организации конференции «КЗИ» Союзного государства.

Отдельно хотел бы остановиться на развитии сотрудничества с дальним зарубежьем.

Безусловно, эта задача более сложная, учитывая высокий уровень конкуренции продуктов и услуг в области ИБ, устоявшийся рынок и сложности законодательных преград.

Вместе с тем, привлекательность РФ, как бизнес-партнера, обладающего серьезными ресурсами, позволяет нам оптими-

стично смотреть на вопрос об учете наших интересов, в том числе и в области принятия решений в области ИБ.

В этой связи Ассоциация в настоящее время работает над проектом конференции «Бизнес без границ» с местом проведения в Европе, на которой предполагается обсудить актуальные вопросы ИБ, встающие перед бизнесом.

Опыт показывает, что только совместными усилиями может быть достигнут положительный результат. И в этой связи Ассоциация готова принимать предложения заинтересованных сторон по месту, форме и тематике проведения конференции.

МЕТОДОЛОГИЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.Н. Бобов, А.А. Обухович,
ОАО «АГАТ-системы управления» –
управляющая компания холдинга «Геоинформационные системы управления»

Оценка рисков информационных технологий (ИТ-рисков), как составная часть системы управления рисками в сфере информационных технологий (СУРИТ), находит в последнее время все более широкое применение для оценки информационных систем (ИС) по критерию стоимость/эффективность.

СУРИТ основывается на совокупности документов, регламентирующих взаимосвязанные процессы идентификации ИТ, оценки ИТ-риска, обработки ИТ-риска, мониторинга ИТ.

Основным компонентом СУРИТ является оценка ИТ-риска, которая, в общем случае, определяется как комбинация вероятности наступления реализации угрозы безопасности и ущерба от ее реализации.

Известные нормативные документы [1-3] предлагают различные подходы к оценке рисков информационной безопасности, которые по методам получения оценок можно разделить на качественные, количественные и комбинированные.

К качественным, неформальным относят методы получения экспертных оценок вероятности реализации угроз и ущерба от их реализации. Неформальный подход основывается на знаниях и практическом опыте конкретных экспертов и называется базовым.

Количественный метод предполагает проведение детального анализа риска, включающего подробную идентификацию активов, оценку возможных угроз и уровня их уязвимости, основанные на расчетах значений вероятности оцениваемых событий и численных значениях ущерба.

К комбинированным относятся методы, сочетающие качественную и количественную оценки.

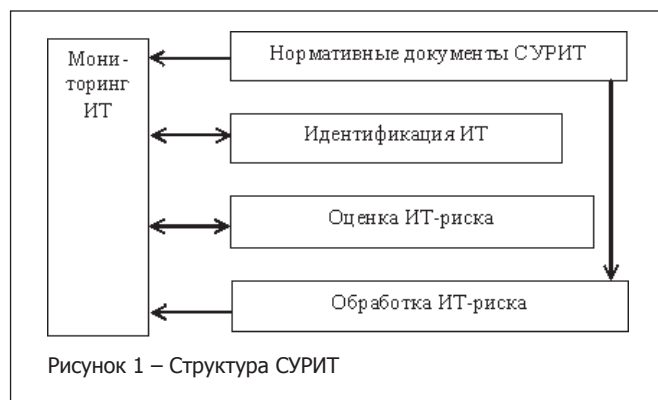


Рисунок 1 – Структура СУРИТ

Предлагается в качестве основы для разработки методик оценки риска информационной безопасности использовать комбинированный метод, заключающийся в обязательном проведении базовой (качественной) оценки и выборочной детальной (количественной) оценке риска. При этом, детальная оценка рисков проводится для событий, связанных с надежностью технических средств и программного обеспечения, стойкостью средств защиты, ошибками персонала.

На рисунке 2 приведена последовательность выполнения работ по оценке риска с указанием исходных данных для их выполнения.

Идентификация источников рисков включает:

- определение подлежащих рассмотрению источников рисков;
- определение элементов ИС, на которые могут воздействовать источники рисков;
- определение частоты воздействия источников рисков.

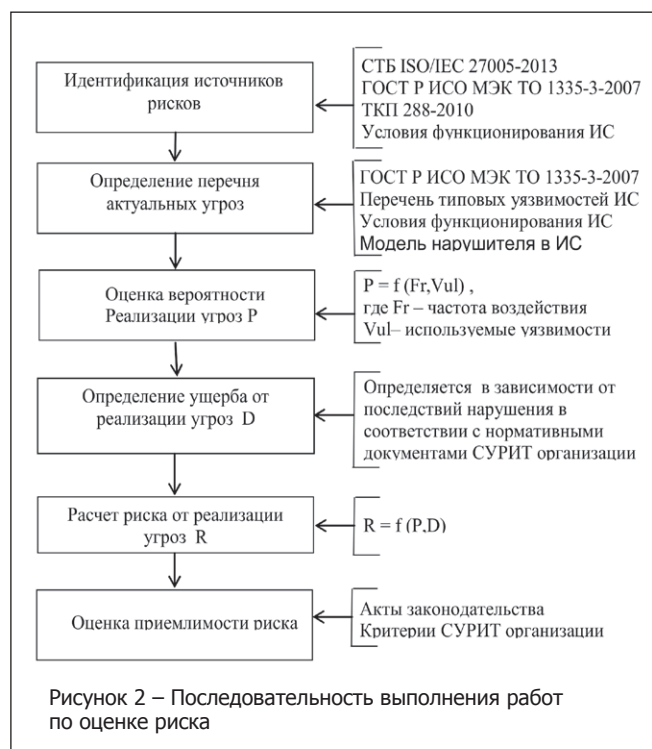


Рисунок 2 – Последовательность выполнения работ по оценке риска

Перечень актуальных угроз формируется для всех технических средств ИС с учетом условий их функционирования и модели нарушителя и для каждого типа источников:

- персонал ИС;
- посторонние лица за пределами контролируемой территории ИС;
- факторы, приводящие к отказам технических средств и программного обеспечения (техногенные, климатические и т.п.).

На основании совместного анализа полученного перечня угроз и информационных процессов в системе составляется перечень активов, подвергающихся угрозам.

Оценка вероятности реализации угроз определяется с учетом оценки частоты воздействия источников угроз, имеющихся средств защиты и присущих системе уязвимостей.

При детальной оценке рассчитываются вероятности реализации угроз, связанные с преодолением средств защиты, надежностью технических средств и программного обеспечения, ошибками персонала. В общем случае, вероятность событий, приводящих к реализации указанных угроз, является функцией от показателей надежности, стойкости к преодолению средств защиты и интервала времени, для которого рассчитывается вероятность.

Для базовой оценки риска вероятность реализации угроз безопасности (P) определяется соотношением: $P = Fr * Vul / (Fr * Vul)_{max}$, где: Fr – оценка частоты воздействия источников угроз; Vul – оценка уязвимостей (условий реализации угроз).

Для определения частоты воздействия источников угроз предлагается следующая шкала оценок:

- 0 – для значения «крайне редко»;
- 1 – для значения «редко»;
- 2 – для значения «регулярно»;
- 3 – для значения «часто»;
- 4 – для значения «очень часто».

Оценка уязвимостей производится экспертами на основе анализа исполнения технических и программных средств,

модели нарушителя и условий функционирования системы и может принимать значения:

- 0 – для показателя «нет условий»;
- 2 – для показателя «могут иметь место»;
- 5 – для показателя «имеются некоторые условия»;
- 8 – для показателя «имеются все условия».

Оценка ущерба проводится экспертным методом на основании анализа подвергаемых угрозам информационных активов. Применяется вербальный показатель ущерба (D), который может принимать три значения:

- низкий ущерб – 60;
- средний ущерб – 150;
- высокий ущерб – 250.

Показатель риска (R) рассчитывается по формуле $R = P * D$.

Оценка приемлемости риска производится путем сравнения полученного значения с критерием приемлемости риска. Для принятых в предложенной методике шкал значений вероятности реализации угроз безопасности и оценки ущерба был выбран следующий критерий приемлемости:

- риски, имеющие оценку менее или равны 30, считаются приемлемыми.
- риски, имеющие оценку более 30, считаются неприемлемыми – требующими обработки.

Предложенная методика прошла апробацию.

Литература:

1. ГОСТ Р ИСО/МЭК ТО 13335-3:2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент безопасности информационных технологий. Часть 3. Методы менеджмента безопасности информационных технологий.
2. СТБ ISO/IEC 27005-2013 Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности.
3. ТКП 288-2010 Банковские технологии. Управление рисками в сфере информационных технологий.

КИБЕРНЕТИЧЕСКИЕ ВОЙНЫ: ОСНОВНЫЕ ВЫЗОВЫ И ИГРОКИ

**В.А. Артамонов,
МНОО «Международная академия
информационных технологий» (ООН)**

Сегодня много говорится об «информационных и кибернетических» войнах». Однако вряд ли кто сможет точно ответить, что это такое. Более того, даже специалисты не смогут точно ответить на вопрос о том, когда же все-таки родилось само словосочетание «информационная и/или кибернетическая» война, когда впервые был поставлен вопрос о том, чтобы рассматривать информацию в качестве оружия?

Рассмотрим основные понятия и определения столь тонкой и специфичной для рядового обывателя именно сущности информационного мироздания.

Информационная война (Information war) – это воздействие на противника посредством информации с

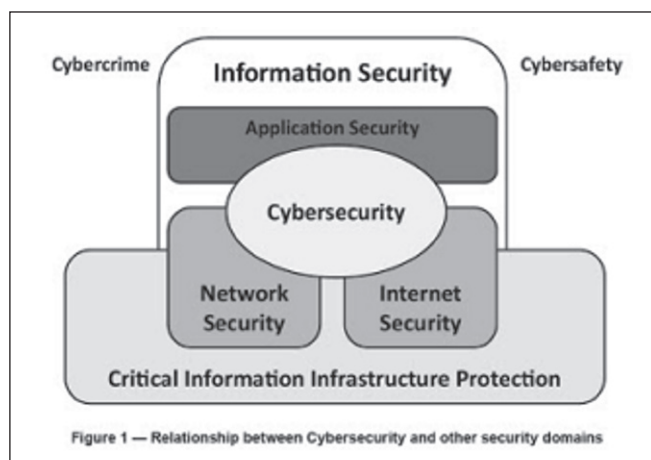
деструктивными целями. Понятие это очень широкое и в наш век информатизации и информационных технологий включает в себя очень многое. Но все эти методы, технологии и техники объединяет цель – деструктивное воздействие на противника и то, посредством чего, это воздействие осуществляется (информация). На западе информационные войны иногда, не совсем правильно, принято называть кибервойнами (Cyber-warfare). Выражение «информационная война», по сути, заимствовано из военной среды США, в которой означает воздействие на население какой-либо страны путем использования определенной информации (или дезинформации). Для

более детального изучения данных понятий можно ознакомиться с одним из учебных пособий Национального Университета обороны США (<http://www.dtic.mil/cgi-bin/>). Синонимом этого выражения может являться термин «психологическая война».

Кибервойна, с другой стороны, представляет собой вид военных действий с использованием компьютеров и Интернета, посредством электронных способов, а не физических. Во многих документах, в том числе и международных, понятие информационной войны включает в себя признаки кибервойны. Главной целью информационной войны является изменение психологического состояния людских ресурсов с целью дестабилизации политической или общественной ситуации. Главным оружием является информация как таковая – увиденная, услышанная или прочитанная. Кибервойна же нацелена, в первую очередь, на важнейшие системы функционирования и жизнеобеспечения государства – электростанции, энергетические сети, пути сообщения, водооборотные, трубопроводные транспортные системы и тому подобные. Несмотря на то, что оба понятия подразумевают воздействие на информационные активы, сферы их приложения все же различны, как и виды информации, на которые распространяется их влияние.

Кибервойна – компьютерное противостояние в пространстве Интернета, которое направлено, прежде всего на дестабилизацию компьютерных систем и доступа к Интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на Интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находят продолжение в Интернете в виде кибервойны: вандализме, пропаганде, шпионаже и непосредственных атаках на компьютерные системы и серверы. Одно из определений термина звучит так: «кибервойна – использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической и информационной безопасности и суверенитету другого государства». Как писал эксперт по безопасности правительства США Ричард А. Кларк в своей книге «Кибервойна» (вышла в мае 2010 года) «кибервойна – действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Американский журнал *The Economist* описывает кибервойну как «пятую область войны, после земли, моря, воздуха и космоса». О важности готовности к ведению военных действий в киберпространстве свидетельствует факт создания в США целого воинского подразделения – киберкомандования США. Основными задачами обеспечения информационной безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Кибербезопасность являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Рассматривая различные стратегии информационной и кибербезопасности, хочется обратить внимание, на наш взгляд, на наиболее точное описание этих понятий и их связь с другими



терминами из области информационной безопасности, приведенное в http://lukatsky.blogspot.ru/2013/01/blog-post_28.html, которое опирается на Международный стандарт. Речь идет о стандарте ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity, который был принят в июле прошлого года. Он дает однозначное понимание связи термина Cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур. И с точки зрения международных экспертов все эти термины объединяет понятие Information Security (информационная безопасность). В стандарте приводится вот такая картинка, которая визуализирует связь этих терминов:

И сразу становится понятно, что кибербезопасность и так нам привычная информационная безопасность – это совсем не одно и то же. И безопасность критичных информационных инфраструктур хоть и связана с кибербезопасностью (так как ее понимают во всем мире), но только частично.

Киберпреступность (cybercrime) же вообще стоит особняком и не имеет никакого отношения ни к информационной безопасности, ни к кибербезопасности. Также как и понятие cybersafety, которое в русском языке не имеет прямого и емкого перевода, но смысл его таков – безопасное поведение в киберпространстве и, в первую очередь, защита детей от негативной информации в Интернет.

Нет никакого сомнения в том, что наиболее продвинутые и хорошо финансируемые военные структуры многих стран имеют планы ведения не только обычной, но и кибервойны – как оборонительного, так и наступательного характера. Разговоры на эту тему идут давно, поэтому со стороны военных было бы глупо игнорировать потенциальные угрозы кибератак, не вкладывая средства в укрепление своих оборонительных возможностей. А также не задумываться о тех стратегических или тактических возможностях, что дают кибератаки на врага в условиях реальной войны. Отсюда следует, что на случай войны вооруженные силы должны накапливать и совершенствовать инструменты для проведения Интернет-атак. Это могут быть средства для атак типа «отказ в обслуживании» и для тайного проникновения разведок в военные системы противника, использующие слабости распространенных компьютерных платформ. Плюс «черви» и вирусы, похожие на те, что используются криминальными структурами, но с заточкой под определенную страну или ведомственную сеть. Это могут быть троянцы для перехвата информации в сетях,

нарушения сетевых операций или устройства «тоннелей» для проникновения в более защищенные уровни сетей.

Давайте с этих позиций проанализируем соответствующие стратегии и структуры противодействия и ведения кибервойн основных Международных игроков на поле «кибернетической брани».

США. Кибернетическое командование в составе Стратегического командования Вооруженных сил США было создано в 2009 году для централизованного управления всеми операциями в области кибербезопасности. Возглавил командование генерал Кит Александр (Keith Alexander), он же с 2005 года является директором Агентства национальной безопасности США. В этом году оборонное ведомство США одобрило план пятикратного увеличения численности подразделений кибербезопасности. Об этом 28 января 2013 г. пишет The Washington Post со ссылкой на информированные источники в правительстве. Расширение штата проводится по требованию киберкомандования Пентагона. В настоящее время командование насчитывает 900 сотрудников. В соответствии с принятым планом, это число возрастет до 4900 военных и гражданских специалистов. Согласно замыслу, после реформы оборонное ведомство сможет не только отражать кибератаки на критическую инфраструктуру США, но проводить наступательные кибероперации против иностранных противников. В частности, работу киберкомандования предполагается вести по трем основным направлениям: защита американских компьютерных сетей и критической инфраструктуры, защита компьютерных сетей Пентагона и поддержка боевых операций за пределами США.

Россия. Кибервойска РФ рождаются в Генштабе: первый зампред комитета Госдумы по обороне Виктор Заварзин по итогам заседания комитета с участием главы Генерального штаба Валерия Герасимова сообщил, что в Генштабе Вооруженных сил России начало работу специальное подразделение по кибербезопасности. «Серьезная работа была проделана по информационной безопасности, создается новая структура в Генштабе», – сказал Заварзин, добавив, что она уже начала работать. По его словам, в перспективе система кибербезопасности останется в структуре Генштаба, а не будет выделена в отдельный род войск, как предполагалось ранее, передает РИА «Новости». Как сообщалось ранее, в январе 2013 г. Владимир Путин своим Указом поручил ФСБ создать систему отражения кибератак на российские государственные порталы. В подписанном 15 января 2013 г. Указе основными задачами создаваемой системы определены прогноз ситуации в области информационной безопасности страны и контроль степени защищенности критической информационной инфраструктуры России от компьютерных атак, а также установление причин компьютерных сбоев. К информресурсам в Указе отнесены «информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом».

Далее, в докладе рассматриваются стратегии и структуры противодействия и ведения кибервойн ведущих мировых государств и межгосударственных объединений, таких как: Евросоюз, Великобритания, Китай, Япония, Израиль, СНГ и др.

VECTOR OF TECHNOLOGIES

**ПРЕДЛАГАЕМ ПОСТАВКИ СО СКЛАДА И ПОД ЗАКАЗ:
ЧАСТОТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ, СЕРВОДВИГАТЕЛЕЙ,
ЭЛЕКТРОДВИГАТЕЛЕЙ, ИНДУКТИВНЫХ ДАТЧИКОВ, ФОТОДАТЧИКОВ,
ТВЕРДОТЕЛЬНЫХ РЕЛЕ И ДРУГОГО ОБОРУДОВАНИЯ
ОТ ВЕДУЩИХ МИРОВЫХ ПРОИЗВОДИТЕЛЕЙ.**



**Компания «Вектор Технологий»
является официальным дистрибьютором
на территории Республики Беларусь компаний
YASKAWA, DATALOGIC, STEUTE, FOTEK, WEG и VIPA.**

Наши специалисты с радостью помогут решить ваши задачи.
Tel: +375-17-265-60-15, fax: +375-17-265-60-16, mob: +375-29-685-60-15.
info@vec-tech.by, web: <http://www.vec-tech.by>

ЗАОЧНОЕ УЧАСТИЕ

КЛАССИФИКАЦИЯ НЕДЕКЛАРИРОВАННЫХ ФУНКЦИЙ В МИКРОСХЕМАХ

О.К. Барановский, Е.Е. Орлов,

Государственное предприятие «НИИ ТЗИ», г. Минск

Аппаратное обеспечение современных компьютерных систем создается путем интеграции большого числа базовых компонент (модулей). Сложность таких систем является причиной того, что характеристики и выполняемые аппаратным обеспечением функции описаны в технической документации не в полной мере. Недекларируемые отличия могут вноситься преднамеренно, например, в качестве инструментов производственного тестирования компаниями-производителями, в целях реализации каких-либо действий в процессе эксплуатации без ведома или согласия пользователя, а также могут быть вызваны ошибками в технологических процессах разработки и производства. Описанные отличия оказывают влияние на информационную безопасность компьютерных систем, при этом наибольший риск несут недекларируемые функции, специально вносимые для выполнения вредоносных действий. Обнаружение и противодействие угрозам внесенных включений и модификаций является одной из первостепенных задач, направленных на предотвращение нарушения штатного режима функционирования (вплоть до выхода из строя) критически важных объектов информатизации, эксплуатируемых в различных сферах деятельности государства и общества.

В открытых источниках информации отсутствуют достоверные данные о фактах обнаружения недекларируемых аппаратных функций в микросхемах. Однако это не означает, что угроза их применения отсутствует, поскольку реализация относительно простых недекларируемых функций с технической точки зрения не представляется сложной для производителя, а методы их обнаружения требуют наличия специализированного оборудования и методик поиска.

В связи с этим, создание классификации недекларируемых функций в микросхемах (НФМ) для решения задач разработки, оценки качества и выбора методов их поиска является актуальной задачей.

Среди недекларируемых функций выделяют закладные схемы – составные элементы интегральных микросхем. В то же время, к недекларируемым функциям относят, например, изменение химического состава отдельных элементов или всего кристалла микросхемы с целью усиления эффекта старения объекта [1].

Классификация НФМ должна удовлетворять двум основным требованиям:

- 1) все существующие объекты должны описываться классификацией;
- 2) объекты классификации, отличающиеся по существенным признакам, должны классифицироваться как разные классы [2].

В открытых источниках приведено несколько вариантов классификаций НФМ.

Первая классификация [3] содержит три группы признаков: «физические характеристики», «активационные характеристики» и «характеристики действия». Физические характеристики содержат следующие признаки: «тип», «размер», «распределение». Группа активационных характеристик, как и характеристик действия, представлена одним классификационным признаком, имеющим составные значения.

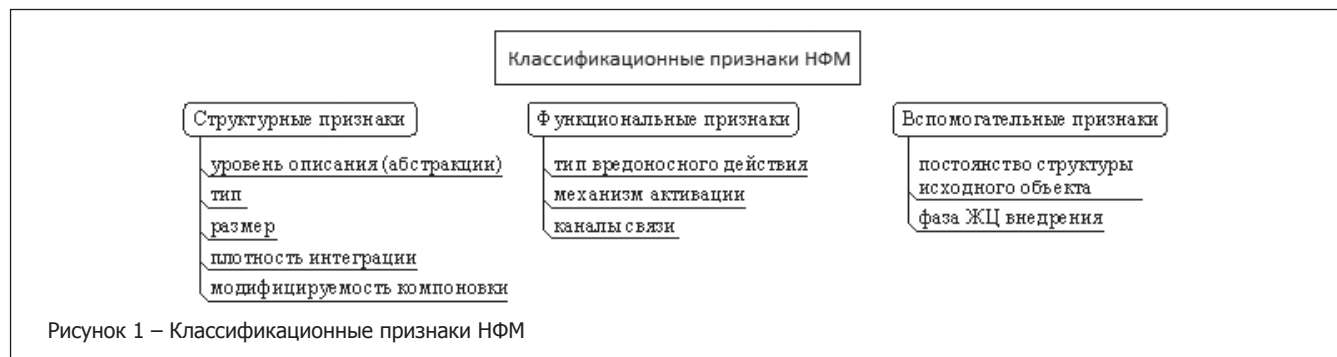
Вторая классификация [2] содержит пять признаков: «фаза внедрения», «уровень абстракции», «механизм активации», «действия» и «расположение».

Выделим основные недостатки упомянутых классификаций. В обеих классификациях не выделен отдельно фактор, описывающий способ передачи информации между НФМ и внешним субъектом. Данный фактор является важным для описания НФМ, реализующих утечку информации либо получающих команды управления извне. Кроме этого, в первой классификации есть признак «размер», имеющий два значения: «большой» и «малый». Критерий выбора между этими значениями является нечетким, поскольку для одного метода поиска конкретная НФМ может быть большой, а для другого – малой. Также во второй классификации имеется избыточный признак «расположение» [2]. Классифицируемая микросхема может не соответствовать определенному типу из предложенных вариантов [2].

Таким образом, необходимо разработать классификацию, основывающуюся на описанных в литературе [2, 3], но исправляющую их недостатки.

Классификационные признаки предлагаемой классификации представлены на рисунке 1.

Исходя из определения объектов классификации (НФМ, нарушающие информационную безопасность компьютер-



ной системы) выделено несколько групп классификационных признаков. Группа структурных признаков описывает НФМ как составные части микросхем в понятиях, применяемых для описания внутренней структуры микросхем. Группа функциональных признаков описывает механизмы реализации вредоносных действий с применением НФМ. Группа вспомогательных признаков служит для вторичных целей.

Группа структурных признаков включает в себя следующие: «уровень описания (абстракции)», «тип», «размер», «плотность интеграции», «модифицируемость компоновки».

Для описания функции важными являются следующие параметры: действие функции, способ вызова функции и способ получения результатов действия функции. Соответственно, в группу функциональных классификационных признаков отнесены следующие признаки: «тип вредоносного действия», «механизм активации», «каналы связи».

Вспомогательные признаки содержат следующие: «постоянство структуры исходного объекта» и «фаза жизненного цикла внедрения».

Классификационные признаки «уровень описания (абстракции)», «фаза жизненного цикла внедрения» соответствуют классификации [2].

Классификационные признаки «тип», «размер», «плотность интеграции» соответствуют классификации [3]. Изменены значения для признака «размер»: при проведении классификации НФМ необходимо указывать как относительный, так и абсолютный размер НФМ. Также предлагается определять абсолютный размер в зависимости от типа НФМ:

1) для НФМ параметрического типа – как величину изменения параметра, наиболее важного при внедрении параметрической НФМ, для всей микросхемы (например, НФМ – несколько лишних проводников; ее размер – изменение суммарной длины всех проводников микросхемы, то есть сумма длин внедренных проводников НФМ);

2) для НФМ функционального типа – как число измененных (удаленных, добавленных) в НФМ элементов того уровня, на котором проводится их описание.

Классификационные признаки «тип вредоносного действия» и «механизм активации» соответствуют классификации [2], [3].

Признак «постоянство структуры исходного объекта» соответствует необходимости изменения компоновки микросхемы,

в которую внедряется НФМ. Выделение данного признака обосновано тем, что от того, необходима ли перекомпоновка, зависит, например, будет ли микросхема с НФМ сильно отличаться по побочным сигналам от микросхемы без НФМ [3]. Данный признак выделен в группу вспомогательных признаков в связи с тем, что он важен только в том случае, когда существуют микросхемы без НФМ и возможно провести сравнение с эталоном.

Признак «модифицируемость компоновки» описывает, необходимо ли для создания НФМ в заданной микросхеме использовать определенную компоновку (относительное расположение в кристалле элементарных единиц (элементов) микросхемы, например, проводников), либо НФМ может быть реализована с различными типами компоновок. Признак выделен с целью учета фактора поиска НФМ: при фиксированной компоновке однажды найденную НФМ проще обнаружить в других микросхемах.

Признак «каналы связи» описывает возможные виды и варианты использования каналов передачи, которые могут использоваться для создания утечек данных и приема команд управления НФМ. Данный признак необходим для того, чтобы выделить способ, которым НФМ обменивается с внешним субъектом (например, злоумышленником). Это важно на этапах поиска НФМ и оценки вероятности их использования на конкретных объектах.

Разработанная система классификационных признаков была апробирована при классификации тестовых НФМ, разработанных в рамках конкурса «CSAW» [4].

Литература:

1. Shiyonovskii Y., Wolff F., Papachristou C., Weyer D., Clay W. Hardware Trojan by Hot Carrier Injection // URL: <http://arxiv.org/pdf/0906.3832>.
2. Karri R., Rajendran J., Rosenfeld K., Tehranipoor M. Trustworthy Hardware: Identifying and Classifying Hardware Trojans // IEEE Computer, October 2010.
3. Wang X., Tehranipoor M., Plusquellic J. Taxonomy of Trojans for IC Trust // http://www.ece.unm.edu/~jimp/HOST/papers/Trojan_taxonomy.pdf.
4. Embedded Systems Challenge // <http://www.poly.edu/csaw2011/csaw-embedded>.

МАТЕРИАЛЫ НА ОСНОВЕ ДЕНАТУРИРОВАННОГО КОЛЛАГЕНА И ПОРОШКООБРАЗНЫХ ОТХОДОВ ПРОИЗВОДСТВА ЧУГУНА ДЛЯ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТ ВНЕШНИХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ

О.В. Бойправ, Т.В. Борботько, Г.А. Пухир, БГУИР, г. Минск

Автоматизированные системы обработки информации базируются на основе средств вычислительной техники (СВТ). От работоспособности последних зависит скорость обработки информации и ее целостность в процессе хранения либо передачи. Работоспособность СВТ может быть нарушена вследствие воздействия на ее узлы внешнего электромагнитного излучения (ЭМИ), источником которого могут являться функционирующие вблизи радиоэлектрон-

ные устройства. Защитить узлы СВТ от внешнего ЭМИ возможно путем их экранирования при помощи материалов, обеспечивающих ослабление энергии ЭМИ. Такие материалы должны характеризоваться эффективностью, пониженной массой на фоне малой стоимости, которая может быть обеспечена путем выбора нетрудоемкой технологии их изготовления с использованием при этом недорогостоящих компонентов.

В настоящей работе на основе порошкообразных отходов производства чугуна (шлама очистки ваграночных газов – ШОВГ) размера фракций 5...30 мкм и водного раствора денатурированного коллагена, взятого в различных фазах, изготовлены материалы для ослабления энергии ЭМИ. Образцы материалов №1–№6 были сформированы путем смешивания 30%-ого водного раствора денатурированного коллагена с ШОВГ размера фракций 5 мкм (образец №1, №4), 20 мкм (образец №2, №5) и 30 мкм (образец №3, №6), причем при формировании образцов №4–№6 использовался вспененный водный раствор денатурированного коллагена. Образцы материалов №7, №8 и №9 изготавливались путем нанесения слоя ШОВГ с фракциями размера 5 мкм, 20 мкм и 30 мкм соответственно на слой вспененного водного раствора денатурированного коллагена, находящегося в жидкой фазе. Переход образцов из жидкой фазы в твердую наблюдался при комнатной температуре. Объемное соотношение водного раствора денатурированного коллагена и ШОВГ в образцах – 4:5. Изменение данного соотношения приводит к ухудшению технологичности и эксплуатационных свойств формируемых материалов. Толщина полученных образцов составляла 3 мм.

ШОВГ представляет собой порошкообразные отходы, являющиеся результатом фильтрации и обработки в осевом циклоне газов, поступающих из вагранок. Размер фракций и соотношение компонентов ШОВГ определяются тем, на каком этапе обработки он был отобран. В состав ШОВГ входят оксиды металлов: двух- и трехвалентного железа, алюминия, магния, калия, кальция и т. д., а также оксиды кремния и серы. ШОВГ по своим магнитным свойствам, так же, как и ферриты, относится к ферромагнетикам: значение его относительной магнитной проницаемости зависит от величины индукции внешнего магнитного поля и составляет в зависимости от размера фракций 8...40, для него характерны явления остаточной намагниченности. Следовательно, ШОВГ, так же, как и ферриты, взаимодействуя с ЭМИ, способен обеспечивать потери его энергии на магнитную проницаемость. При этом, в отличие от ферритов, ШОВГ характеризуется низкой стоимостью, в связи с чем его выгодно использовать в качестве компонента при формировании материалов, обеспечивающих ослабление энергии ЭМИ.

Денатурированный коллаген является желирующим веществом, относящимся к числу фибриллярных или волокнистых белков, имеющих макромолекулы в виде вытянутых нитей. Денатурация (сваривание, гидролиз) коллагена сопровождается нарушением специфической конфигурации полипептидных цепей его молекулы, при котором уменьшается длина, увеличивается диаметр его волокон и образуется глютин. Между сближенными сегментами фибрилл коллагена при его денату-

рации легко образуются так называемые водородные мостики, превращающие макромолекулы в единую непрерывную сетку. При растворении в воде денатурированного коллагена наблюдается явление сшивания его макромолекул, вследствие чего водные растворы денатурированного коллагена при температуре 20...25 °С превращаются в студни. Прочность таких студней зависит от концентрации в них глютина, а значит, и денатурированного коллагена. Таким образом, использование денатурированного коллагена при формировании материалов, обеспечивающих ослабление энергии ЭМИ, дает возможность управлять их гибкостью, а также влагосодержанием.

При проведении измерений ослабления и коэффициентов отражения изготовленных образцов материалов использовалась установка, содержащая генератор качающейся частоты 61 и индикатор КСВН и ослабления Я2Р-67. Измерения проводились в частотном диапазоне 8...12 ГГц. В качестве излучателя и приемника сигнала использовались концы волноводов. Такой способ при малой толщине образца (до 3 мм) принимается эквивалентным использованию измерительной ячейки.

Индикатор Я2Р-67 работает по принципу отдельного выделения и непосредственного детектирования уровней падающей и отраженной волн. Сигнал, пропорциональный мощности, падающей на нагрузку, выделяется направленным детектором падающей волны (ДНпад). Ослабление, вносимое исследуемым образцом, определяется отношением сигналов, выделяемых ДНотр и ДНпад (рисунок 1, а). Для нахождения коэффициента отражения образцов определяется сигнал, отраженный от исследуемой нагрузки и выделенный направленным детектором отраженной волны (ДНотр) (рисунок 1, б).

Установлено, что значения коэффициентов отражения образцов №1, №2 и №3 составляют –2,5...–3,5 дБ при значениях ослабления 11...12 дБ, 13,5...15,5 дБ и 28,8...32 дБ соответственно. Изменение фазы водного раствора денатурированного коллагена (вспенивание) приводит к увеличению ослабления формируемых на его основе образцов до 20 дБ и >40 дБ (в образцах №4, №5 и №7, №8 соответственно), до 35 дБ и >40 дБ в образцах №6 и №9 соответственно) на фоне снижения коэффициентов отражения до –7...–8 дБ (в образцах №7, №8 и №9).

Частотные зависимости ослабления образцов, изготовленных на основе ШОВГ с размером фракций 5 мкм, и коэффициентов их отражения при наличии за ними металлической пластины, представлены на рисунке 2 и рисунке 3 соответственно.

Электромагнитное излучение, взаимодействуя с водными растворами, находящимися в твердой либо жидкой фазах, в значительной степени отражается от их поверх-

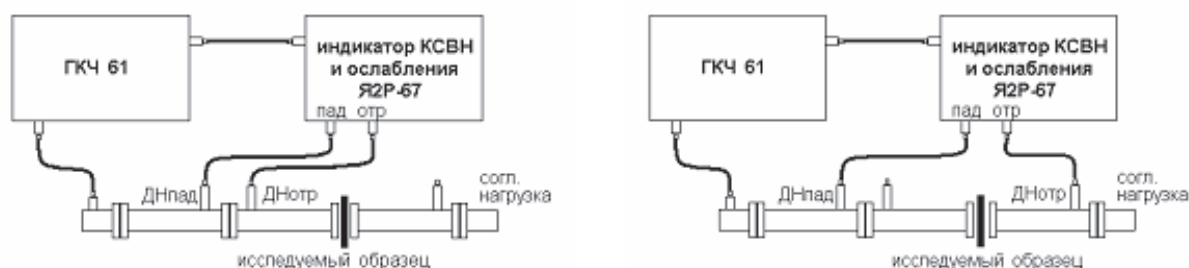


Рисунок 1 – Структурная схема установки для измерения ослабления (а) и коэффициентов отражения ЭМИ (б) исследуемого образца

ности, ввиду большой разности между диэлектрической проницаемостью его начальной среды распространения (воздуха) и диэлектрической проницаемостью воды и водных растворов.

Вспенивание водных растворов приводит к снижению содержания в единице их объема воды по сравнению с невспененными водными растворами аналогичного состава. Поэтому при взаимодействии ЭМИ со вспененными растворами, находящимися в твердой либо жидкой фазах, наблюдается явление рассеяния его энергии на многочисленных границах раздела воздух–раствор, многократное его переотражение от этих границ, а также частичное его поглощение их материалом.

Описанные явления и объясняют причину снижения значений коэффициентов отражения и увеличения ослабления образцов, сформированных на основе вспененных водных растворов коллагена.

Добавление в водные растворы порошкообразных компонентов приводит к увеличению доли энергии ЭМИ, рассеиваемой внутри них. Величина данной энергии зависит от размеров частиц этих компонентов.

Таким образом, на основе смесей ШОВГ и растворов денатурированного коллагена (в том числе и вспененных) можно создавать покрытия для корпусов и оплеток кабельных линий СВТ. Изменять экранирующие, механические и массогабаритные свойства данных покрытий возможно путем изменения размеров фракций используемого при их формировании ШОВГ, объемного содержания

денатурированного коллагена и/или фазы его водного раствора. Такие покрытия будут обеспечивать снижение степени влияния на работоспособность СВТ (а значит, и на целостность обрабатываемых, хранимых либо передаваемых ими данных) внешнего ЭМИ.

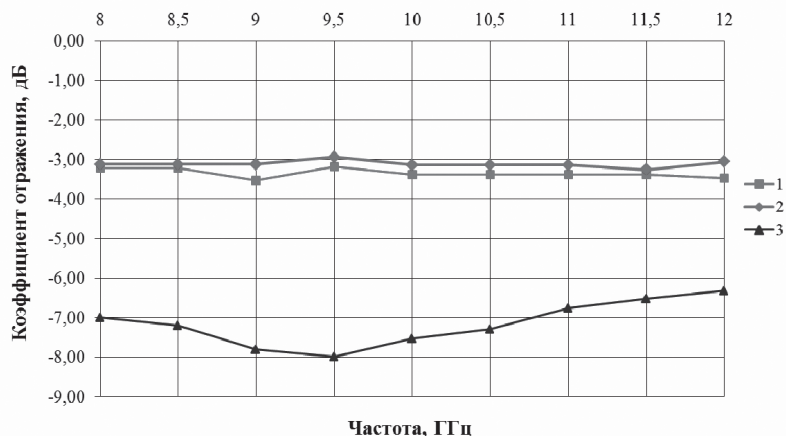


Рисунок 2 – Частотные зависимости коэффициентов отражения:
1 – образца №1; 2 – образца №4; 3 – образца №7

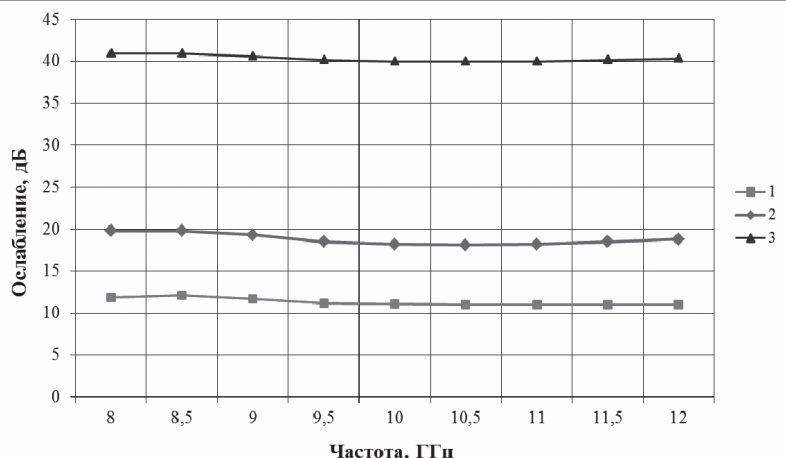


Рисунок 3 – Частотные зависимости ослабления:
1 – образца №1; 2 – образца №4; 3 – образца №7

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПОНИЖЕННЫХ ТЕМПЕРАТУР НА СВОЙСТВА ШУНГИТОБЕТОННЫХ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Е.С. Белоусова, М.Ш. Махмуд, Е.А. Криштопова, научный руководитель: Л.М. Лыньков, БГУИР, г. Минск

Условия эксплуатации электронного оборудования и других источников электромагнитного излучения (ЭМИ) предъявляют зачастую особые требования к защитным конструкциям экранов ЭМИ. К таким требованиям можно отнести устойчивость к коррозии, экстремальным температурам и неоднократному механическому воздействию. При этом, особо важным является сохранение высокой эффек-

тивности защиты от нежелательного воздействия ЭМИ на организм человека или электронное оборудование. Поэтому было решено в настоящей работе провести исследование экранирующих и эксплуатационных свойств порошковых композиционных материалов на основе шунгита при длительном воздействии на них повышенных и пониженных температур в широких пределах.



Шунгит представляет собой природный материал с равномерным распределением высокодисперсных кристаллических силикатных частиц размером в среднем около 1 мкм в аморфной графитоподобной углеродной матрице с элементами глобулярной структуры. Между углеродом и силикатами в материале имеется исключительно развитый (около 20 м²/г) и плотный контакт [1]. Остальные составляющие шунгита – оксиды металлов железо- и алюмосиликаты и т.д. [2] также могут содержать микровключения сульфидов металлов Fe₂S, NiS, Ni₂FeS₄ и др. Предполагается присутствие вкраплений типа углерод – карбид металла – металл [3].

По мнению исследователей [4] в большинстве случаев элементарным фрагментом структуры шунгитового углерода является глобула с размерами ~ 100 А. Элементы структуры могут быть окружены случайной сеткой атомов углерода и атомами примесей, они могут быть ориентированы как случайным образом, так и собираться в пачки, волокна, пакеты, слои, т.е. упорядочены настолько, что может проявляться анизотропия физических свойств. Предполагается, что углерод присутствует в цепочечном виде и характеризуется устойчивыми связями типа $\text{C}\equiv\text{C}$ - и $\text{C}=\text{C}$ -. В углеродных глобулах распределены вода, микроэлементы, дифильная битумоидная органика, фуллерены в форме C₆₀ и C₇₀ и нанотрубки [5].

Такие свойства шунгита, как высокая механическая прочность и электропроводность, способность к взаимодействию со всеми связующими обеспечивают получение строительных материалов в виде кирпича, бетона, кладочных и штукатурных растворов с электропроводными свойствами, способных экранировать электромагнитные излучения высоких частот. Наполненные шунгитом строительные материалы защищают человека от вредных излучений высоких и сверхвысоких частот. Такие материалы находят применение для строительства жилых и общественных зданий в зонах линий электропередачи, радиостанций и ретрансляторов, в частности, работающих на частотах мобильной сети, локаторов. Шунгитовые экраны – экологически чистые и безопасные. Особенностью их является способность экранировать только вредные для здоровья высокочастотные излучения и быть прозрачными для магнитного поля Земли.

Композитный состав, невысокая стоимость, ингибиторные свойства, относительно невысокая масса обуславлива-

ют возможность его использования в качестве основы для создания материалов, для электронной техники.

В работе были изготовлены экспериментальные образцы композиционных поглотителей ЭМИ из порошка шунгита, выполненные в виде модуля конструкции размером 100×100 мм и толщиной 3 мм, закрепленного на трикотажной матрице неорганическим синтетическим связующим. Для создания равномерной структуры поверхности и распределения элементов композита по всему объему образца, создавалась вязкая структура с влагосодержанием по объему не менее 20 %. Измерения экранирующих характеристик производились через сутки после их изготовления, влагосодержание конструкций понизилось вдвое, что подтвердилось гравиметрическими измерениями.

Измерение характеристик ослабления и отражения проводили в диапазоне 0,7...18 ГГц при помощи измерительного комплекса SNA 0,01-18.

Исследования влияния эксплуатации шунгитобетонных пирамидальных покрытий на целлюлозном основании проводили путем выдерживания в морозильной камере при -18°C. После извлечения из морозильной камеры проводились измерения экранирующих свойств (ослабления ЭМИ и коэффициента отражения) при температурах -10 °C, 5 °C, 23 °C. На рисунке 1 представлены экспериментальные зависимости изменения коэффициента отражения покрытий из шунгитобетона при вышеуказанных температурах. Проведенные измерения показали, что данные зависимости незначительно (в пределах погрешности измерений) отличаются одна от другой.

Таким образом, эксплуатация шунгитобетонных покрытий при температурах ~-10°C не вызывает существенных изменений их экранирующих характеристик.

Литература:

1. Волков И.А. Версия о фуллереновой природе пористости глобулярных шунгитов Карелии / И.А. Волков, И.А. Кушмар // Углеродсодержащие формации в геологической истории: Тез. докл. междунар. симп., 2-7 июня 1998 г. Петрозаводск: Карельский научный центр Российской академии наук, Институт геологии, 2000. – С. 121-124.
2. Березкин, В.И. Исследование структуры природного стеклоглерода шунгитов методом рамановской спектроскопии / В.И. Березкин, Ю.В. Холодкевич, В.Ю. Давыдов // Углеродсодержащие формации в геологической истории: Тез. докл. междунар. симп., 2-7 июня 1998 г. – Петрозаводск: Карельский научный центр Российской академии наук, Институт геологии, 2000. – С. 111.
3. Зайденберг, А.З. Микроэлементный состав шунгитов первой разновидности / А.З. Зайденберг // Сб. тез. докл. 7-й конф. по ХТТ России и стран СНГ, 1996 г. – М.: 1996. – С. 66-67.
4. Соловьева, А.Б. Органическое вещество шунгитовых пород / А.Б. Соловьева, Н.Н. Глаголев, Н.А. Зайченко // Углеродсодержащие формации в геологической истории: Тез. докл. междунар. симп., 2-7 июня 1998 г. – Петрозаводск: Карельский научный центр Российской академии наук, Институт геологии, 2000. – С. 131-133.
5. Борботько, Т.В. Углеродсодержащие минералы и области их применения / Т.В. Борботько [и др.]; под ред. Л.М. Лынькова. – Минск: Бестпринт, 2009 – 156 с.

ОБЗОР ОБНОВЛЕННОЙ РЕДАКЦИИ БАЗОВОГО СТАНДАРТА ОЦЕНКИ БЕЗОПАСНОСТИ

Е.П. Максимович, Т.С. Мартинович,
А.Б. Степанян, В.К. Фисенко,
ОИПИ НАН Беларуси, г. Минск

В настоящее время в Республике Беларусь ведутся работы по подготовке обновленной версии стандарта оценки безопасности СТБ 34.101.3-20XX «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности», идентичного по содержанию международному стандарту ISO/IEC 15408-3:2008 [1]. Актуальность данной работы обусловлена тем, что ныне действующий стандарт СТБ.34.101.3-2004, являясь одним из базовых стандартов в области информационной безопасности, уже устарел и перестал соответствовать аналогичному международному стандарту. В докладе обсуждаются основные изменения, произошедшие в новой версии стандарта.

Общая концепция новой версии СТБ.34.101.3 – обеспечение гарантии безопасности путем проведения активного исследования продукта информационных технологий (ИТ) с целью независимой и достоверной оценки его фактических свойств безопасности – осталась, по сравнению с СТБ.34.101.3-2004, прежней. Однако методы исследования претерпели ряд существенных изменений.

Можно выделить следующие основные изменения.

1. Объектом рассмотрения в новой версии СТБ.34.101.3 являются продукты ИТ (а не продукты и системы ИТ как СТБ 34.101.3-2004).

2. Введены два основных типа объектов оценки (ОО): простые (однокомпонентные) и составные. Составной объект предполагает выбор двух или более объектов ИТ, прошедших успешную оценку безопасности в соответствии с новой версией СТБ.34.101.3 и объединение их для использования без какой-либо дальнейшей доработки каждого из составляющих компонентов. Составной ОО образует новый продукт, который может быть установлен и интегрирован в любой конкретный вариант среды, обеспечивающей выполнение сформулированных задач безопасности для среды. В составном ОО один компонент обычно опирается на сервисы, предоставленные другим компонентом. Компонент, которому необходимы сервисы, называется зависимым компонентом, а компонент, предоставляющий сервисы, – базовым. Введение простых и составных ОО обусловлено потребностью в использовании принципиально разных подходов к их оценке (в частности, в составном объекте особое внимание уделяется исследованию интерфейсов между составляющими его компонентами).

3. Изменился состав классов гарантийных требований:

- введен новый класс АСО «Составной объект»;
- исключен класс АСМ «Управление конфигурацией»;
- исключен класс АДО «Поставка и ввод в эксплуатацию»;
- исключен класс АМА «Поддержка гарантии».

3.1. Класс АСО «Составной объект» дает методологическое обеспечение процесса оценки составного

ОО, включая общие требования к проведению тестирования взаимодействия его компонентов и анализу возможного внедрения уязвимостей в ходе объединения компонентов. Введенные гарантийные требования предназначены для обеспечения уверенности в том, что составной ОО будет надежно функционировать, опираясь на функциональные возможности безопасности, обеспечиваемые его ранее оцененными составляющими: ПО, программно-аппаратными или техническими компонентами.

3.2. Вместо класса АСМ «Управление конфигурацией» в рамках класса АLC «Поддержка жизненного цикла» введены семейства АLC_CMC «Возможности управления конфигурацией» и АLC_CMS «Область действия управления конфигурацией».

3.3. Вместо класса АДО «Поставка и ввод в эксплуатацию» в рамках класса АLC «Поддержка жизненного цикла» введено семейство АLC_DEL «Поставка».

3.4. Вместо класса АМА «Поддержка гарантии», предназначенного для решения проблемы поддержки гарантии в ходе эксплуатации ранее оцененного ОО, в рамках семейства АLC_LCD «Определение жизненного цикла» класса АLC «Поддержка жизненного цикла» устанавливаются требования по формированию и независимой экспертной оценке модели жизненного цикла информационной системы (ИС). Данная модель должна охватывать процедуры, инструментальные средства и технологии, используемые для разработки и сопровождения ИС, и, в частности, процедуры контроля изменений и методы тестирования, направленные на поддержку выполнения установленных для ИС функциональных требований безопасности. Модель жизненного цикла зависит от специфики ИС и условий ее функционирования. В силу этого, жесткие требования четкого следования одному определенному стандарту не налагаются, хотя отмечается необходимость учета существующих стандартизованных моделей жизненного цикла, например, типа каскадной модели (модели водопада).

3.5. В состав класса ADV включены новые семейства ADV_ARC «Архитектура безопасности» и ADV_TDS «Проект ОО».

Семейство ADV_ARC «Архитектура безопасности» предназначено для того, чтобы обеспечить надлежащее описание архитектуры функциональных возможностей безопасности ОО. Данное семейство содержит требования к описанию архитектуры безопасности на основе принципов самозащиты, разделения на области и невозможности обхода, включая описание того, как эти принципы поддерживаются теми частями ОО, которые используются для реализации функций безопасности.

Семейство ADV_TDS «Проект ОО» дает материал для всестороннего описания функциональных возможностей безопасности. Если гарантия должна быть увеличена,

то уровень детализации, предоставляемого описания также возрастает. Когда размер и сложность ОО возрастают, целесообразно использовать множество уровней разбиения. В семействе различают разбиения на уровне подсистем и разбиения на уровне модулей. Уровень модулей является наиболее конкретным описанием функциональной возможности – это описание их реализации. Требования к проекту призваны обеспечить такое представление информации, на основании которого можно будет определить выполняются ли функциональные требования безопасности. Требования данного семейства определяют множество подлежащих реализации свойств подсистем и модулей.

3.6. Изменена структура класса AGD «Руководящие документы» – вместо деления на документы типа «Руководство пользователя» и «Руководство администратора», принятого в СТБ 34.101.3-2004, в новой версии СТБ.34.101.3 руководящие документы делятся на руководства по подготовке поставляемого ОО к эксплуатации в соответствии с описанной и оцененной конфигурацией (семейство AGD_PRE «Подготовительные процедуры») и руководства по безопасному использованию ОО в процессе его эксплуатации (семейство AGD_OPE «Руководство пользователя»). Такой подход отражает два важных этапа жизненного цикла ОО (установка и эксплуатация) и позволяет более четко и полно учесть и отразить в документации возникающие на каждом из них проблемы.

4. Претерпел изменения подход к оценке таких свойств безопасности как разбиение на области, самозащита и невозможность обхода политики безопасности. Признано, что по сравнению с проверкой корректности реализации функциональных требований безопасности эти свойства трудно доказуемы и требуют принципиально другого подхода к их проверке. Разница в анализе реализации функциональных требований безопасности и реализации разбиения на области, самозащиты и невозможности обхода состоит в том, что функциональные возможности, связанные с функциональными требованиями безопасности, более или менее четко видны и относительно легко тестируются, в то время как указанные свойства требуют значительно более многоаспектного и сложного анализа функциональных возможностей. Требования и вопросы анализа объекта оценки, связанные с проверкой указанных свойств, приведены в упомянутых выше новых семействах ADV_ARC «Архитектура безопасности», ADV_TDS «Проект ОО» и семействе ADV_INT «Внутренняя структура функций безопасности ОО» из класса ADV «Разработка».

5. Во избежание излишних затрат при рассмотрении объектов, допускающих оценку по первому уровню гарантии оценки (УГО), предусмотрена возможность написания и проведения оценки на основе ограниченных (усеченных) профилей защиты и заданий по безопасности, в которых функциональные требования безопасности устанавливаются разработчиком без предварительного определения предположений, угроз, политик безопасности и соответствующих им задач безопасности.

6. По сравнению с ныне действующей версией из новой версии СТБ.34.101.3 исключены вопросы, связанные с анализом скрытых каналов и оценкой стойкости функций

безопасности. Отсутствует понятие проектов верхнего и нижнего уровней.

7. Для поддержки разных уровней гарантии оценки составных объектов введены три иерархических составных пакета гарантии (СПГ), применяемые к объектам, состоящим из компонентов, которые прошли предварительную покомпонентную оценку. Увеличение гарантии для более высокого уровня СПГ достигается использованием иерархически более высокого компонента из того же семейства гарантии и/или добавлением новых компонентов из других семейств гарантии. СПГ являются необходимым дополнением к уровням гарантии оценки, так как для объединения компонентов ранее оцененных по УГО и получения результирующей гарантии по УГО все гарантийные требования безопасности из УГО необходимо применить к составному ОО. Несмотря на то, что можно повторно использовать результаты оценки компонентов ОО, необходимо учитывать, что в составном ОО для компонентов часто возникают дополнительные характеристики, подлежащие обязательному рассмотрению (например, связанные с интерфейсами между базовым компонентом и зависимым компонентом, на которые опирается зависимый компонент для реализации функциональных возможностей безопасности). Вследствие того, что в оценке составного ОО участвуют различные стороны, обычно невозможно получить все необходимые свидетельства об этих дополнительных характеристиках компонентов для применения соответствующего УГО. С помощью СПГ решается проблема объединения оцененных компонентов и получения на этом пути значимого результата оценки ОО в целом.

8. Существенно изменен состав уровней гарантии оценки, хотя по сравнению с СТБ 34.101.3-2004, общее их количество осталось прежним (семь). В частности, во все УГО включены компоненты класса ASE «Оценка задания по безопасности», что представляется совершенно оправданным, так как процессы испытания и аттестации объекта базируются на проверке требований задания по безопасности, и допущенные при его написании упущения и ошибки могут свести на нет эффективность данных процессов.

9. В целях совершенствования процессов реализации и оценки функциональных возможностей безопасности введены и используются для оценки понятия функциональных возможностей и интерфейсов, осуществляющих функциональные требования безопасности, поддерживающих функциональные требования безопасности и не влияющие на функциональные требования безопасности.

В целом, новая версия стандарта стала более гибкой и предоставляет больше свободы в применении множества методов оценки по отношению к множеству свойств безопасности продуктов ИТ. В такой ситуации субъекту предоставляется больше свободы, но возрастает и его ответственность за неправильное использование указанной гибкости стандарта.

Литература:

1. ISO/IEC 15408-3:2008 Information technology - Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

ОЦЕНКА ЗАДАНИЙ ПО БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ОБНОВЛЕННОЙ РЕДАКЦИЕЙ БАЗОВОГО СТАНДАРТА ОЦЕНКИ БЕЗОПАСНОСТИ

Е.П. Максимович, Т.С. Мартинович,
А.Б. Степанян, В.К. Фисенко,
ОИПИ НАН Беларуси, г. Минск

В докладе рассматривается подход к оценке заданий по безопасности (ЗБ), предлагаемый в новой версии стандарта СТБ 34.101.3-20XX «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий Часть 3. Гарантийные требования безопасности», идентичного по содержанию стандарту ISO/IEC 15408-3:2008 [1]. Обсуждаются изменения, произошедшие по сравнению с прежней версией стандарта СТБ 34.101.3-2004.

Общее назначение процедуры оценки ЗБ не изменилось. Она необходима для демонстрации того, что ЗБ является обоснованным и внутренне непротиворечивым, и, если ЗБ базируется на профилях защиты (ПЗ) или пакетах, то призвана показать, что ЗБ является правильной реализацией данных ПЗ и пакетов. Оценка ЗБ позволяет установить его пригодность для использования в качестве основы при оценке продукта информационных технологий (ИТ).

Изменения в подходе к оценке ЗБ, произошедшие в новой версии стандарта, во многом обусловлены следующими факторами:

а) объектом оценки (ОО) теперь являются продукты ИТ (а не продукты и системы ИТ как СТБ 34.101.3-2004), поэтому в новой версии стандарта рассматриваются только ЗБ, разрабатываемые для продуктов ИТ;

б) в новой версии стандарта ISO/IEC 15408 [1-3] допускается использование упрощенного ЗБ, разработанного по первому уровню гарантии оценки (УГО), для которого по сравнению со стандартным ЗБ определены следующие упрощения:

- не требуется приводить описание проблемы безопасности, формулировать угрозы, политики и предположения безопасности;

- не требуется излагать задачи безопасности для ОО. Но при этом задачи безопасности для среды функционирования должны быть изложены;

- не требуется приводить обоснование задач безопасности, поскольку в ЗБ не приводится описание проблемы безопасности;

- в обосновании требований безопасности необходимо привести только обоснование неудовлетворения зависимостей, поскольку в ЗБ не приводятся задачи безопасности для ОО;

в) новая версия стандарта стала более гибкой и предоставляет разработчику и эксперту большую свободу действий. Подчеркивается, что хотя обеспечение гарантии безопасности по-прежнему базируется на экспертном оценивании (активном исследовании) качества сопровождающих документов и самого ОО, стандарт не исключает и не комментирует эффективность других мер гарантии, признавая актуальность исследований

в области поиска новых альтернативных путей обеспечения гарантии;

г) исключено из рассмотрения понятие стойкости функций безопасности, что позволяет исключить из рассмотрения соответствующие экспертные проверки.

Анализ требований класса ASE «Оценка задания по безопасности» позволил выявить следующие основные изменения, произошедшие в новой версии СТБ 34.101.3 по сравнению с ныне действующей версией.

1. Набор семейств, входящих в состав класса, принципиальных изменений не претерпел, скорее изменились сформулированные в них требования безопасности. В частности, в классе ASE «Оценка задания по безопасности» СТБ 34.101.3-2004 все семейства содержат по одному компоненту, а в новом стандарте семейства ASE_OBJ «Задачи безопасности», ASE_REQ «Требования безопасности» и ASE_TSS «Общая спецификация объекта оценки» содержат по два иерархических компонента, нижний из которых содержит требования к разработке и оценке упрощенного ЗБ, а иерархичный ему – требования к разработке и оценке стандартного ЗБ.

2. По сравнению с СТБ 34.101.3-2004 в новой версии СТБ 34.101.3 отсутствует семейство ASE_DES, включающее требования к оценке качества описания объекта оценки (ОО). Однако данное изменение является принципиальным и, по сути, не изменяет состав работ по оценке ЗБ. В новой версии СТБ 34.101.3 соответствующие требования к экспертной оценке сформулированы в рамках семейства ASE_INT «Введение в задание по безопасности», что обусловлено тем, что в соответствии с новыми требованиями к ЗБ описание ОО входит в состав введения (введение должно включать описание ОО на трех, не противоречащих друг другу, уровнях: идентификация ОО, обзор ОО и описание ОО).

3. В новой версии СТБ 34.101.3 семейство ASE_ENV «Задание по безопасности, среда безопасности» из СТБ 34.101.3-2004 заменено семейством ASE_SPD «Определение проблемы безопасности». Как и прежде, эксперт должен оценить предоставляемое разработчиком описание угроз, политики и предположений безопасности. По сравнению с СТБ 34.101.3-2004 особо подчеркивается, что описания угроз, политик и предположений должны быть представлены в составе определения проблемы безопасности, которая должна быть решена ОО и средой его функционирования. Требуется, чтобы все угрозы были описаны в терминах нарушителя, активов и метода атаки.

Отмечается, что для физически распределенного ОО может быть предпочтительным определение угроз, политик безопасности и предположений отдельно для каждой области (домена) среды функционирования ОО.

4. В новой версии СТБ 34.101.3 семейство ASE_PPC «Задание по безопасности, соответствие профилю защиты» из СТБ 34.101.3-2004 заменено более широким семейством ASE_CCL «Утверждение о соответствии». В частности, предъявляются требования к предоставлению утверждений о соответствии ПЗ, требования к описанию и проверке соответствия ЗБ стандарту СТБ.34.101.2 либо расширению по отношению к СТБ.34.101.2, стандарту СТБ.34.101.3 либо расширению по отношению к нему с указанием версии стандарта, относительно которой провозглашается соответствие ЗБ и ОО. Утверждение о соответствии СТБ.34.101 должно согласовываться с определением дополнительных требований.

Обоснование утверждения о соответствии должно демонстрировать, что определение проблемы безопасности, формулировка задач и требований безопасности согласуются с соответствующими определениями и формулировками в профилях защиты, относительно которых объявляется соответствие.

5. В семействе ASE_OBJ «Задачи безопасности» компоненты упорядочены, исходя из того, установлены ли задачи безопасности только для среды или же и для среды, и для ОО. Для упрощенного ЗБ в новой версии СТБ 34.101.3 допускается возможность определения разработчиком только задач безопасности для среды, причем предоставление их обоснования (т.е. сопоставления задач безопасности с угрозами, политиками безопасности либо предположениями) не требуется. В остальных случаях в ЗБ требуется четкое разделение проблемы безопасности между задачами безопасности для ОО и для среды и требуется обосновать задачи путем демонстрации того, что они противостоят всем угрозам безопасности, реализуют все политики безопасности и обеспечивают выполнение всех предположений безопасности.

6. В семействе ASE_REQ «Требования безопасности» компоненты упорядочены, исходя из того, установлены ли требования безопасности сами по себе или получены из задач безопасности для ОО. Компонент ASE_REQ.1 используется только для упрощенных ЗБ и не требует от разработчика ЗБ обоснования соответствия между задачами безопасности и требованиями безопасности. В остальных случаях ЗБ должно содержать сопоставление каждого функционального требования безопасности задачам безопасности для ОО и демонстрировать, что функциональные требования безопасности обеспечивают выполнение всех задач безопасности для ОО. Требуется также оценить качество обоснования выбора гарантийных требований безопасности. Каких-либо конкретных требований к обоснованию не предъявляется, оно просто должно обеспечить пользователям ЗБ понимание причины выбора конкретной совокупности ГТБ. Как и в ныне действующей версии стандарта, необходимо проверять непротиворечивость требований друг другу. Требование из СТБ 34.101.3-2004 о том, что формулировки гарантийных требований безопасности ОО должны включать УГО, из новой версии исключено. Исключены также требования о необходимости идентификации требований безопасности для среды ИТ и требования, связанные со стойкостью.

7. В семействе ASE_TSS «Общая спецификация ОО» компоненты упорядочены, исходя из того, нужна ли

общая спецификация только для описания того, как ОО обеспечивает выполнение функциональных требований безопасности, или также еще для описания того, как ОО защищается от логических злонамеренных действий и обхода средств безопасности. Это дополнительное описание может быть использовано в случае, когда возникают вопросы относительно архитектуры безопасности ОО. В каждом из компонентов налагается требование проверки непротиворечивости общей спецификации обзору и описанию ОО.

Примечание. В новой версии стандарта такие свойства безопасности как разбиение на области, самозащита и невозможность обхода политики безопасности рассматриваются отдельно от функциональных требований безопасности вследствие того, что они трудно проверяемы и требуют особого многоаспектного и сложного анализа функциональных возможностей на уровне архитектуры средств безопасности и проекта ОО.

В отличие от СТБ 34.101.3-2004 в новых требованиях семейства ASE_TSS отсутствует упоминание мер гарантии, в частности, требование сопоставления мер гарантии с гарантийными требованиями так, чтобы можно было видеть, какими мерами гарантии реализуются гарантийные требования, а также требование демонстрации того, что меры гарантии отвечают всем гарантийным требованиям ОО.

Отсутствуют требования, связанные со стойкостью.

8. Семейство ASE_SRE «Задание по безопасности, дополнительные требования безопасности информационных технологий» из СТБ 34.101.3-2004 заменено семейством ASE_ECD «Определение дополнительных компонентов». Требуется, чтобы было обеспечено определение дополнительного компонента для каждого дополнительного требования безопасности. Определение дополнительных компонентов должно описывать, каким образом каждый дополнительный компонент соотносится с существующими компонентами, семействами и классами СТБ 34.101.

Ряд полезных рекомендаций, которые можно использовать при реализации и оценке ЗБ в соответствии с требованиями класса ASE, приведен в Приложениях в новой версии СТБ 34.101.1.

Более подробно процесс оценки ЗБ в соответствии с новой версией СТБ 34.101.1-3 предполагается рассмотреть в подлежащей разработке новой версии стандарта СТБ 34.101.5-20XX «Информационные технологии и безопасность. Методология оценки безопасности информационных технологий», идентичного по содержанию ISO/IEC 18045:2008 [4].

Литература:

1. ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.
2. ISO/IEC 15408-3:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
3. ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.
4. ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation.

АНАЛИЗ ТЕРМОГРАММ ФУНКЦИОНАЛЬНЫХ УЗЛОВ АППАРАТУРЫ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В.И. Воробьев, Г.В. Давыдов, П.П. Мазур,
БГУИР,

Оперативно-аналитический центр при Президенте Республики Беларусь

Тепловое рассеяние современной аппаратуры вычислительной техники характеризуется значительными мощностями. В этих условиях профилактическое обследование тепловых режимов работы отдельных ее устройств, неожиданный выход из строя которых может привести к серьезным последствиям в основном оборудовании и привести к недопустимым потерям информации, становится важным средством комплексной защиты информации в целом.

Одним из наиболее перспективных методов исследования тепловых полей устройств вычислительной техники является их бесконтактный термографический контроль [1]. В докладе рассмотрены некоторые основные методические и технические вопросы диагностики функциональных узлов и устройств вычислительной техники на основе обработки и анализа их термограмм, получаемых с помощью современных тепловизоров.

Современные тепловизоры [2,3] обеспечивают высокую точность измерений температуры и разрешающую способность по угловым координатам, позволяющие получать детальное отображение температурных различий у элементов наблюдаемого объекта. Однако необходимая степень детализации отображения теплового поля при формировании анализируемого в ПЭВМ изображения требует корректного обоснования.

По оценкам лаборатории технического контроля фирмы ИБМ, «для полной уверенности, что все компоненты изделия работают в пределах допусков, предусмотренных их спецификациями, требуется измерение температуры с точностью до 1 К» [1,4].

Полностью автоматизировать процессы получения и анализа термограмм пока не удается, и принятие окончательных решений приходится возлагать на оператора. Форму и содержание графических данных, представляемых оператору в результате обработки термограмм, требуется согласовывать с особенностью восприятия и осмысления изображений человеком. Поэтому рациональное устранение избыточности и обеспечение наглядности таких изображений приобретают большую важность.

Необходимо, по возможности автоматически, компенсировать детерминированные помехи, обеспечивать четкость и лаконичность машинной графики. В частности, весьма продуктивным представляется использование изображений температурных рельефов и наборов изотерм исследуемых термограмм [1].

В [1] анализ рельефа распределения температуры по поверхности платы ЭВМ ЕС-1060 в установившемся тепловом режиме позволил определить элементы с максимальным тепловыделением, оценить эффективность выбранной системы охлаждения, выявить наличие дефектов в электрических цепях.

Полезную ориентацию в поиске средств обработки термограмм дает и приведенный в [1] перечень разрабо-

танных и использованных авторами прикладных программ для контрастирования; выделения контуров; подчеркивания контуров; видоизменения гистограммы; фильтрации изображений; выполнения арифметических операций над изображениями; геометрических преобразований изображений; удаления шума и др.

Современные пакеты компьютерной обработки цифровых изображений предоставляют самые широкие возможности при разработке средств решения задач, подобных перечисленным. Так, программное средство MATLAB содержит объемный специальный пакет Image Processing Toolbox (IPT) средств цифровой обработки изображений [5]. Многие программы этого пакета допускают адаптацию под конкретные задачи пользователя.

На рисунке 1 для иллюстрации возможностей устранения избыточности термограмм представлен пример преобразования в среде MATLAB снимка, выполненного тепловизором типа FLIR T640bx и переданного в компьютер в формате JPEG.

Приведенная сглаженная термограмма наглядно представляет оператору картину теплоизлучения анализируемого устройства. Однако для обеспечения видимого качества этой картины требуется весьма основательный ресурс компьютерной системы цифровой обработки изображений. На практике требуется использовать лишь необходимые и достаточные ресурсы компьютерной системы цифровой обработки термограмм.

На рисунке 2 иллюстрируются два способа дополнительного устранения избыточности термограммы, помещенной на рисунке 1.

Взаимно дополняющие друг друга рисунки 2(а) и 2(б) представляют рельеф (а) и изотермы (б) указанной термограммы. Преобразование термограммы выполнено с

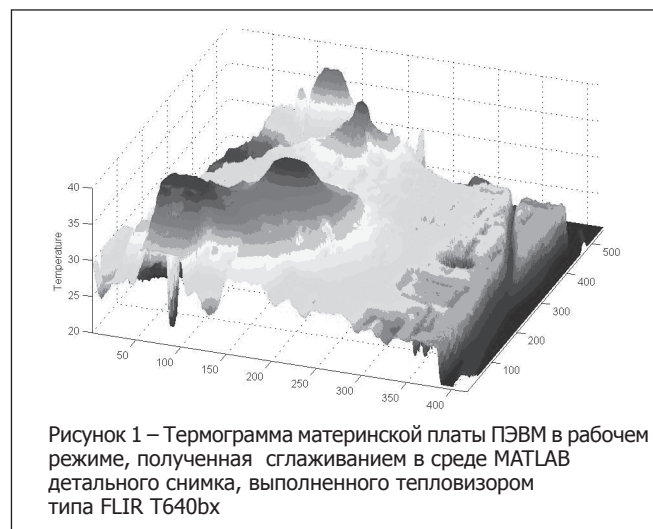
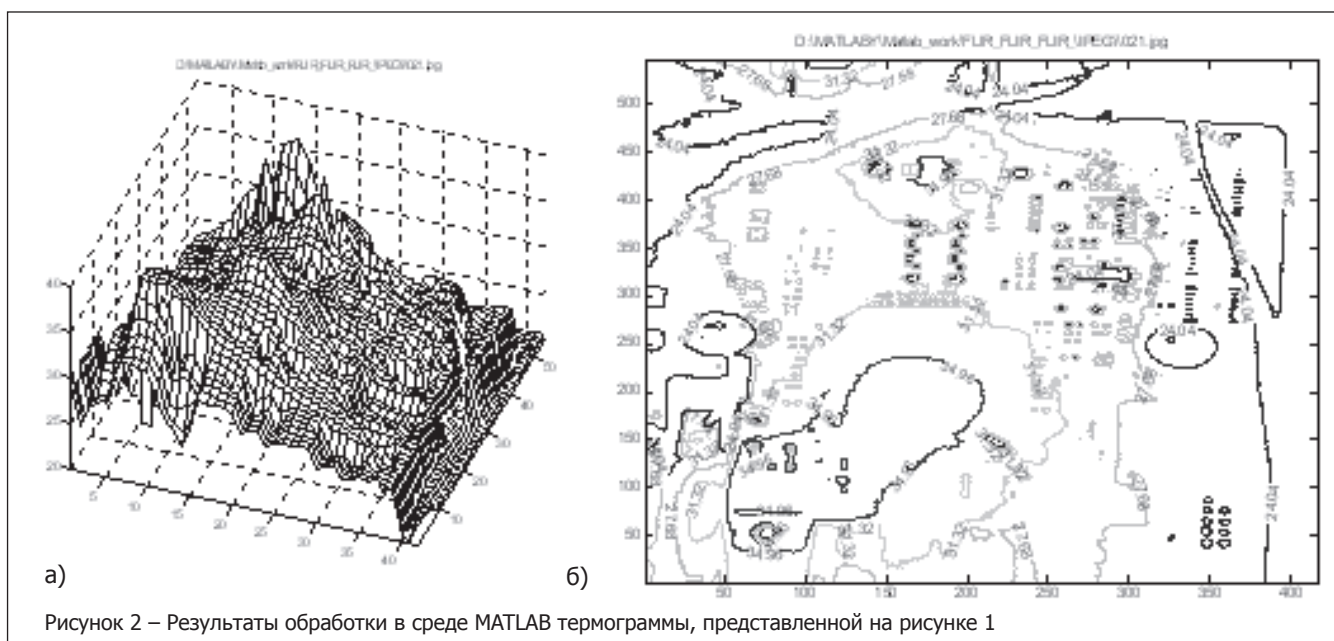


Рисунок 1 – Термограмма материнской платы ПЭВМ в рабочем режиме, полученная сглаживанием в среде MATLAB детального снимка, выполненного тепловизором типа FLIR T640bx



помощью программы, вновь написанной на языке среды MATLAB.

Количество выводимых изотерм, исследуемый температурный диапазон и подробность графического представления распределения температур в виде рельефа целесообразно определять в соответствии с конкретными задачами проводимого анализа.

Определенно перспективным является и создание аппаратных средств цифровой обработки термограмм в виде платы расширения используемых компьютеров.

Продуктивность такого подхода убедительно продемонстрирована в [6–8]. Представленный [6,7] кадровый видеопроцессор KBП-2003, конструктивно выполненный в виде платы расширения ПЭВМ типа IBM PC, в комплексе измерительной аппаратуры обеспечивает решение следующих задач анализа растровых изображений: обнаружение малоразмерных изображений объектов на фоне шумов и помех с использованием операций накопления и межкадровой разности; формирование бинарного изображения с фиксированным пороговым уровнем; сегментацию бинарного изображения; разделение пространственно-связанных локальных объектов; автоматическое измерение габаритных размеров и селекцию по ним обнаруженных объектов; измерение координат геометрического центра и центра тяжести изображения выделенного объекта.

Изложенное целесообразно кратко резюмировать следующим образом.

Современные цифровые тепловизоры обеспечивают весьма высокое качество термограмм. При решении практических задач их анализа приходится устранять избыточность изображений.

Эффективными способами устранения избыточности изображений, представляемых оператору в результате цифровой обработки термограмм, являются машинные графические построения их рельефов и изотерм.

Для разработки алгоритмов решения каждой конкретной технической задачи требуются учет специфики

основных механизмов формирования регистрируемого тепловизором теплового поля и изучение его статистических характеристик.

Важнейшее значение приобретает поиск рационального распределения функций между аппаратурой извлечения тепловизионной информации и средствами ее обработки.

Перспективным следует считать применение встраиваемых цифровых устройств и создание аппаратных средств цифровой обработки термограмм в виде платы расширения используемых компьютеров.

Многие задачи анализа термограмм целесообразно решать на универсальных ПЭВМ с использованием среды MATLAB.

Литература:

1. Драгун, В.Л., Филатов, С.А. Тепловизионные системы в исследованиях тепловых процессов. – Минск: Наука и техника, 1989. – 175 с.
2. IRTIS -2000 C // [Электронный ресурс]. 2013 Режим доступа: http://www.security.ukrnet.net/d-book-2/ch_10.pdf. Дата доступа: 10.01.2013.
3. FLIR Sistem // [Электронный ресурс]. 2013 Режим доступа: <http://www.flir.com>. Дата доступа: 10.01.2013.
4. Форд Ф. Термографический контроль – неотъемлемая часть обеспечения качества на заводе «ИБМ» в Хаванте // Infrared Observer. – 1987. – № 14.
5. Гонсалес, Р. Цифровая обработка изображений в среде MATLAB / Гонсалес Р., Вуд Р., Эддинс С. – М.: Москва: Техносфера, 2006. – 616 с.
6. Сальников, И.И. Анализ пространственно-временных параметров удаленных объектов в информационных технических системах. – М.: ФИЗМАТЛИТ, 2011. – 252 с.
7. Сальников И.И., Кутаев Ю.Ф., Абачкин С.Н. Устройство для селекции изображений и измерения размеров объекта. Патент на изобретение № 2163395 от 20.02.2001 г.
8. Иванюк, А.А. Проектирование встраиваемых цифровых устройств и систем: монография / А.А. Иванюк. – Минск: Бестпринт, 2012. – 337 с.

ПАСТООБРАЗНЫЕ ЭКРАНИРУЮЩИЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ СМЕСИ НА ОСНОВЕ ШУНГИТА

Е.С. Белоусова, М.Ш. Махмуд, Л.М. Лыньков,
БГУИР, г. Минск

Весьма распространенным строительным материалом, используемым для создания элементов конструкций, является гипсовый алебастр, который представляет собой порошкообразный вяжущий материал, получаемый путем термической обработки природного двухводного гипса $\text{CaSO}_4 \cdot 2\text{H}_2\text{O}$ при температуре 150–180 градусов в аппаратах, сообщающихся с атмосферой, до превращения его в полуводный гипс $\text{CaSO}_4 \cdot 0,5\text{H}_2\text{O}$ – гипс β -модификации. По большей части его применяют в различных ремонтных и строительных процессах. При помощи алебаstra можно легко выровнять неровности на стенах и потолке.

Для исследований были изготовлены образцы экранов электромагнитного излучения (ЭМИ) в виде плиток толщиной от 3 до 5 мм из смеси 45%-раствора CaCl_2 (30%) с добавлением порошкообразных компонентов – шунгита (35%) и гипсового алебаstra (35) (рисунок 1).

Сроки схватывания гипса зависят от свойств сырья, технологии изготовления, длительности хранения, количества вводимой воды, температуры вяжущего вещества и воды, условий перемешивания, наличия добавок и др.

В смеси с водой гипсовый порошок быстро твердеет (20... 60 мин), превращаясь в двухводный гипс, но при добавлении более 25 % водного раствора CaCl_2 сохраняет пастообразное состояние. Шунгит обладает высокой механической прочностью и электропроводностью, способностью к взаимодействию со всеми связующими обеспечивают получение строительных материалов с электропроводными свойствами, способных экранировать электромагнитные излучения высоких частот.

Для измерения экранирующих характеристик использовался панорамный измеритель ослабления и КСВН Я2Р-67 с ГКЧ-61 и волноводным трактом. Коэффициент отражения был получен на основании пересчета из КСВН по стандартной методике [1]. Измерения характеристик ослабления и отражения ЭМИ образцами производили для диапазона частот 8...12 ГГц

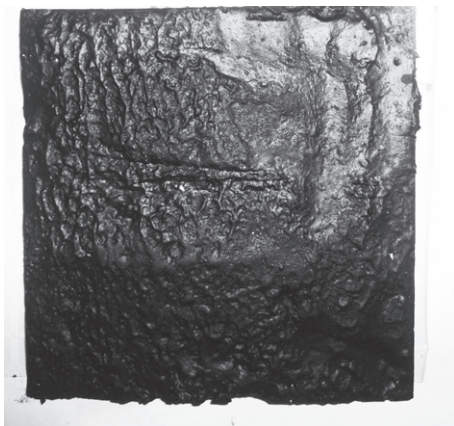


Рисунок 1 – Внешний вид образца на основе пастообразной шунгитовой смеси

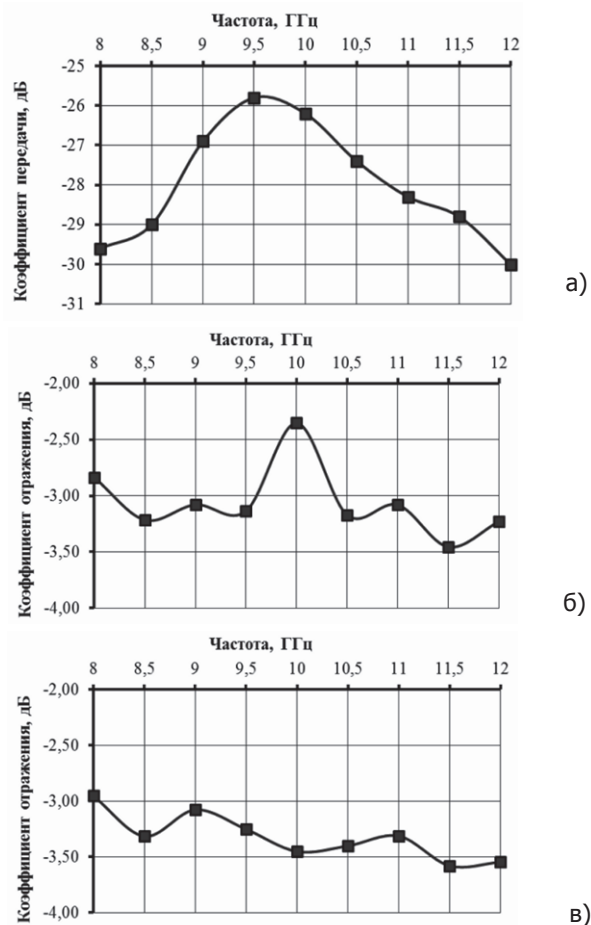


Рисунок 2 – Частотная зависимость экранирующих характеристик пастообразной смеси на основе шунгита в диапазоне частот 8...12 ГГц: коэффициент передачи (а), коэффициент отражения без металлического отражателя (б) и с металлическим отражателем (в)

Как видно из рисунка 2, коэффициент передачи составляет –26... –30 дБ в исследуемом диапазоне с максимумом –26 дБ на частоте 9,5 дБ. Коэффициент отражения при измерениях без металлического отражателя составляет в среднем –3 дБ, при использовании металлического отражателя –3... –3,5 дБ.

Таким образом, полученная пастообразная смесь на основе шунгита, обладает хорошими экранирующими характеристиками (коэффициент отражения –3 дБ, коэффициент передачи –26 дБ) и может быть использована в качестве декоративного покрытия любых поверхностей.

Литература:

1. Криштопова, Е.А. Влияние свойств выбранного связующего на эффективность поглотителей ЭМИ, изготовленных из порошкообразного шунгита / Е.А. Криштопова, Л.М. Лыньков, Т.В. Борботько // Доклады БГУИР. – 2007. №6. – С. 3-8.

КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ ПРИЕМА/ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ С USB-ИНТЕРФЕЙСОМ

УДК 004.312

Г.Ф. Астапенко, П.В. Кучинский, Н.А. Раценя,
НИИ ПФП им. А.Н. Севченко БГУ, г. Минск

Приведены данные по разрабатываемому автономному криптографическому модулю приема и передачи данных, который позволяет хранить ключи и критические данные во внутренней смарт-карте типа simblock, передавать и принимать данные как по проводной Ethernet сети, так и беспроводной IEEE 802.11 (Wi-Fi) сети, взаимодействовать с хост-компьютером через интерфейс USB 2.0.

На данный момент, для передачи и хранения конфиденциальной информации широко используется инфраструктура компьютерных систем и сетей. На информационном рынке предлагается широкий спектр услуг в виде аппаратно-программных надстроек в виде виртуальных частных сетей, туннелирования, использования стандартизованных протоколов MACsec, Ipsec, SSL/TLS, HTTPs. Однако эти продукты не всегда обеспечивают необходимый уровень безопасности, имеют экспортные ограничения, не адаптированы для использования отечественных стандартов шифрования, цифровой подписи и распределения ключей. К тому же на практике часто возникают потребности в автономных аппаратно-программных модулях, которые бы легко встраивались в существующие открытые компьютерные и сетевые инфраструктуры и могли бы стать мобильными, безопасными инструментами хранения и передачи конфиденциальных данных.

Нами разрабатывается автономный аппаратно-программный криптографический модуль, который обеспечивает:

- аппаратные функции шифрования, хэширования, формирования электронной цифровой подписи согласно соответствующим отечественным стандартам;
- хранение конфиденциальных ключей и критических данных на персональной смарт-карте (форм-фактор – simblock);
- передачу конфиденциальных данных в сети Ethernet по IPsec-туннелю между двумя абонентами, использующими данный модуль;
- передачу конфиденциальных данных в сети IEEE 802.11 b/g (WiFi) с использованием технологии IEEE 802.11i (MAC расширения безопасности);
- взаимодействие с хост-компьютером по открытому USB-2.0 интерфейсу.

Таблица 1 – Технические характеристики модуля «Икар»

Технические характеристики	Тип модуля	
	«Икар-2Е»	«Икар-2W»
Тип микроконтроллера	Stellaris LM3S9997 [1]	Stellaris LM3S9D96 [2]
Тактовая частота (МГц)	80	80
Объем флэш-памяти (Кбайт)	256	512
Объем памяти ОЗУ (Кбайт)	64	96
Интерфейс взаимодействия со смарт-картой (типа simblock)	ISO 7816-2,3 и 4	ISO 7816-2,3 и 4
Интерфейс взаимодействия с хост-компьютером (USB 2.0)	Скорость передачи – до 12 Мбит/с	Скорость передачи – до 12 Мбит/с
Интерфейс взаимодействия с внешней картой типа microSD	Объем памяти – 1–2 Гб	Объем памяти – 1–2 Гб
Коммуникационный сетевой интерфейс Ethernet MAC+PHY	Скорость передачи – 10/100 Мбит/с	
Беспроводной интерфейс WLAN (IEEE 802.11 b/g)		Скорость передачи – до 54 Мбит/с

Модуль разрабатывается в двух модификациях – «Икар-2Е» и «Икар-2W». Технические характеристики модулей представлены в таблице 1. Структурная схема модуля «Икар-2» представлена на рисунке 1.

В состав программного обеспечения модуля «Икар-2Е»/«Икар-2W» входят следующие компоненты:

ВПО микроконтроллеров серии Stellaris LM3S*, состоящее из следующих модулей:

- инициализации и тестирования;
- диспетчера взаимодействия с хост-компьютером;
- обеспечения USB-взаимодействия по обмену данными;
- программное обеспечение сетевого Ethernet взаимодействия на основе стека TCP/IP (с элементами протокола IPsec);
- программное обеспечение беспроводного взаимодействия в соответствии с технологией IEEE 801.11 b/g/i (с элементами протокола WPA-2(EAP));
- обеспечения взаимодействия с внешней картой памяти microSD;
- обеспечения взаимодействия со смарт-картой в соответствии со стандартом IEEE-7816-3 и IEEE-7816-4;
- симметричного шифрования данных по ГОСТ 28147-89 и СТБ 34.101.31 2011;

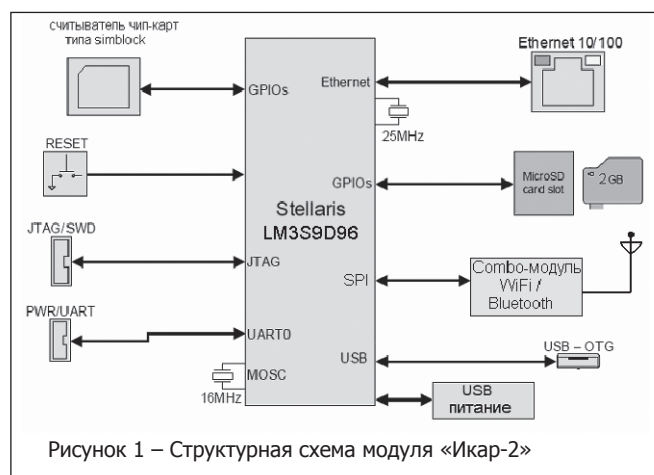


Рисунок 1 – Структурная схема модуля «Икар-2»

– вычисления хэш-функции по ГОСТ Р 34.11-94 и СТБ 34.101.31 2011 (функция хэширования);

– вычисления электронной цифровой подписи по ГОСТ Р 34.10-2001, а также вычисления цифровой подписи и обеспечения функции транспорта ключей по СТБ П 34.101.45-2011;

– встроенное фирменное программное обеспечение StellarisWare с возможностью его перепрограммирования со стороны хост-компьютера через USB интерфейс;

– драйвер и библиотека StellarisWare, обеспечивающие программный интерфейс взаимодействия с устройством со стороны хост-компьютера;

– прикладная программа icar_mod.exe, обеспечивающая тестирование и основные функции взаимодействия и обработки открытых и конфиденциальных данных.

Разрабатываемый модуль обеспечит:

– скорость шифрования данных по ГОСТ 28147-89 в режиме гаммирования без обмена с хост-компьютером – не менее 800 кбайт/с;

– скорость шифрования данных по ГОСТ 28147-89 в режиме гаммирования при обмене данными с хост-компьютером – не менее 600 кбайт/с;

– время формирования цифровой подписи при объеме блока данных 1 Кбайт – не более 2 сек;

– время вычисления хэш-функции при объеме данных 400 Кбайт – не более 4 сек.

Разрабатываемый модуль обеспечит защиту информации в распределенных проводных и/или беспроводных информационно-коммуникационных системах.

Литература:

1. Stellaris LM3S9997 Microcontroller. Datasheet. – Texas Instruments Incorporated, 2011. – 1328 p.

2. Stellaris LM3S9D96 Microcontroller. Datasheet. – Texas Instruments Incorporated, 2012. – 1408 p.

Abstract

The description of autonomous unit, designed in Institute of Applied Physical Problems of name A.N.Sevchenko BSU, is given in this work. The unit allows storing cryptographic keys and critical data in internal smart card such as simblock, to transmit data on the Ethernet network and wireless local area networks (IEEE 802.11 b/g-compliant), to interact with host-computer through the interface USB 2.0.

ПОВЫШЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОМ ПАРКЕ ВУЗА ЗА СЧЕТ БУФЕРИЗАЦИИ И ИЗОЛЯЦИИ РЕСУРСОВ

П.С. Пойта, Д.А. Костюк, С.С. Дереченник, П.Н. Луцюк,
БрГТУ, г. Брест

Одной из проблем, сопутствующих развитию современного учебного заведения, как и любой иной крупной организации, является обеспечение работоспособности инфраструктуры внутреннего информационного пространства, объединяющего вычислительные ресурсы подразделений. Решения, обеспечивающие функционирование локальной вычислительной сети (ЛВС), должны выполнять защиту данных и программного обеспечения (ПО) от внешних и внутренних угроз. Централизованное администрирование компьютерного парка и общий набор накладываемых на пользователей ограничений, однако, часто не распространяется на подсети кафедр компьютерного профиля, например, взамен дополнительных мер контроля сетевого трафика на шлюзах, соединяющих их с основной ЛВС. Это обусловлено требованиями учебного процесса, т. к. в рамках ряда дисциплин, изучаемых специалистами компьютерного профиля, требуется предоставить студентам более полный доступ к аппаратной подсистеме рабочих станций [1, 4]. Данные кафедры обычно используют свой набор средств защиты – как существующих для нужд учебного процесса (например, практическое изучение средств «Аккорд NT/2000», «Аккорд – РАУ» и «Шипка-1.6», переданных Брестскому государственному техническому университету (БрГТУ) ОКБ «САПР» и Всероссийским НИИ проблем вычислительной техники и информатизации в рамках Соглашения о научно-техническом сотрудничестве [1]), так и разработанных сотрудниками кафедр в рамках исследовательских проектов в сфере информационной безопасности. Последний аспект

обеспечивает площадку для тестирования инновационных подходов перед их возможным внедрением в ЛВС вуза.

Ниже, нами рассмотрен один из таких подходов, направленный на прозрачное усиление безопасности данных и снижение возможного ущерба от активности вредоносного кода, разработанный и примененный кафедрой электронных вычислительных машин и систем БрГТУ.

Сервисы (службы), предоставляемые пользователям в рамках подсети ЛВС БрГТУ, принадлежащей данной кафедре, включают:

- аутентификацию пользователей для работы в сети;
- функции файл-сервера (хранение личных файлов пользователей на персональных сетевых дисках, а также предоставление централизованного сетевого доступа к методическим материалам и ряду программных продуктов);
- обмен трафиком TCP/IP с внешней частью ЛВС (включая опосредованный доступ к ресурсам сети Интернет).

Основные роли пользователей сегмента сети – это студенты, преподаватели и учебно-вспомогательный персонал. Соответственно, защита сегмента ЛВС в рамках обеспечения учебного процесса и предоставления пользователям перечисленных сервисов, в свою очередь, подразделяется на следующие категории:

- физическая защита аппаратных средств;
- защита от вредоносной активности со стороны пользователей;
- резервное копирование системных и прикладных данных.

Физическая защита обеспечивается использованием отдельных помещений с ограниченным доступом для размещения коммутационных узлов сети и серверов. Авторизация пользователей в сегменте ЛВС кафедры выполняется сервером под управлением GNU/Linux, предоставляющим LDAP-базу пользовательских учетных записей (этот же сервер предоставляет доступ к сетевым дискам по протоколу CIFS), что является типичным для белорусских вузов [2]. Защита от возможной вредоносной активности пользователей выполняется заданием прав доступа, как на рабочих станциях, так и на сетевом разделе с методическими и демонстрационными материалами. Однако, в ряде случаев, пользователям необходимы повышенные привилегии. Помимо собственно администрирования компьютерного парка, в рамках сегмента сети кафедры таких задач две:

1. Предоставление преподавательскому составу возможности простой модификации раздела файл-сервера с методическими материалами и программным обеспечением;
2. Предоставление студентам более полного набора прав доступа к рабочей станции при изучении отдельных дисциплин [3].

В первом случае от файл-сервера требуется обеспечить права на запись и модификацию файлов без риска их повреждения. Во втором случае необходимо ослабить защиту рабочей станции, частично изолированной от окружающей среды, с последующей быстрой отменой сделанных изменений и возвращением системы к исходному состоянию.

Особенность первой задачи в том, что классическая защита с помощью антивирусного ПО не может полностью решить проблему. Преподавательскому составу периодически требуются права для модификации файлов на разделе файл-сервера с методическими материалами и ПО. Однако эти модификации могут иметь негативные последствия в случае доступа к серверу с зараженного компьютера (например, персонального ноутбука), на котором антивирусный контроль либо отсутствует, либо не справляется со своей работой, из-за чего вредоносное ПО, получив доступ к сетевым дискам, может подменять на них исходные файлы. Установленный на файл-сервере антивирусный монитор заблокирует доступ к зараженному файлу, предотвратив его дальнейшее распространение. Однако файл может ока-

заться недоступным до вмешательства системного администратора: во-первых, возможность «лечения» зараженных файлов имеют не все антивирусные системы и не для всех разновидностей заражения, а во-вторых, специфика механизма «лечения» не может гарантировать идентичность восстановленного файла исходному.

Для решения этой проблемы нами использована схема, показанная на рисунке 1-а. Помимо основного сетевого ресурса, содержащего методические материалы и ПО, в ЛВС доступен дополнительный ресурс, связанный с буферной файловой системой, имеющей специфический набор прав доступа: в ней запрещена модификация файлов, а доступны только их создание и удаление (причем удаление по умолчанию не уничтожает файл или каталог, а переносит объекты в «корзину»). Оба сетевых ресурса (основной и буферный) предоставляются рабочим станциям с помощью пакета Samba версии 3.x. Содержимое буфера анализируется антивирусным монитором (в качестве которого, например, может выступать ClamAV) и в случае обнаружения вредоносных свойств блокируется. Затем незаблокированные файлы средствами монитора Lsyncd автоматически переносятся на основной раздел файл-сервера, сетевой доступ к которому предоставляется только на чтение, независимо от привилегий пользователя. Помимо очевидной защиты данных от заражения, буферный ресурс одновременно играет роль хранилища резервных копий.

Вторая задача решалась нами с помощью средств виртуализации. ОС от Microsoft, которые помещались на рабочих станциях в изолированные окружения (рисунок 1-б). Особенности типичного офисного оборудования (в первую очередь, отсутствие аппаратной поддержки виртуализации в дешевых процессорах) оставляет систему виртуализации Oracle VirtualBox в качестве единственного решения приемлемой производительности, не требующего оплаты лицензий и обладающего к тому же открытым исходным кодом. По сходной причине в качестве хост-системы выбрана ОС GNU/Linux [1].

Сеть гостевой системы настроена в режиме трансляции адресов. Результатом является недоступность гостевой ОС извне при сохранении комфортного доступа из нее к сетевым сервисам – так же, как это происходит с рабочими станциями

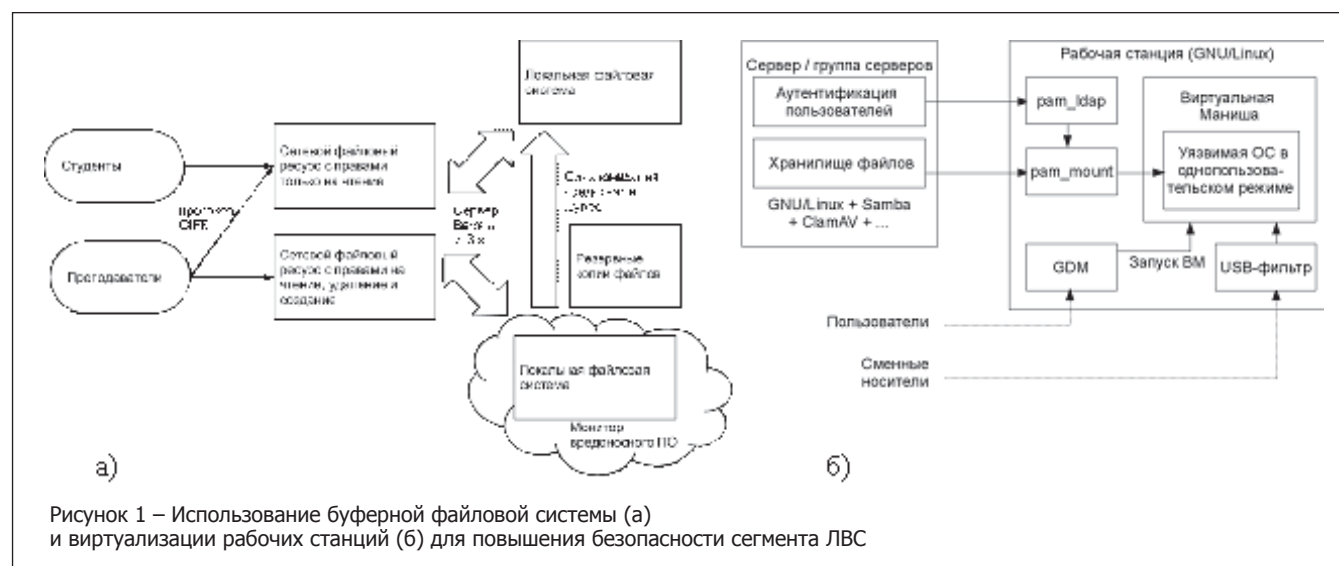


Рисунок 1 – Использование буферной файловой системы (а) и виртуализации рабочих станций (б) для повышения безопасности сегмента ЛВС

локальной сети, имеющими только локальные сетевые адреса и соединяющимися с внешней сетью проху-сервером.

Хост-системы рабочих станций, работающие под управлением GNU/Linux, получают доступ к учетным записям и персональным файлам пользователя на файл-серверах сети с помощью стандартных модулей системы аутентификации Linux LDAP. При этом рабочие станции различаются только IP-адресом и имеют идентичный дисковый образ, что выгодно отличается от решения с ОС от Microsoft, работающей под управлением контроллера домена [3, 4]. Для обеспечения прозрачного доступа к виртуализованному окружению, полноэкранный запуск нужной виртуальной машины включен в список доступных графических оболочек на хост-системе и выбирается пользователем при вводе логина и пароля в менеджере сеансов GDM. Каталоги файл-сервера однотипно монтируются в файловую систему рабочей станции как при входе пользователя в гостевое окружение, так и при входе в графическую оболочку на хост-системе: гостевая система работает в однопользовательском режиме, автоматически (через механизм разделяемых папок VirtualBox) монтируя при запуске каталоги хост-системы, уже отображающие соответствующие конкретному пользователю сетевые ресурсы. Так выполняется изоляция гостевой ОС от внешней сетевой активности и делегирование аутентификации хост-системе.

Дисковый образ гостевой ОС при завершении сеанса работы автоматически откатывается к исходному состоянию (его фиксация выполняется функцией «immutable disk image» VirtualBox). Гостевое окружение благодаря этому становится «неповреждаемым», что позволяет безопасно работать в нем с правами администратора.

При необходимости автоматизировать передачу USB-накопителей в гостевое окружение, проброс может

автоматически выполняться VirtualBox, для чего необходимо создание соответствующего фильтра устройств в настройках. Фильтрация USB-устройств позволяет в ряде случаев обеспечить дополнительную безопасность гостевой системы: например, может быть разрешен только проброс аппаратных ключей защиты, с игнорированием накопителей и других устройств, подсоединяемых к USB-разъемам.

Литература:

1. Д.А. Костюк, С.С. Дереченник. Построение прозрачных виртуализованных окружений для изоляции уязвимых программных систем // Комплексная защита информации: матер. XVI научно-практич. конф., Гродно, 17-20 мая 2011 г. Гродно, 2011. – С. 209-212.

2. S.S. Derechennik, D.A. Kostiuk, D.A. Pynkin. Free/libre software usage in the Belarusian system of higher education institutions // Друга міжнародна науково-практична конференція FOSS Lviv 2012: Збірник наукових праць, Львів, 26–28 квітня 2012 р. Львів, 2012. – С. 62–65.

3. П.С. Пойта, В.И. Драган, А.П. Дунец, Д.А. Костюк, В.И. Хведчук, С.С. Дереченник. Подход к модернизации гетерогенной сетевой инфраструктуры на примере информационно-вычислительной сети университета // Вестник БрГТУ. – 2010. – №5: Физика, математика, информатика. – С. 75–78.

4. Д.А. Костюк, Р.В. Сченснович. Использование в образовательном процессе вычислительных сетей на базе Windows Server 2008 // Информационные технологии в образовании: материалы Международной научно-практической конференции (Минск, 21–22 мая 2009). – Минск: БНТУ, 2009. – С. 109–113.

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В ТЕСТИРОВАНИИ СЛОЖНЫХ ПРОГРАММНЫХ СИСТЕМ

Д.В. Бабин,
ОКБ САПР, г. Москва

Разработка программного обеспечения – сложный и трудоемкий процесс, в ходе которого непременно возникают ошибки. Часть из них так и не будут выявлены, пока программный продукт не попадет к конечному пользователю. Для того, чтобы сократить число скрытых проблем, применяются различные методы тестирования ПО. Проанализируем их.

1. Модульное тестирование. Автоматический метод тестирования, позволяющий проверять работоспособность небольших модулей, за счет написания unit-тестов. На сегодняшний день имеется огромное количество библиотек, помогающих быстро и удобно писать такие тесты.

2. Непрерывное интегрирование. Метод тестирования связей между модулями, за счет частых сборок разрабатываемого проекта и выполнения небольших проверок на совместимость модулей.

3. Поведенческие скрипты. Этот метод применяется как для частей ПО, так и для всей программы в целом. Суть его довольно проста. Пишутся небольшие «жесткие»

скрипты, симулирующие работу человека. Но этот метод ограничен, так как разработка таких скриптов трудоемка, в них отсутствует случайность и реакция на исключительные ситуации.

4. Ручное тестирование. Пожалуй, лучший метод, так как ни одна программа не может заменить человека. Однако он имеет существенный недостаток, человеческие ресурсы ограничены.

Перечисленные методы автоматического тестирования показывают довольно хорошие результаты в своих узких областях. Но когда необходимо проверить работоспособность всего ПО в целом, ни один из автоматических методов не может даже близко приблизиться к ручному тестированию. Это обусловлено следующими проблемами:

– сложность написания тестов не линейно зависит от сложности ПО;

– отсутствует случайность в поведении тестов.

Таким образом, возникают две задачи:

1. Необходимо упростить создание или автоматически создавать тестовое покрытие.

2. Необходимо добавить случайность в поведение тестового скрипта.

ПО, по своей сути, представляет функцию в многомерном пространстве. В такой математической модели легко можно применить методы нечеткой логики, то есть нейронные сети.

Нейронная сеть – это математическая модель, основанная на когнитивных процессах мозга. Так же как и мозг, нейронная сеть состоит из узлов (нейронов) и переменных связей между ними (веса нейронных связей). Нейроны разделяются на 3 группы по своим свойствам: входные нейроны, выходные нейроны и нейроны скрытого слоя (вычислительные узлы). Фактически нейронная сеть – это особый способ задания функции. Чтобы работать с ней, необходимо проделать следующую работу.

Обучить сеть

Процесс обучения довольно прост. Подготавливается обучающая выборка – множество пар входных и выходных векторов, с заранее известными и правильными значениями. Элементы этого множества удовлетворяют следующему свойству: независимость, следовательно, выборку можно расширять, и ее элементы могут быть переставлены в любом порядке. Обучающая выборка пропускается через нейронную сеть, и в результате этого процесса веса в нейронных связях меняются таким образом, чтобы задать функцию, удовлетворяющую обучающей выборке. Очевидно, что качество работы нейросети зависит от качества ее обучения.

Проверить результат обучения

Подготавливается тестовая выборка аналогично обучающей, но на других значениях. Если результат тестирования неудовлетворительный, стоит лучше обучить сеть или изменить ее структуру.

Хорошо обученная нейросеть способна предсказывать результат по набору входных значений. Вместе с этим дополнительно она решает задачу классификации, если заранее заданы классы во входном множестве, или задачу кластеризации, то есть выявление классов в множестве.

Вернемся к тестированию ПО. Таким образом, нейронная сеть в задаче тестирования способна решить сразу обе подзадачи, за счет механизма предсказания результата. Но остается несколько технических вопросов:

- объем генерируемого тестового покрытия для модульного тестирования (поскольку в тривиальном случае придется создать все возможные переборы входных значений);

- степень случайности и способ ее задания для симуляции пользовательской работы (поскольку набор случайных действий – не лучший способ тестирования);

- структура нейросети остается уникальной для каждой задачи, что препятствует ее массовому распространению.

Исходя из вышесказанного, нейросетевые технологии совместно с широко используемыми методами автоматического тестирования вполне способны улучшить результаты автоматического тестирования в задачах тестирования сложных программных систем.

МАРШ!: ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К СЕТИ

**А.Ю. Батраков,
ОКБ САПР, г. Москва**

В настоящий момент уже множество организаций оценило плюсы использования ПАК СОДС «МАРШ!». Одна из приоритетных задач, решаемых МАРШ!ем, – дистанционное банковское обслуживание. Очевидно, для работы с ДБО требуется доступ в Интернет.

Кажется, что в настоящее время все компьютеры подключены к Интернету. Но множество компьютеров подключено специфическими устройствами или через специфические сети.

Возможные устройства подключения:

- сетевые карты Ethernet;
- Wi-Fi;
- ADSL-модемы;
- беспроводные модемы и др.

При использовании доверенной системы все исполняемые программы так же должны быть доверенными. Это касается и драйверов устройств. Поэтому в среде «МАРШ!» невозможна установка дополнительных драйверов пользователем. А это значит, что поддержка всех возможных устройств принципиально невозможна.

Второй проблемой могут стать особенности промежуточных сетей, через которые будет осуществляться доступ в Интернет. Сети могут требовать специфической настройки клиента (например, необходимо специальное программное обеспечение для доступа к сети), сети могут содержать межсетевые экраны (например, с закрытым доступом к 443 порту), сети просто могут блокировать необходимые сайты.

Таким образом, даже если на компьютере есть доступ к Интернету, еще не факт, что Интернетом удастся воспользоваться для решения своих задач.

Решением может служить USB 3G-модем, для которого есть драйвер в ОС МАРШ!а. Операторы мобильных сетей предоставляют простой доступ к Интернету без необходимости дополнительных программных средств. В настоящее время уже сложно найти место, где не работает мобильный Интернет. А значит, всегда можно получить доступ к необходимому ресурсу.

Из минусов данного решения можно назвать необходимость всегда иметь при себе, кроме МАРШ!а, еще и модем, а так же относительно низкую скорость подобного подключения.

Первая проблема теряет актуальность при совмещении в одном корпусе МАРШ!а и модема. Одного такого устройства будет достаточно для обеспечения сеанса доверенной связи с любого компьютера – и МАРШ!, и устройство доступа к Интернету всегда с собой.

В случае же, когда на компьютере уже есть более быстрый Интернет и проблем при его использовании не возникает, можно воспользоваться им, что решает вторую проблему.

Таким образом, использование МАРШ!а со встроенным модемом выглядит как наиболее удобное и универсальное решение для безопасного дистанционного банковского обслуживания.

ПРОБЛЕМЫ ТЕСТИРОВАНИЯ СЗИ, ФУНКЦИОНИРУЮЩИХ ДО СТАРТА ОС

А.В. Кузнецов, Т.М. Борисова,
ОКБ САПР, г. Москва

В настоящее время при разработке средств защиты информации (СЗИ) производители все больше внимания уделяют их тестированию. Тестирование стало неотъемлемой частью общего процесса разработки, без которого не может быть выполнен выпуск продукта «в свет». Если говорить о тестировании программных СЗИ, то, как правило, оно выполняется в соответствии со всеми правилами тестирования программного обеспечения: проводится функциональное, нефункциональное тестирование и тестирование, связанное с изменениями. Однако существуют еще и программно-аппаратные СЗИ, которые, в свою очередь, состоят из программного обеспечения (ПО) и аппаратной базы, реализующей необходимую аппаратную функциональность. Естественно, такие СЗИ также необходимо тестировать, но уже не просто, как программное обеспечение (программное СЗИ), а с учетом наличия аппаратной составляющей.

Программно-аппаратные СЗИ можно разделить на две группы:

- СЗИ, функционирующие до момента загрузки операционной системы (ОС);
- СЗИ, функционирующие в ОС.

В данной статье мы рассмотрим проблемы тестирования СЗИ первой группы – функционирующие до старта ОС, и не будем рассматривать тестирование СЗИ второй группы. Это связано с тем, что тестирование СЗИ, функционирующих в ОС, в основном, сводится к тестированию, аналогичному по своему составу и способам тестирования, тестированию программных СЗИ (естественно, с учетом наличия и особенностей аппаратной базы). Как правило, СЗИ, функционирующие до старта ОС, представляют собой аппаратный модуль, подключаемый в средство вычислительной техники (СВТ) и перехватывающий на себя управление до момента загрузки ОС. Примером такого СЗИ является средство защиты информации от несанкционированного доступа (НСД) «Аккорд-АМДЗ».

СЗИ НСД «Аккорд-АМДЗ» – это аппаратный модуль доверенной загрузки (АМДЗ) для IBM-совместимых ПК – серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от несанкционированного доступа.

Принцип работы СЗИ НСД «Аккорд-АМДЗ» следующий: контроллер перехватывает управление сразу после выполнения штатного BIOS ПК и позволяет выполнить дальнейшую загрузку ОС только после прохождения ряда контрольных процедур, а именно:

- идентификация/аутентификация пользователя;
- проверка целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности).

Кроме этого «Аккорд-АМДЗ» позволяет выполнять загрузку различных ОС только с заранее определенных постоянных носителей информации (например, только с жесткого диска). Таким образом, обеспечивается доверенная загрузка ОС.

Попробуем применить существующие виды тестирования программного обеспечения (функциональные, нефункциональные и связанные с изменениями) к тестированию СЗИ, функционирующих до старта ОС. Рассмотрим аспект тестирования таких СЗИ с точки зрения автоматизации этого процесса. В этом случае, можно выделить:

- ручное тестирование – все действия выполняются тестировщиком;
- автоматизированное тестирование – для выполнения тестирования применяются специализированные сторонние программные средства;
- полуавтоматизированное тестирование – часть проверок выполняется специализированными сторонними программными средствами, а часть – вручную.

Тестирование программно-аппаратных СЗИ (в нашем случае, «Аккорд-АМДЗ»), выполняемое вручную, проводится по заранее разработанной тестировщиком программе и методике тестирования (ПМИ). Однако, как и при тестировании любого другого продукта, существует необходимость автоматизации данных действий. При автоматизированном тестировании, как правило, используются скрипты (тесты, разработанные при помощи специальных программ), эмулирующие действия пользователя. Однако, в данном случае, так как эти скрипты могут функционировать только в операционной системе, их использование для тестирования СЗИ, функционирующих до старта ОС, является невозможным. Это одна из главных проблем тестирования СЗИ, функционирующих до старта ОС.

Попробуем понять, можно ли в данном случае хотя бы частично автоматизировать действия тестировщика. Для этого разделим тестирование рассматриваемых СЗИ на две части: тестирование исполняемого кода СЗИ отдельно от аппаратной составляющей (например, в среде хостовой ОС) и тестирование конечного функционала СЗИ, доступного пользователю (то есть исполняемого кода вместе с аппаратной составляющей).

Исполняемый код СЗИ может быть запущен на выполнение не в среде ОС аппаратного устройства (в нашем случае, контроллера Аккорд), а в среде аналогичной ОС, установленной на СВТ. Для исполнения этого кода не в операционной системе, а в виртуальной машине требуется возможность «пробрасывания» аппаратного компонента в конкретной среде виртуализации, что часто бывает невозможно (в нашем случае, это невозможно, за счет того, что среды виртуализации не позволяют «пробросить» PCI/PCI-Express-устройство). Таким образом, в рамках ОС СВТ можно автоматизировать процесс проверки корректности исполнения различных модулей, провести нагрузочное и стрессовое тестирование, проверить корректную работу интерфейса. Но в данном случае не будет ответа на главный вопрос: как будет работать финальный продукт, ведь весь этот код должен также корректно выполняться и в среде ОС-контроллера Аккорд. Таким образом, дополнительно необходимо выполнять ручное тестирование по ПМИ, ко-

торое также можно автоматизировать, но лишь частично. К тому же не всегда получится отслеживать результаты всевозможных проверок. В случае тестирования отдельно исполняемого кода СЗИ в ОС СВТ мы можем получить некоторый результат (код возврата, код ошибки и т.п.), на основе которого можно сказать об успешности проверки. В случае же аппаратного компонента такой результат получить нельзя за счет того, что все выполняется внутри контроллера и не передается наружу. Единственное, что удастся отследить при автоматизации тестирования всего СЗИ – корректность отработки функционала контроллера (вообще всего, без конкретики того, что могло отработать не так), причем, в случае неуспешной отработки все равно требуется ручное вмешательство (так как ПК, например, может зависнуть и т.п.).

На основании этого, можно сделать вывод, что в случае с программно-аппаратными СЗИ, функционирующими до старта ОС, можно использовать только полуавтоматизированное тестирование.

Отдельно стоит выделить вопрос совместимости СЗИ с оборудованием, используемого пользователем ПК. Тестирование СЗИ, функционирующего до старта ОС, как правило, выполняется на одном или нескольких ПК, то есть в некой абстрактной «песочнице», которая не включает все возможные варианты СВТ, представленные на современном рынке. А поскольку речь идет о программно-аппаратном

СЗИ, включающем аппаратную часть (контроллер Аккорд), то вполне возможны несовместимость с различным СВТ по питанию, поддержке работы сторонних периферийных устройств и т.п. К примеру, перехват управления контроллером «Аккорд-АМД3» является аппаратно зависимым и зависит от реализации BIOS, UEFI и различных прерываний. В связи с этим, по результатам проведенного тестирования (в абстрактной «песочнице») нельзя судить о корректности работы рассматриваемого СЗИ вообще на любом оборудовании, которое может использовать пользователь. А перед внедрением СЗИ пользователю предварительно нужно запросить информацию о совместимости у производителя данного СЗИ и, возможно, предоставить свое оборудование для проверки.

Таким образом, можно сделать вывод, что при тестировании СЗИ, функционирующих до старта ОС, существует ряд проблем, которых нельзя встретить при проверке программных СЗИ, а также программно-аппаратных СЗИ, функционирующих в ОС. Это обусловлено тем, что тестирование аппаратной компоненты без возможности доступа к ее функциональности из ОС достаточно затруднительно. Также при тестировании таких СЗИ, как «Аккорд-АМД3», возникает проблема возможности проверки совместимости с многообразием существующих СВТ, так как провести тестирование совместимости на всем существующем оборудовании практически невозможно.

ХРАНЕНИЕ ДАННЫХ СКЗИ: ШИПКА-ЛАЙТ ИЛИ СЕКРЕТ

Ю.П. Ладынская, Т.М. Борисова,
ОКБ САПР, г. Москва

В настоящее время все большую актуальность обретает проблема выбора хранилища для критичной информации, генерируемой и используемой программными средствами криптографической информации (СКЗИ).

С точки зрения хранения и применения криптографических ключей в Автоматизированной системе принципиальное значение имеют 2 фактора:

- защищенное хранение ключа (и, соответственно, носитель ключа)

- условия доступа к ключу и работы с ним при непосредственном выполнении СКЗИ функций по обработке данных (то есть среда функционирования криптографии).

В части доступа к ключу очевидна необходимость учитывать как условия доступа пользователя (человека), так и условия доступа СКЗИ и другого системного и функционального программного обеспечения.

В части среды функционирования криптографии необходимо учитывать особенности сред и систем, в которых пользователи выполняют задачи, связанные с криптографическими преобразованиями: работа в различных ОС, загруженных на СВТ различных архитектур из различных источников различными способами, может иметь целый ряд особенностей, существенно влияющих на безопасность ключа.

Отсюда вытекают требования к защищенному ключевому носителю.

Требования к защищенному ключевому носителю

Защищенный носитель ключа в идеальном случае должен быть способен контролировать

- доступ к ключу через любые интерфейсы, в том числе и путем применения разрушающего программного воздействия (РПВ);

- среду, в которой производится попытка доступа к ключу.

При этом, очевидно, что в любом случае, если применяется внешнее СКЗИ, защищенный ключевой носитель не должен контролировать корректность его работы или собственно обеспечивать среду его функционирования (это функция средства доверенной загрузки).

Иными словами, задача «контроля» среды, из которой осуществляется доступ к ключу, сводится к тому, чтобы доступ к ключу предоставлялся не только исключительно легальному пользователю, но и исключительно на заданных рабочих местах (наличие «правильной» среды на которых обеспечивается в установленном в организации порядке).

Основные требования

- быть персональным устройством;
- быть специализированным именно для хранения ключей устройством (то есть обеспечивать возможность защищенного хранения криптографических ключей с при-

менением интерфейсов работы со смарт-картой (ccid или pkcs#11));

- предоставлять доступ к ключам только легальному пользователю после успешной аутентификации в устройстве;
- предоставлять легальному пользователю доступ к ключам только на тех СВТ, на которых данному пользователю разрешено работать с данным ключевым хранилищем;
- удовлетворять требованию патентной чистоты.

Дополнительные требования

- предоставлять возможность защищенного с учетом основных требований хранения ключей различных СКЗИ одновременно (для минимизации количества устройств у каждого пользователя);
- предоставлять СКЗИ интерфейс для использования встроенного ДСЧ;
- соответствовать требованиям эргономики и дизайна, принятым в эксплуатирующей организации (цвет и размер, наличие аксессуаров, требуемых регламентом использования).

Современный рынок информационных технологий предлагает множество решений в данной области, это могут быть отчуждаемые носители информации (смарт-карты, токены, обычные флэш-накопители), среди которых есть и специализированные устройства (такие как устройства с защищенной памятью, так и флэш-накопители). Примером таких специализированных устройств может служить ПСКЗИ ШИПКА и Секрет. Рассмотрим различные аспекты их применения и постараемся выяснить, какое из устройств является наиболее подходящим для решения задач по хранению критичной информации программных СКЗИ.

ПСКЗИ ШИПКА – это USB-устройство, которое совмещает аппаратно реализованные криптографические функции с целым рядом дополнительных защитных функций и возможностей, таких как использование ШИПКи в качестве идентификатора и для хранения ключевой информации сторонних программных СКЗИ и т.д.

Одно из устройств семейства ПСКЗИ ШИПКА, а именно ШИПКА-лайт, также аппаратно реализует криптографические алгоритмы, но в отличие от остальных конструктивов ШИПКи, скорости ее криптоопераций достаточно малы. Еще одно устройство семейства – ШИПКА-лайт Slim – вовсе не обладает криптографическим функционалом. Поэтому, в основном применение этих устройств сводится к использованию их в качестве идентификатора и для хранения ключевой информации программных СКЗИ.

ШИПКА-лайт состоит из смарт-карты, работающей по базовым стандартам ISO-7816, и CCID-совместимого карт-ридера. ШИПКА-лайт Slim реализована в виде цельнокорпусного микропроцессорного устройства, имеющего несъемный ключевой контейнер. Оба устройства поддерживают стандартный протокол обмена данными CCID, используемый для работы с традиционными смарт-картами.

Драйвер смарт-карты, необходимый для работы ШИПКи-лайт и ШИПКи-лайт Slim (далее – ШИПКА-лайт), автоматически подгружается из центра обновлений в операционных системах, начиная с Windows Vista и выше, что позволяет использовать устройства в качестве ключевого хранилища программных СКЗИ без установки программного обеспечения (ПО) ШИПКи.

Для получения доступа к файлу с ключевой информацией программного СКЗИ необходим PIN-код, количество попыток ввода которого ограничено аппаратно, что исключает возможность подбора. Поскольку ключи хранятся во встроенной защищенной энергонезависимой памяти, получить к ним доступ без знания PIN-кода невозможно.

ШИПКА-лайт имеет небольшой объем памяти – всего 128КБ (в случае ШИПКи-лайт Slim – 64КБ), однако, данного объема достаточно для хранения ключевой информации программных СКЗИ.

При использовании ШИПКи-лайт и ШИПКи-лайт Slim в качестве ключевого хранилища, данные в устройстве хранятся в формате PKCS#11, и именно в этом формате работают с ключами СКЗИ. Однако оказывается, что ключи – это не единственная информация, которая по требованиям к применению тех или иных СКЗИ должна храниться защищенно. И хранение в памяти данных устройств другой информации программных СКЗИ (например, справочников сертификатов), которые существуют в отличных от указанного форматах, невозможно. Помимо прочего такая информация занимает значительно больший объем, поэтому при необходимости хранить не только ключи, но и еще какую-либо информацию программных СКЗИ, целесообразнее не дорабатывать механизмы работы с данным токеном, а использовать другие устройства, имеющие, в том числе, больший объем памяти. Такими устройствами могут быть защищенные носители Секрет.

Секрет существует в трех вариациях: ПАК «Личный Секрет», ПАК «Секрет Фирмы» и ПАК «Секрет Особого Назначения». В состав каждого комплекса входит специальный носитель пользователя (СН).

ПАК «Личный Секрет», состоящий из ПО «Секретный агент» и специального носителя Секрет, предназначен для защиты личных данных пользователя, в том числе и при утрате этого носителя. Использовать «Личный Секрет» можно только на разрешенных администратором рабочих станциях (РС). При подключении устройства к неразрешенным РС, диск устройства не будет примонтирован и определен ПК, как флэш-накопитель.

ПАК «Секрет фирмы» – это корпоративное развитие ПАК «Личный Секрет».

ПАК «Секрет Особого Назначения» состоит из специального носителя Секрет, все необходимое для работы программного обеспечения располагается в одном из разделов внутренней памяти устройства, доступного только для чтения. Установка дополнительного ПО не требуется, устройство поддерживает стандартный CCID-интерфейс.

Принципиальное отличие «Секрета Особого Назначения» от «Личного Секрета» и «Секрета Фирмы» заключается в том, что в его аппаратном журнале фиксируются все попытки работы с ним на различных АРМ, вне зависимости от того, была ли попытка успешной. В случае «Секрета Особого Назначения» администратор может настроить политики использования специального носителя, предоставив доступ без ограничений по доменам и РС, или задать список разрешенных рабочих станций.

Для доступа к данным СН Секрет, как в случае ШИПКи-лайт, необходим PIN-код (или код авторизации – КА).

СН Секрет обладает значительным объемом флэш-памяти: в стандартной комплектации – 4 Гб, что в случае его использования в качестве хранилища информации про-

граммного СКЗИ позволяет помимо ключей, хранить еще и справочники сертификатов, а также копии библиотек и другую необходимую информацию.

Если рассматривать представленные устройства с точки зрения контроля среды функционирования, то в случае использования каждого из устройств (и ШИПКи-лайт, и Секрета), доступ к ключам предоставляется только легальному пользователю после успешной аутентификации в устройстве посредством ввода PIN-кода (или КА), а в случае использования Секрета, доступ к ключам предоставляется еще и исключительно на разрешенных рабочих станциях.

Также оба устройства имеют возможность защищенного хранения ключевой информации с применением стандар-

тных интерфейсов работы (CCID или PKCS#11), что обеспечивает совместимость с различными программными СКЗИ.

Таким образом, каждое из рассмотренных устройств имеет свои особенности, и под каждую конкретную задачу можно подобрать наиболее подходящее решение.

Однако наиболее универсальным и надежным стало бы устройство, сочетающее преимущества и ШИПКи-лайт и Секрета. Ключевое хранилище, имеющее привязку к разрешенным ПК, защищенное PIN-кодом (или КА), обладающее значительным объемом криптографически защищенной памяти, работающее со стандартными протоколами передачи данных, – вот оно, идеальное устройство, отвечающее всем требованиям безопасности и общепринятым нормам практичности применения.

СПОСОБЫ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ СЗИ, ФУНКЦИОНИРУЮЩИХ В ОС, НА ПРИМЕРЕ ПСКЗИ ШИПКА

А.И. Обломова, Т.М. Борисова,
ОКБ САПР, г. Москва

Способы автоматизации тестирования СЗИ, функционирующих в ОС, на примере ПСКЗИ ШИПКА.

Уже давно ни у кого не вызывает сомнения, что тестирование должно являться неотъемлемой частью разработки программного обеспечения (ПО) или программно-аппаратных средств.

Согласно общепринятой классификации выделяют несколько основных видов тестирования ПО:

- функциональное, которое отвечает за проверку реализуемых функциональных требований;
- нефункциональное, которое отвечает за тестирование таких характеристик, как производительность, стабильность/надежность (тестирование на отказ, нагрузочное, стрессовое тестирование), а также за тестирование удобства использования.

Помимо этого, существует еще тестирование после исправления ошибок в ПО, призванное подтвердить факт устранения этих ошибок. В этом случае выделяют регрессионное тестирование, проверку согласованности/исправленности, тестирование сборки. Данный вид тестирования также подразумевает функциональное и нефункциональное тестирование, таким образом, просто расширяя их.

Рассмотренные виды тестирования ПО также применимы для тестирования программно-аппаратных средств с учетом определенных особенностей, которые будут рассмотрены ниже.

Естественно, перечисленные виды тестирования, имеют множество подвидов. Очевидно, что в тестировании любого ПО или программно-аппаратного средства, должно быть уделено внимание каждому из них. Проведение проверок, связанных с каждым из этих видов тестирования, может быть выполнено как ручным способом, так и с использованием автоматизированных средств.

На начальном этапе развития ПО или программно-аппаратного средства, как правило, превалирует ручное

тестирование, но в дальнейшем, когда его функционал растет и расширяется, и уже ручное тестирование становится не оптимальным и не дает ожидаемых результатов, необходимо оптимизировать ручную работу и использовать средства автоматизированного тестирования.

Рассмотрим преимущества автоматизированного тестирования по сравнению с ручным тестированием:

- повторяемость – все написанные тесты всегда будут выполняться однообразно, то есть исключен «человеческий фактор», «компьютер» не пропустит тест по неосторожности и ничего не напутает в результатах;
- быстрое выполнение – автоматизированному тесту не нужно «сверяться» с инструкциями и документациями, это сильно экономит время проверки;
- меньшие затраты времени на анализ результатов тестирования и адаптацию тестов в случае изменения функционала – анализ результатов тестирования автоматических тестов при изменении какого-либо функционала продукта, их адаптация и повторное проведение тестирования требует, как правило, меньшего времени, чем аналогичные действия того же объема тестирования вручную;
- автоматическое формирование и рассылка отчетов – автоматизированные тесты могут автоматически рассылать и сохранять отчеты о результатах тестирования;
- выполнение без вмешательства человека – во время выполнения тестов тестирующий может заниматься другими полезными делами, или тесты могут выполняться в нерабочее время.

Рассмотрим способы автоматизации тестирования на примере программно-аппаратных средств защиты информации (СЗИ). Естественно, что при разработке СЗИ необходимо также выполнять их всестороннее тестирование, как и любых других выпускаемых программных или программно-аппаратных средств. Программно-аппаратные средства защиты информации, в свою очередь, грубо можно разделить на 2 группы: СЗИ,

функционирующие до старта операционной системы (ОС), и СЗИ, функционирующие в ОС. В данной статье мы рассмотрим автоматизацию тестирования СЗИ второй группы – функционирующие в операционной системе, и не будем рассматривать автоматизацию тестирования СЗИ первой группы, в связи с тем, что автоматизация тестирования последних затруднена по ряду причин и требует отдельного рассмотрения.

Функциональное тестирование СЗИ, выполняемое вручную, проводится по заранее разработанной тестировщиком программе и методике тестирования (ПМИ). При автоматизированном функциональном тестировании СЗИ, как правило, используются скрипты (тесты, разработанные при помощи специальных программ) для эмуляции действий пользователя. Существует множество программ, позволяющих разрабатывать подобные скрипты. Одни из них основываются на технологии поиска и автоматизации работы с элементами графического интерфейса на основе изображений (скриншотов), другие на основе ключевых слов и т.д. Главным плюсом использования скриптов является экономия времени на тестировании монотонных и однотипных действий, например, при переборе входных данных. Таким образом, один раз написанный тест может долго служить, экономя время тестировщика. Но это будет так до первого изменения в поведении тестируемого СЗИ. Если СЗИ начинает функционировать по-другому, даже если это незначительные отклонения (например, выводится новое информационное окно или была изменена цветовая гамма), то требуется вносить изменения в скрипт теста. Это одна из проблем при использовании такого вида автоматизации – будет ли сэкономленное время перевешивать время написания\изменения скриптов. И, конечно, нужно учитывать, что автоматизировать тестирование дружелюбности интерфейса невозможно.

Для нефункционального тестирования используются средства автоматизации, которые имитируют одновременное обращение к системе предельного количества пользователей (максимального или минимального) или формируют непрерывные запросы этого предельного количества клиентов к системе. Как правило, нагрузочное и стрессовое тестирования проводятся непрерывно в течение нескольких дней. При этом использование автоматизированных программ не только значительно экономит средства, но иногда является единственным возможным способом проверить работу системы при пиковых нагрузках.

Рассмотрим способы тестирования СЗИ, функционирующих в ОС, на примере персонального средства криптографической защиты информации – ПСКЗИ ШИПКА.

Первый способ, это классический способ уже рассмотренный выше, – использование автоматизированных скриптов, разработанных при помощи специальных программ автоматизации. Эти скрипты позволяют проводить и функциональное и нефункциональное тестирование ПСКЗИ ШИПКА. Однако поскольку ПСКЗИ ШИПКА состоит из программного и аппаратного компонента, это обязательно нужно учитывать при организации тестирования – в ходе функционального тестирования ПСКЗИ ШИПКА аппаратную часть продукта необходимо переподключать к USB-порту ПК, что нарушает идеологию проведения автоматизированных тестов, которые должны проводиться без участия

«человека». Поэтому полностью автоматизировать такое функциональное тестирование затруднительно, так как в данном случае необходимо участие тестировщика для выполнения указанных действий. Аналогичная проблема возникает при нефункциональном тестировании – в случае возникновения ошибок в ходе выполнения скрипта устройство необходимо физически переподключить к ПК.

Второй способ автоматизации тестирования ПСКЗИ ШИПКА представляет собой использование комплекта разработчика (SDK – Software Development Kit) для стандартных интерфейсов, который реализован для ПСКЗИ ШИПКА в целях возможности использования криптографической функциональности устройства сторонними разработчиками в своих продуктах. В настоящее время для ПСКЗИ ШИПКА реализовано три стандартных интерфейса: Crypto API, PKCS#11, APDU, а SDK для них включает набор примеров по их использованию. Эти примеры можно использовать для автоматизации функционального тестирования ПСКЗИ ШИПКА, так как их успешное прохождение гарантирует, конечно, не полностью, но частично, что и те утилиты, которые работают на базе этих интерфейсов, будут работать корректно с ШИПКой. Естественно, при этом остается необходимость функционального и нефункционального тестирования самих утилит продукта.

На основании описанного в данной статье можно сделать вывод, что ручное и автоматизированное тестирование – две неотъемлемые части при проверке качества любого выпускаемого продукта, в том числе и СЗИ. Невозможно полностью автоматизировать все тесты, так как при работе, например, с ПСКЗИ ШИПКА, может потребоваться переподключение устройства в USB-порт ПК. Также автоматизированный тест никогда не сможет проверить «дружелюбность» интерфейса и т.д. Но однозначно нужно признать, что внедрение автоматизированного тестирования значительно сокращает время на проведение проверок, и с помощью него становится возможным провести тестирование, которое человек сможет выполнить только за достаточно большой период времени, а, возможно, и никогда не сможет. А именно, сложно представить, как тестировщик вручную тестирует предельные значения, например, в случае с ПСКЗИ ШИПКА, проверяет корректность функционирования устройства с максимально возможным количеством криптографических ключей в устройстве, которое может быть больше 200. Для этого тестировщику нужно вручную сгенерировать все эти ключи и только потом проверить корректность функционирования устройства. Если же окажется, что в этом процессе возникнут ошибки, то нужно будет поэтапно уменьшать количество ключей и повторять тестирование до определения критического значения. Также тестировщику сложно вручную проводить стрессовое тестирование, при котором он должен генерировать различные случайные значения и подавать их в качестве входных параметров в устройство, для проверки реакции ПСКЗИ ШИПКА на каждое из них. В случае с ПСКЗИ ШИПКА, например, необходимо задавать различные случайные значения длины PIN-кода и проверять, как устройство будет реагировать на каждое из введенных значений. Эти факты подтверждают правильность подхода использования автоматизированного тестирования наряду с ручным тестированием.

ОСОБЕННОСТЬ ТЕСТИРОВАНИЯ СЗИ, В КОНСТРУКТИВ КОТОРЫХ ВХОДИТ ФЛЕШ-ПАМЯТЬ

Т.М. Борисова,
ОКБ САПР, г. Москва

Применяемые в настоящее время СЗИ бывают различных видов и предназначены для решения совсем разных задач. Существуют средства обеспечения доверенной загрузки ОС, защищенной загрузки ПО ТС по сети, разграничения доступа, криптографической защиты информации, обеспечения доверенного сеанса связи и т.д. Нужно признать, что одним из важных этапов в процессе разработки СЗИ является их тестирование. Если говорить о тестировании программных СЗИ, то оно должно выполняться в соответствии со всеми правилами тестирования программного обеспечения, то есть необходимо проводить функциональное, нефункциональное тестирование и тестирование, связанное с изменениями. Как правило, такое тестирование выполняется либо вручную с использованием специально разработанных программ и методик испытаний (ПМИ), либо с использованием автоматизированных тестов, разработанных на основании этих ПМИ. Однако существуют еще и программно-аппаратные СЗИ, которые, в свою очередь, состоят из программного обеспечения (ПО) и аппаратной базы, реализующей необходимую аппаратную функциональность. Естественно, такие СЗИ также необходимо тестировать, но уже не просто, как программное обеспечение (программное СЗИ), а с учетом наличия аппаратной составляющей.

При тестировании аппаратной составляющей программно-аппаратного СЗИ необходимо различать специфичные и неспецифичные компоненты аппаратной базы, требующие, в свою очередь, специализированного и универсального тестирования соответственно. Тестирование программно-аппаратного СЗИ в части защитных функций носит специализированный характер и выполняется аналогично тестированию программных СЗИ, но с учетом наличия аппаратной составляющей и всех нюансов ее функционирования.

К аппаратным составляющим СЗИ, требующим универсального тестирования, относится флеш-память с доступом как Mass Storage (далее флеш-память). Примерами СЗИ с такой флеш-памятью являются ПСКЗИ ШИПКА на базе ШИПКА-2.0, которое может использоваться и как самостоятельное СКЗИ, так и в составе ПАК «Центр-Т», и служебные носители (СН) Секрет из ПАК «Личный Секрет», «Секрет Фирмы», «Секрет Особого Назначения».

ШИПКА-2.0 состоит из микропроцессора, в котором аппаратно реализованы все современные российские криптографические алгоритмы, и флеш-памяти, в которой можно хранить различные данные. Флеш-память ШИПКИ-2.0 в ПАК «Центр-Т» используется для хранения образов начальной загрузки и для загрузки образов ПО ТС по сети для получения доступа к терминальному серверу.

СН Секрет, в свою очередь, также состоит из микропроцессора и флеш-памяти. Микропроцессор реализует протокол, направленный на ограничение ПК, на которых может быть получен доступ к данным, хранящимся во флеш-памяти, а также процедуру идентификации/аутентификации пользователей при доступе к флеш-памяти и шифрование

ее содержимого (если устройство поддерживает функцию шифрования пользовательских данных), а флеш-память – это то, что доступно пользователю в качестве привычного для него флеш-носителя (после успешного прохождения процедуры идентификации/аутентификации). А в случае с СН Секрет из ПАК «Секрет Особого Назначения» на флеш-носителе существует дополнительно доступный только для чтения логический раздел, на котором хранятся утилиты для работы комплекса.

Исходя из вышеописанного, видно, что флеш-память указанных устройств в процессе их жизненного цикла используется достаточно активно: пользователь ежедневно загружает свой образ ПО ТС и тем самым задействует флеш-память, не говоря уже о флеш-памяти СН Секрет, в которых чтение и запись данных на нее (в зависимости от активности пользователя) могут происходить гораздо чаще, чем в первом случае. Говоря о Секрете, не стоит забывать, что при его использовании немаловажную роль для пользователя могут играть скорости чтения/записи, и в зависимости от их значения он будет принимать решение о возможности использования данного устройства. Из приведенных фактов вытекает, что при выпуске данных СЗИ важно гарантировать возможность качественной работы с флеш-памятью. Помимо этого, нужно точно определить, зафиксировать и опубликовать скорости чтения/записи при работе с устройством. Поэтому разработчикам необходимо знать характеристики производимых устройств по параметрам, которые бы подтверждали корректность функционирования их флешки и давали информацию о скоростях ее работы. Эти данные дадут возможность производителям предоставить пользователям необходимые характеристики флеш-памяти их СЗИ, а также вовремя отбраковывать некорректно работающие устройства, и устройства, с которыми в процессе эксплуатации могут возникнуть проблемы. Для этих целей используется ряд утилит, которые позволяют выполнять тестирование флеш-памяти выпускаемых устройств.

Существует два направления тестирования флеш-памяти: тестирование скорости чтения/записи и нагрузочное тестирование. Оба эти подвиды тестирования должны использоваться для тестирования флеш-памяти рассмотренных выше СЗИ.

Тестирование скорости флеш-дисков состоит из изменения и анализа следующих параметров:

- время доступа при чтении и записи с использованием фиксированных тестовых блоков 4, 64 и 1024 Кб;
- скорость записи и чтения одного большого файла объемом несколько Гб;
- скорость записи и чтения пакета мелких файлов размером от нескольких байтов до 500 Кб, представляющих собой, например, сохраненные html-странички, небольшие PDF-документы, материалы в форматах .doc и .xls.

Результатом такого тестирования является скорость чтения/записи с/на флеш-память. Этот параметр произво-

датель фиксирует и анонсирует впоследствии в качестве одной из характеристик разрабатываемого СЗИ с флеш-памятью. На основании данной характеристики пользователь может судить о скорости работы с устройством.

Нагрузочные тесты подразделяются на:

- тестирование на физическом уровне (со всей доступной областью памяти). Результатом такого тестирования является показатель общей устойчивости памяти к частоте записи на нее произвольной информации (реальное количество возможных циклов перезаписи информации без нарушения нормального функционирования памяти). В данном тестировании проводится проверка именно равномерной записи данных на носитель.

- тестирование на уровне абстракции файловой системы (с разделами, логическими дисками, партициями). Результатом такого тестирования является показатель рабочей устойчивости памяти к частоте записи на нее произвольной информации – т.е. будет учитываться частая запись в наиболее активные области раздела.

На основании полученных данных производитель может вовремя отбраковать некорректно работающие устройства, а также те устройства, с которыми в процессе эксплуатации могут возникнуть проблемы.

Для проведения всех перечисленных видов тестирования СЗИ может использоваться ряд утилит, широко доступных в настоящее время для тестирования устройств хранения информации (HDD, CD-ROM, Flash-drive, floppy и т.д.). Примером таких утилит, находящихся в бесплатном доступе, могут служить утилиты HD_Speed и CheckFlash.

Утилита HD_Speed предназначена для тестирования скорости чтения/записи устройств для хранения информации.

В этой утилите можно задать смещение и размер считываемого/записываемого блока, выбор этих параметров может повлиять на скорость работы. Помимо этого, можно выбрать отдельный логический раздел на жестком диске и проверить, как, например, влияет файловая система или наличие «плохих» кластеров на производительность.

Check Flash – утилита, предназначенная для проверки работоспособности флеш-накопителей, а также позволяющая при помощи тестов определить мгновенную и среднюю скорость чтения/записи. В этой утилите можно проверить стабильность чтения/записи с носителя и на него, как на логическом уровне, так и на физическом.

При использовании обеих утилит можно определить количество ошибок чтения/записи, возникших в процессе тестирования, а вся полученная информация может сохраняться в журнал для дальнейшего анализа и сравнения результатов.

Как уже говорилось выше, данные утилиты могут использоваться для тестирования флеш-памяти СЗИ, в которых она присутствует. На основании полученных результатов можно сделать вывод о пригодности данного устройства для использования в составе программно-аппаратного комплекса, однако, не стоит забывать и о тестировании основного функционала конкретного СЗИ.

Таким образом, можно сделать вывод, что тестирование СЗИ, в конструктив которых входит флеш-память (с доступом как Mass Storage), немного отличается от тестирования СЗИ без нее, и состоит из двух составляющих: тестирование СЗИ плюс тестирование его флеш-памяти, только в этом случае можно судить о достаточности тестирования СЗИ с флеш-памятью.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ МЕХАНИЗМА ОЧИСТКИ ОСВОБОЖДАЕМЫХ ОБЛАСТЕЙ ОПЕРАТИВНОЙ ПАМЯТИ В GNU/LINUX

**В.С. Прокопов, А.М. Каннер,
ОКБ САПР, г. Москва**

Одним из требований к средствам защиты информации от несанкционированного доступа (СЗИ НСД) является наличие механизма очистки или обезличивания освобождаемых областей оперативной памяти при ее перераспределении. Необходимость в наличии такого механизма защиты регламентирована требованиями государственных регуляторов в области защиты информации:

- РД ФСТЭК «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» (для классов СВТ 4, 3, 2 и 1);

- РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (для классов АС 3А, 2А, 1Г, 1В, 1Б и 1А).

Вообще говоря, в ОС семейства Linux за счет изолированности памяти каждого процесса (каждый процесс выполняется в собственном адресном пространстве), требование по очистке оперативной памяти носит скорее

дополнительный характер. Связано это с тем, что в соответствии с остальными требованиями, предъявляемыми к СЗИ НСД, «нелегитимно» получить доступ к памяти какого-либо процесса может только пользователь с достаточно высокими привилегиями (т.е. это внутренний нарушитель и только с административными полномочиями). В рамках же любого класса защищенности по РД возможность такого доступа фактически пропадает с корректным вводом политик безопасности. Так или иначе очищать оперативную память необходимо хотя бы для уверенности. Разберемся по порядку, чем может быть опасен вариант отсутствия механизмов очистки памяти.

Очистка оперативной памяти: что и зачем очищать?

В оперативную память в процессе работы любого СВТ и любой ОС загружается любая обрабатываемая информация, в том числе и критично важные данные, такие как:

- ключи шифрования или подписи;
- пароли, вводимые пользователем;

- конфиденциальная информация;
- прочее.

В ОС Linux в определенных ситуациях существует возможность получить доступ на чтение к оперативной памяти (/dev/mem, /dev/kmem) и, следовательно, получить доступ к критичной информации. Чтобы минимизировать риск утечки информации при освобождении участков памяти, необходимо их затирать (например, записывать последовательность из 0-й или каких-то произвольных значений).

Очевидно, что сам процесс затирания участков оперативной памяти СЗИ НСД должен быть реализован в виде модуля ядра ОС, который будет производить все свои действия в моменты перехвата определенных системных вызовов, связанных с выделением и освобождением областей памяти. В ходе реализации такого модуля порождается сразу несколько задач, которые необходимо решить:

- необходимо определить, что и в какой момент нужно очищать, не вызвав при этом нарушений работы приложений или самой ОС;
- необходимо определить адреса начала и конца подлежащих очистке данных;
- необходимо использовать методы очистки, которые не будут оказывать сильного влияния на общую производительность системы.

При решении первой задачи необходимо учитывать, что не всегда можно обнулить/очистить конкретную область памяти, не вызвав краха какого-нибудь приложения, использующего эту область памяти в данный момент (или в ближайшем будущем). В качестве примера можно привести разделяемые области памяти. Нет никаких технических сложностей в том, чтобы очищать эти области, скажем, при завершении определенного приложения (которое инициировало выделение этой области памяти). Однако это может привести к неопределенным последствиям, так как ОС не запрещает выделить одному приложению разделяемую область памяти, завершить его работу, а потом запустить другое приложение, которое должно в своей работе использовать ту же разделяемую область памяти. Этот пример показывает, что, в первую очередь, нужно понять, какого типа данные и, дополнительно, при перехвате какого системного вызова мы должны/можем очищать.

При решении второй задачи могут возникнуть сложности. Иногда нужные адреса начала и конца подлежащих очистке данных передаются в параметрах системных вызовов, а иногда эти данные могут отсутствовать в интересующем нас виде или могут отсутствовать вообще. К примеру, бывает необходимо подождать завершения системного вызова `mmap` (который изменяет область отображения файла в память), а адреса, которые передавались в параметрах, в определенный момент могут уже потерять свою актуальность. Кроме того, могут возникать некоторые сложности при очистке большого диапазона адресов – некоторые страницы могут отсутствовать в оперативной памяти.

При разработке методов очистки памяти всегда нужно учитывать возможность нарушения производительности системы (третья задача). Необходимо следить, чтобы методы, которыми решается задача очистки данных, не вызывали хотя бы ощутимого снижения производительности системы. В одних случаях включение механизма очистки может почти не влиять на скорость выполнения определенных операций, в других же при неосмотрительном выборе метода очистки

скорость выполнения операций может замедлиться в два и более раз. Также необходимо понимать, что вмешательство в работу системных вызовов по работе с памятью может само по себе серьезно сказываться на производительности, т.к. эти вызовы используются ядром ОС довольно активно.

Итак, что же вообще нужно очищать? Для начала стоит рассмотреть структуру памяти, которая используется для работы процессов (примерная схема изображена на рисунке 1).

В ядре ОС Linux все области виртуальной памяти, которые выделяет ядро ОС, характеризуются структурой `struct vm_area_struct` (эту структуру можно найти с помощью функции `find_vma`, зная виртуальный адрес в памяти). В этой структуре содержатся адреса начала и конца области памяти, права доступа к памяти, а также некоторые интересующие нас флаги, в частности флаг `VM_SHARED`, который обозначает разделяемую область памяти. Все части процесса расположены в этих областях памяти (в областях памяти, описываемых структурой `vm_area_struct`), также мы можем получить список всех структур `vm_area_struct`, принадлежащих конкретному работающему процессу.

С другой стороны, существует более детальное деление процесса на секции и сегменты, такие как:

- куча;
- стек;
- секция инициализированных данных;
- секция кода;
- секция не инициализированных данных;

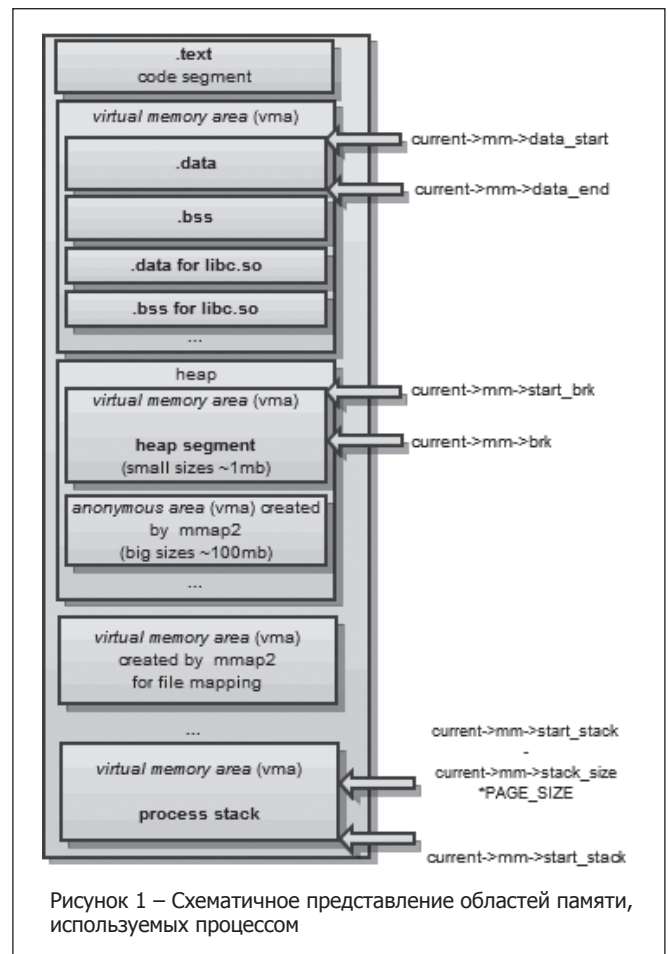


Рисунок 1 – Схематичное представление областей памяти, используемых процессом

– секции инициализированных/неинициализированных данных для каждой загруженной в память разделяемой библиотеки.

Каждая секция/сегмент расположен в одной или нескольких областях памяти (`vm_area_struct`), таким образом, можно считать, что секции и сегменты отображаются на области памяти. С позиции очистки памяти нам интересны секции и сегменты, непосредственно хранящие данные – это сегмент кучи, отображаемые в оперативную память файлы, секции данных приложения и библиотек, стек приложения, стеки порождаемых приложением потоков. Далее рассмотрим методы, применяемые для очистки тех или иных областей памяти.

Методы очистки памяти в куче (heap)

Со стороны интерфейса программирования куча управляется вызовами `malloc` (выделение памяти), `realloc` (изменение размера выделенной памяти), `free` (освобождение памяти). Однако сами системные вызовы, которые вызываются при работе этих функций, могут функционировать по-разному (например, в зависимости от размера выделяемой/выделенной памяти).

При относительно маленьких размерах памяти (до 1-10 Мб), память выделяется в сегменте кучи приложения, начальный и конечный (текущий) адреса которой можно узнать из структуры, описывающей процесс – `task_struct`. В этом случае, все управляется системным вызовом `brk` (т.е. вызовы `malloc` и `free` вызывают `brk` с соответствующим значением), который используется для того, чтобы изменить конечный (текущий) адрес кучи. При этом подчеркнем факт того, что при вызове `free`, `brk` может и не вызываться для уменьшения размера кучи, например, `free` не станет делать лишний системный вызов при освобождении нескольких байт (освобождение будет отложено, а память будет зарезервирована на случай дополнительного выделения). Конкретная стратегия работы функций по работе с памятью зависит от их реализации.

Иначе обстоит дело с выделением памяти больших размеров (например, 100 Мб). В данном случае функция `malloc` использует системный вызов `mmap2` с флагом `MAP_ANONYMOUS`. Соответственно, в оперативной памяти выделяется еще одна область памяти и соответствующая ей структура `vm_area_struct` добавляется в список областей памяти, принадлежащих процессу. Соответствие библиотечных и системных вызовов здесь будет иное: `malloc` будет вызывать `mmap2`, `realloc` – `mremap`, а `free` – `munmap`.

Таким образом, чтобы очищать память в куче необходимо перехватывать системные вызовы `brk`, `mremap` и `munmap`.

При перехвате системного вызова `brk` нужно посмотреть на передаваемый ему адрес, и сравнить его с текущим адресом конца сегмента кучи (его можно узнать из структуры `task_struct` для текущего выполняемого процесса – `current`). В случае, если передаваемый адрес меньше текущего и больше адреса начала кучи, необходимо очистить данные между передаваемым значением адреса и до текущего адреса конца кучи.

При перехвате `mremap` и `munmap` (в случае кучи) необходимо найти структуру типа `vm_area_struct` (с помощью функции `find_vma`) и проверить, что область не является разделяемой областью памяти, область не принадлежит отображению из файла, есть права на запись в эту область памяти (в противном случае присутствует высокий риск обнулить служебную область памяти, выделенную системой). Если указанные проверки пройдены успешно, – можно очистить необходимые

участки памяти. В случае `munmap` необходимые адреса передаются в параметрах системного вызова, в случае `mremap` их необходимо сначала вычислить на основании четырех адресов, которые передаются в параметрах (старые начальный и конечный адреса и новые начальный и конечный адреса изменяемого участка памяти).

В процессе тестирования обнаружилось, что ядро ОС Linux версии 2.6.32 при вызове `mmap` самостоятельно обнуляет ненужную более область памяти. Однако подтвердить наличие этой особенности во всех версиях ядра ОС Linux (включая более ранние, хотя бы ветки 2.6) на данный момент не получилось. Да и не стоит полагаться в этом вопросе на ядро ОС – его функционал может измениться непредсказуемым образом с любой новой версией, да и вообще нет гарантии того, что очищается вся память (это не основная функция ядра). Для этих целей лучше использовать собственное узконаправленное СЗИ. Кроме этого, отметим, что аналогичные системные вызовы применяются в большом количестве других Unix-подобных ОС, так что методы, изложенные в данной статье, с небольшими поправками применимы и для них.

Методы очистки памяти в секциях инициализированных/неинициализированных данных приложения и разделяемых библиотек

При завершении приложения, то есть при выполнении системного вызова `exit_group`, необходимо очищать секции данных приложения и всех подключенных к нему разделяемых библиотек. Однако из структуры процесса `task_struct` можно найти лишь адреса начала и конца секции данных самого приложения. На данный момент нами не было найдено действенного способа поиска адреса секции неинициализированных данных или секций данных для разделяемых библиотек. Но, к счастью, все эти секции расположены в одной области памяти, а так как мы знаем адрес, который точно находится в этой области памяти, то можно найти дескриптор данной области памяти (структуру типа `vm_area_struct`). В этой структуре содержится начальный и конечный адреса интересующей нас области памяти, поэтому очищая память в этом диапазоне адресов сразу очищаются и все указанные секции.

Методы очистки стека приложения

Со стеком приложения все относительно просто. Адрес начала стека и его размер в страницах можно узнать из структуры `task_struct` для текущего процесса. Единственное, что нужно помнить – стек растет вверх, а не вниз (соответственно адрес его начала больше адреса его конца).

Приведем пример кода для очистки стека приложения (необходимо выполнить при перехвате системного вызова `exit_group`):

```
unsigned int size = current->mm->stack_size * PAGE_SIZE;
char *start = (char *) (current->mm->stack_start - size);
memset(start, 0, size);
```

Методы очистки стека потока

Со стеком потока дела обстоят иначе. На уровне ядра ОС потоки (`thread`) и процессы (`task_struct`), вообще говоря, не различаются. По сути, поток представляет собой «облегченный» процесс (поток может разделять с каким-нибудь процессом некоторые ресурсы: память, используемые файловые

объекты и т.д.). Часто поток может иметь свой стек и прочие области памяти (описанные в его структуре `task_struct`). При создании многопоточных приложений вызываются те же самые системные вызовы (системный вызов `clone(2)`), что и при создании процессов, только с установленными флагами по «наследованию» ресурсов (`CLONE_VM`, `CLONE_FS`, `CLONE_FILES`, `CLONE_SIGHAND`). При этом каждый поток будет иметь собственную («облегченную») структуру `task_struct` и свой уникальный идентификатор PID (`process id`). Но при этом все потоки и процесс, который порождает множество потоков, будут иметь один и тот же идентификатор группы потоков TID (`thread id`). Изначально у процесса, порождающего потоки, `PID=TID`.

Поэтому методы для очистки стека потока не будут отличаться от очистки стека приложения. Так как потоки выполняются на уровне ядра ОС как обычные процессы (используются те же механизмы управления процессами в ОС), то и очистка памяти их стека будет осуществляться в методе, описанном выше (при вызове системного вызова `exit`).

Методы очистки области памяти отображенных файлов

Вызовы `mmap`, `mremap` и `mmapr` используются не только для выделения памяти в куче. Главное их предназначение – это отображение файлов в оперативную память. Файл читается с диска в память, процесс работает с этой памятью, а потом изменения записываются на диск. Для очистки памяти в этом случае в вызове `mremap` нужно делать все то же самое, что и для случая очистки памяти в куче, с одним отличием – необходимо проверять, существует ли страница для данного адреса в памяти.

Так как операция чтения с диска занимает относительно долгое время, ядро ОС не осуществляет загрузки сразу всего файла в память – данные считываются по мере необходимости (например, при запросе данных, которые еще не были загружены). Таким образом, необходимо очищать память областями по 4096 байт (размер страницы), а перед очисткой проверять, существует ли эта страница в памяти. Проверить это можно, например, посмотрев на код возврата макроса `put_user`, который записывает данные в адрес пространства пользователя – передаем функции `put_user` адрес в странице, и смотрим на код возврата. Если макрос вернул 0 – очищаем страницу, иначе – игнорируем ее.

Для системного вызова `mmapr` поступить аналогично нельзя, ведь если вызов `close` для файла вызовется после `mmapr`, то в файл запишутся нули (или произвольные данные, смотря как очищать), что приведет к нарушению работы ОС/приложения. То есть в данном случае необходимо еще перехватывать и вызов `close`. На данный момент решение этой проблемы находится в проработке, возможные варианты решения сводятся к определению (запоминанию) всех страниц, соответствующих файлу, в памяти с последующим вызовом `close` и очисткой этих областей памяти. Указанный способ может сильно сказаться на производительности всей системы.

Оставшиеся области памяти

Если к моменту завершения программы (системный вызов `exit_group`) не освобождены какие-либо области памяти отображенных файлов, или просто анонимные области памяти (т.е. не принадлежащие файлу, выделенные с помощью `mmap` с флагом `MAP_ANONYMOUS`), их необходимо очистить в случае, если они не принадлежат файловым отображениям, разрешают запись и не являются разделяемой памятью.

Выводы

В данной статье рассмотрены проблемы очистки оперативной памяти в ОС семейства Linux при ее перераспределении, и предложены пути решения этих проблем. Некоторые проблемы сложно решить без потери производительности. При проведении ряда тестов, рассмотренные в статье методы замедляли работу приложений (и, соответственно, ОС) примерно на 1-2%, что вполне удовлетворяет поставленной задаче по минимизации влияния механизмов очистки на общую производительность системы. Однако в отдельных ситуациях производительность определенного приложения могла упасть в два и более раз.

Стоит отметить, что указанные подходы к очистке памяти необходимо использовать в СЗИ НСД совместно с дополнительными политиками разграничения доступа и механизмом контроля потоков информации, что и реализуется в продукте компании «ОКБ САПР» ПАК СЗИ НСД «Аккорд-Х». Только в случае использования такого средства защиты становится возможным гарантировать сохранность критически важной информации, хранящейся и обрабатываемой в ОС семейства Linux.

LINUX: ОБЪЕКТЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ

А.М. Каннер,
ОКБ САПР, г. Москва

С учетом сложившейся в последнее время тенденции к широкому распространению ОС семейства GNU Linux (программы внедрения «свободного» ПО в учебных и государственных учреждениях РФ, повсеместное встраивание Linux в большое количество портативных электронных устройств) все чаще приходится задумываться о дополнительных мерах защиты данных, которые хранятся и обрабатываются в среде ОС Linux.

Разнообразные дистрибутивы Linux «из коробки» предоставляют достаточно широкий выбор штатных средств

защиты пользовательских данных (такие как средства защиты межсетевого взаимодействия, стандартные и расширенные средства идентификации и аутентификации, права доступа к объектам файловых систем, дополнительные списки контроля доступа – Access Control Lists и расширенные атрибуты файловых объектов, разнообразные фреймворки для расширенных настроек безопасности – SELinux, Tomoyo, AppArmor и т. д.). В целом, можно сказать, что при правильной на-

стройке таких штатных средств защиты ОС семейства Linux являются в достаточной степени защищенными. Однако это является истиной только в случае, когда не учитывается возможность неправомерного физического доступа некоторого злоумышленника к самому носителю данных или СВТ (вопрос защиты от физической кражи в данной статье освещаться не будет – это необходимо обеспечивать соответствующими организационными мерами). При таком доступе ничто не может помешать, например, изменить правила работы штатных средств защиты или вмешаться в штатный режим загрузки ОС.

Вследствие этого факта, а также опираясь на следствие из теоремы об использовании резидентного компонента безопасности (РКБ) [1], для «полноценной» защиты от несанкционированного доступа (НСД) в ОС семейства Linux (вообще говоря, это же справедливо для любых ОС) должен существовать некоторый внешний (по отношению к СВТ) аппаратный компонент, который и будет обеспечивать «полноценность» работы штатных или дополнительных программных механизмов защиты. В качестве такого аппаратного компонента принято использовать аппаратные модули доверенной загрузки (АМДЗ), которые применительно к ОС Linux должны контролировать целостность как минимум следующих компонент:

- главная загрузочная запись (Master Boot Record, MBR);
- загрузочный сектор основного раздела ОС Linux (Partition Boot Record, PBR), если загрузчик ОС при установке был записан в PBR, а не в MBR;
- сектора 1-63 относительно начала загрузочного раздела (некоторые загрузчики, например GRUB, записывают сюда свою часть – grub stage 1.5);
- непосредственно сам загрузчик (в случае GRUB – /boot/grub/stage2);
- файлы конфигурации загрузчика (/boot/grub/grub.conf, возможно ссылку /boot/grub/menu.lst);
- ядро ОС Linux – /boot/vmlinuz-*.*.xxx (в различных дистрибутивах наименование может отличаться);
- initramfs-образ или образ начальной загрузки – /boot/initrd-*.*.xxx.img (в различных дистрибутивах наименование может отличаться);
- какие-то файлы конфигурации и критичные данные ОС (настройки СЗИ НСД и т. д.).

Этот список, устоявшийся, и его было принято считать достаточным для корректной защиты ОС Linux и, в дальнейшем, программных средств защиты от НСД, начиная с раннего этапа загрузки.

Так или иначе, ядро Linux достаточно давно предоставляет возможность динамически загружать дополнительный функционал (выполняемый в kernel mode) с помощью загружаемых модулей ядра – Loadable Kernel Modules (LKM). При этом, если против загрузки в ОС «несанкционированных» модулей еще есть средства защиты (начиная от прав доступа в ОС), то для контроля целостности самих модулей (например, стандартных модулей для поддержки работы ЖД и т. д.), как правило, никаких средств не используется. Также нужно понимать, что такие модули ядра могут загружаться на раннем этапе загрузки ОС – т.е. до начала работы многих средств защиты информации (при этом, само действие по загрузке модуля ядра несколько отличается от запуска на выполнение бинарного файла, при котором обычно

применяют динамический контроль целостности¹). Рассмотрим, чем может быть опасно нарушение целостности модулей ядра ОС Linux.

Инъекция кода в модули ядра Linux

Опасность кроется в том, что существует возможность внедрить некоторый произвольный код в какой-то стандартный модуль ядра (который заведомо загружается по умолчанию), а также обеспечить повторную загрузку этого кода даже после перезагрузки ОС. Причем нужно отметить, что данная возможность существует скорее не за счет какой-то уязвимости в механизме LKM, а за счет особенностей используемого в Linux формата бинарных данных ELF (Executable and Linking Format). Особенность данного формата, которая будет нас сейчас интересовать, заключается в том, что:

1. В процессе линковки/компоновки (linking, т.е. процесса преобразования одного или нескольких скомпилированных объектных файлов в один исполняемый) двух объектных файлов ELF-формата линковщику (linker) необходимо получить некоторую информацию об используемых обоими файлами символах (symbols), например, об используемых функциях или глобальных переменных;

2. Каждый файл ELF-формата содержит в себе 2 секции, содержащие информацию для описания символов – .symtab и .strtab.

Далее необходимо привести краткое описание секций .symtab и .strtab, которое незаинтересованный читатель может пропустить и продолжить читать следующий абзац с сутью использования нами этих секций. В секции .symtab содержатся структуры с данными для линковщика по всем используемым символам ELF-файла (в частном случае – функциям). В каждой структуре есть поле st_name, которое представляет из себя индекс символа в секции .strtab. По указанному индексу в .strtab содержится null-terminated строка – фактически имя символа, при этом смещение секции .strtab определяется механизмом Section name resolution mechanism [2] – т.е. фактически смещение известно (можно определить).

Справочные материалы выше предназначены лишь для того, чтобы понимать – в ELF-формате любой символ можно найти по имени (и, если нужно, каким-либо образом изменить, однако, измененное имя по-хорошему должно содержать то же количество символов). Что вообще это может дать в нашем случае применительно к модулям ядра Linux? По сути, нам становится доступным изменение точки входа модуля ядра и/или выполнение некоторой внешней по отношению к модулю функции до его основного функционала (или если нужно, после).

Не будем вдаваться в глубокое описание того, как именно происходит загрузка модулей ядра в ОС Linux (и в то, что в ходе этой загрузки происходит обращение к символам из формата ELF), для более глубокого изучения читатель может воспользоваться соответствующими материалами [3]. Пр продемонстрируем непосредственно пример возможности инъекции кода. Для этого нужно создать два модуля ядра:

В результате сборки у нас получится модуль origmod.ko (будем считать его исходным), который при загрузке будет

¹ Этот механизм в «классической» реализации применяется непосредственно перед запуском на выполнение бинарных файлов

Тестовый модуль ядра	Инъектируемый модуль
origmod.c: <pre>#include <linux/module.h> int init(void) { printk(KERN_ALERT «original init\n»); return 0; } void clean(void) { printk(KERN_ALERT «original exit\n»); return; } MODULE_LICENSE(«GPL»); module_init(init); module_exit(clean);</pre>	evilmod.c: <pre>#include <linux/module.h> /** init() wrapper */ extern int init(); int evil(void) { printk(KERN_ALERT "evil inject!"); /** * here should be injected code */ /** here we can call init() function of the original module */ init(); return 0; } MODULE_LICENSE("GPL");</pre>
Makefile: <pre>SRC := origmod.c KERNEL_SOURCE_DIR := /lib/modules/\$(shell uname -r)/build obj-m := origmod.o all: \${SRC} \${HEADERS} Makefile \${MAKE} modules -C \${KERNEL_SOURCE_DIR} M=\${shell pwd} clean: -rm -f *.ko *.o -rm -f *.mod.* *.cmd -rm -rf .tmp_versions -rm -f Module.symvers Module.markers modules.order .PHONY: all clean cscope tags .DELETE_ON_ERROR:</pre>	Makefile: <pre>SRC := evilmod.c KERNEL_SOURCE_DIR := /lib/modules/\$(shell uname -r)/build obj-m := evilmod.o all: \${SRC} \${HEADERS} Makefile \${MAKE} modules -C \${KERNEL_SOURCE_DIR} M=\${shell pwd} clean: -rm -f *.ko *.o -rm -f *.mod.* *.cmd -rm -rf .tmp_versions -rm -f Module.symvers Module.markers modules.order .PHONY: all clean cscope tags .DELETE_ON_ERROR:</pre>

выводить в dmesg строку «original init» (module_init определяет «точку входа» в init()), а при выгрузке – «original exit» (module_exit -> clean()). Модуль evilmod.ko (инъектируемый модуль) содержит функцию evil(), которая выводит сообщение «evil injected», а затем вызывает init() (сам модуль содержит символ init(), который не определен, поэтому отдельно загрузиться не сможет).

Рассмотрим полученные модули origmod.ko и evilmod.ko с точки зрения формата ELF, выполнив \$ objdump -t origmod.ko и \$ objdump -t evilmod.ko:

Теперь воспользуемся возможностью ld и слинкуем

оба модуля в модуль evilorigmod.ko (\$ ld -r origmod.ko evilmod.ko -o evilorigmod.ko), при этом таблицы символов будут дополнены недостающими символами из evilmod.ko и origmod.ko (важно, чтобы в модулях не было повторяющихся символов). Опция -r позволяет создать модуль того же формата, что и линкующиеся модули, поэтому модуль evilorigmod.ko будет содержать в себе функции двух модулей, из которых слинкован, и при этом останется загружаемым модулем ядра – его можно загрузить в ядро ОС. Полученный модуль evilorigmod.ko будет иметь следующие символы:

Тестовый модуль ядра	Инъектируемый модуль
<pre>origmod.ko: file format elf32-i386 SYMBOL TABLE: 00000011 g F .text 00000010 cleanup_module 00000000 g F .text 00000011 init_module 00000011 g F .text 00000010 clean 00000000 *UND* 00000000 printk 00000000 g F .text 00000011 init</pre>	<pre>evilmod.ko: file format elf32-i386 SYMBOL TABLE: 00000000 g F .text 00000016 evil 00000000 *UND* 00000000 printk 00000000 *UND* 00000000 init</pre>

evilorigmod.ko: file format elf32-i386
SYMBOL TABLE:

```
.....
00000024 g F .text      00000016 evil
00000000 g O .gnu.linkonce.this_module 00000154 __this_module
00000011 g F .text      00000010 cleanup_module
00000000 g F .text      00000011 init_module
00000011 g F .text      00000010 clean
00000000 *UND*      00000000 printk
00000000 g F .text      00000011 init
```

Теперь, можно изменить «точку входа» в модуль init_module (инструментарий доступен в [3]), при этом таблица символов должна принять следующий вид:

evilorigmod.ko: file format elf32-i386
SYMBOL TABLE:

```
.....
00000024 g F .text      00000016 evil
00000000 g O .gnu.linkonce.this_module 00000154 __this_module
00000011 g F .text      00000010 cleanup_module
00000024 g F .text      00000011 init_module
00000011 g F .text      00000010 clean
00000000 *UND*      00000000 printk
00000000 g F .text      00000011 init
```

При загрузке полученного модуля evilorigmod.ko, будет выведено следующее:

[20436.323297] evil inject!

[20436.323298] original init

Таким образом, мы добились полной работоспособности модуля при добавлении внешнего функционала. Необходимо также отметить, что аналогичным образом можно инжектировать код в процедуру выгрузки модуля clean(), т.е. фактически мы можем полностью инжектировать один модуль ядра в другой.

Аналогичным образом можно инжектировать некоторый модуль в какой-либо стандартный модуль ядра, загружаемый ОС по умолчанию (usbhid.ko, pcspkr.ko и пр., исходные коды модулей иметь не обязательно), при этом контрольные суммы такого модуля естественно будут изменены. Однако, таким образом, можно обеспечить повторное выполнение инжектируемого кода после перезагрузки ОС, при котором не наблюдается каких-либо подозрительных модулей (что сразу бы насторожило администратора). При этом различные системы обнаружения вторжений (HIDS, Host Intrusion Detection System) со стандартными настройками не обнаружат подмены, т.к. модули ядра не являются ни исполняемыми модулями, ни suid-файлами.

Описанная выше ситуация с инжектированием кода в модули ядра также характерна для ОС Solaris, OpenBSD, FreeBSD, NetBSD (с несущественными изменениями).

Выводы

Описанная в статье техника внедрения постороннего кода в модули ядра достаточно опасна, в т.ч. и для современных систем Linux с ядром ветки 3.* (а также для других Unix-подобных ОС). Такое внедрение позволяет, во-первых, выполнять свой код на уровне ядра ОС, а во-вторых, внедрять этот код не слишком заметным способом. Так или иначе указанные возможности уже предполагают, что в системе есть права суперпользователя (иначе, невозможно осуществить выгрузку/загрузку модуля ядра, подменить его в /lib/modules/... или в образе начальной загрузки ОС initrd), однако, в любом случае лучше предпринять какие-то защитные меры.

В первую очередь, желательно контролировать целостность тех модулей ядра, которые автоматически загружаются при загрузке ОС. К сожалению, размер всех модулей на современных ОС Linux (каталог /lib/modules) уже «из коробки» может быть порядка 90-100 Мб и более, поэтому простой статический контроль целостности в данном случае будет выполняться непозволительно долго. Есть вариант дополнить динамический контроль целостности – проводить его не только для бинарных файлов при выполнении ехесве(), а для любых файлов вне зависимости от операции. Данный вариант дополнительно предоставляет возможность провести контроль целостности не только самих бинарных файлов, но и всех используемых ими разделяемых библиотек (/usr/lib, /lib).

Во-вторых, желательно использовать подсистему разграничения доступа, которая бы могла перехватывать и анализировать легитимность загрузки модулей ядра (т.е. перехватывать системный вызов sys_init_module и т.д.).

Оба этих подхода планируется развивать в рамках продукта компании ОКБ САПР – ПАК СЗИ НСД «Аккорд-Х».

Литература:

1. Коняевский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – С. 50.
2. Tool interface specification on ELF // TIS Committee, 1995.
3. Infecting loadable kernel modules: kernel versions 2.6.x\3.0.x // Phrack (Volume 0x0e, Issue 0x44, Phile #0x0b of 0x13), <http://www.phrack.org/issues.html?issue=68&id=11#article>

LINUX: К ВОПРОСУ О ПОСТРОЕНИИ СИСТЕМЫ ЗАЩИТЫ НА ОСНОВЕ АБСОЛЮТНЫХ ПУТЕЙ К ОБЪЕКТАМ ДОСТУПА

А.М. Каннер,
ОКБ САПР, г. Москва

Различные средства защиты от несанкционированного доступа (СЗИ НСД) в Linux, как это и следует из их предназначения, призваны разграничивать доступ различных субъектов доступа к объектам – т.е. к файловым объектам в рамках файловых систем (ФС) ОС. При этом штатные средства защиты в ОС руководствуются в своей работе атрибутами доступа к файловым объектам. Соответствующие же

атрибуты доступа входят в состав мета-данных файловых объектов (сам же механизм разграничения доступа внешний по отношению к ФС), т.е. фактически «неотделимы» от самих данных, содержащихся в файлах – файл = метаданные + данные.

Такая «привязка» атрибутов доступа непосредственно к защищаемым данным является логичной и правильной – за-

щищаемые данные однозначно идентифицированы, а атрибуты доступа, содержащиеся в метаданных, соответствуют вполне определенным блокам с данными (метаданные могут соответствовать только одним данным, т.е. одной цепочке кластеров с данными в ФС, а данные определяются только одними метаданными).

При разработке дополнительных «навесных» средств разграничения доступа, перед разработчиком встает (по крайней мере, должен встать) насущный вопрос – «каким образом идентифицировать защищаемые данные?», т.е., как реализовать работу собственных политик разграничения доступа, чтобы защищать именно те данные, которые были поставлены на контроль?

Дать однозначный ответ не так просто. Можно воспользоваться, по крайней мере, следующими вариантами идентификации объектов доступа в ОС Linux:

- использование абсолютного пути (absolute path) к файловым объектам;
- использование прав разграничения доступа (ПРД) на основе своих атрибутов в метаданных файловых объектов (т.е. добавление своих метаданных);
- использование не абсолютного пути к объекту в ФС, а разграничение доступа к объектам виртуальной файловой системы (VFS) ядра ОС Linux – inode/dentry и т.п. (т.е. фактически к самим метаданным, по которым осуществляется доступ к данным).

Кратко рассмотрим каждый из перечисленных вариантов.

Использование абсолютных путей в ПРД

Наиболее очевидным способом задания ПРД для объекта доступа является указание абсолютного пути к этому файловому объекту в ОС. К сожалению, данный подход при задании ПРД для СЗИ НСД в ОС Linux при всей своей простоте кроет в себе существенные недостатки, а именно:

- неоднозначность абсолютного пути до защищаемого объекта при изменении правил монтирования файловых систем (при разбиении корневой ФС на несколько различных ФС, например, если изменить правила в /etc/fstab);
- возможность «смонтировать» каталог, содержащий защищаемый объект в другую точку монтирования (из которой можно получить доступ к файловому объекту, используя другой абсолютный путь);
- возможность смены корневого каталога с последующим обращением к защищаемому объекту фактически по относительному пути (chroot);
- возможность при переименовании объекта избежать действия ПРД;
- возможная несвязанность файлового объекта с защищаемыми данными (например, объект доступа может являться символической ссылкой);
- и т.д.

Перечисленные недостатки приводят нас к тому, что в СЗИ НСД в ОС Linux кроме стандартных механизмов разграничения доступа должны присутствовать:

1. Механизм контроля точек монтирования – т.е. СЗИ НСД должно контролировать монтирование разделов (каталогов) в различные точки ФС (правила для монтирования при загрузке ОС можно полностью скопировать из /etc/fstab), а при нарушении правил монтирования – не выпол-

нять монтирование. Такие правила можно дополнительно составлять отдельно для различных пользователей.

2. Механизм «пополнения»/изменения ПРД, например, при создании новых объектов или переименовании существующих.

Особые проблемы появляются при возникновении необходимости одновременно смонтировать ФС в две точки монтирования – в данном случае при обращении по разным абсолютным путям к объектам доступа СЗИ НСД должно либо перенести вопрос правомерности такого доступа на пользователя (администратора), либо само перебирать на уровне ядра ОС всевозможные точки монтирования для объекта (структура vfstmount) и запрещать доступ, если доступ запрещен хотя бы в одной точке монтирования. Аналогичным образом СЗИ НСД должно поступать в случаях, когда на уровне ядра не представляется возможности определить точку монтирования (если файловый объект располагается на отличной от корневой ФС – на уровне ядра путь к объекту иногда можно определить только относительно точки монтирования этой ФС, т.е. путь будет относительным).

Так или иначе, все это не позволяет решить основную проблему при использовании абсолютных путей для файловых объектов – возможная несвязанность указываемого пути к объекту доступа непосредственно с защищаемыми данными. Поэтому, в дополнение к указанным дополнительным механизмам защиты, лучше осуществлять идентификацию объекта доступа в СЗИ иначе (см. способы ниже).

Дополнение метаданных собственными атрибутами доступа

В данном случае, как и в случае со штатными атрибутами доступа в ОС, дополнительные атрибуты доступа предполагается хранить вместе с метаданными файловых объектов (в некотором дополнительном атрибуте ФС или как-то иначе), а не отдельно от них и соответственно от самих данных. Используя такой способ «привязки» атрибутов доступа к данным, удастся избежать всех недостатков идентификации субъектов доступа по абсолютному пути:

- в случае изменения порядка монтирования ФС в ОС, при монтировании каталога с защищаемыми объектами доступа к какой-либо другой точке монтирования или при смене корневого каталога (chroot) ПРД будут продолжать действовать, т.к. «связанность» атрибутов доступа с данными в данном случае не нарушается (в отличие от случая использования абсолютных путей);

- в случае переименования объекта доступа или при обращении к этому объекту с использованием символических ссылок ПРД будут также учитывать атрибуты доступа самого объекта доступа (дополнительного «пополнения» ПРД самим СЗИ в случае переименования объекта доступа не требуется).

Даже в случае переноса носителя данных на другое СБТ, в случаях копирования данных или при переустановке ОС легко возобновить работу СЗИ, т.к. атрибуты доступа будут переноситься вместе с самими данными (если это будет поддерживаться в соответствующих ФС).

Кроме всего прочего, необходимо отметить, что при таком дополнении метаданных объектов доступа отсутствует необходимость в контроле точек монтирования, однако, механизм «пополнения» ПРД при создании новых объектов доступа должен присутствовать (нужно заносить

некоторые стандартные атрибуты доступа в метаданные созданного объекта).

Отрицательной чертой такого подхода является то, что фактически изменяются сами данные (добавление метаданных – тоже изменение файла), что может вызвать подозрение как у администратора, так и у некоторых средств защиты (HIDS, Host Intrusion Detection System). Кроме того, этот подход может быть недоступен для некоторых типов файловых систем (или как минимум будет требовать отдельной реализации для многих типов файловых систем, которых в ОС Linux поддерживается огромное количество).

Контроль доступа к структурам VFS в ядре ОС Linux

Рассмотрим вариант адаптации метода использования абсолютных путей для идентификации объектов доступа. Существует вариант контроля доступа к данным не по абсолютным путям к файловым объектам, а с использованием механизма контроля доступа к объектам, представляющих собой сами файловые объекты на уровне ядра ОС Linux – inode/dentry и т.п. Поскольку такие объекты формируются при загрузке ядра ОС (вообще говоря, при загрузке соответствующего модуля ядра для поддержки определенного типа ФС и после монтирования раздела с таким типом ФС), то изначально все равно придется использовать абсолютные пути до объектов доступа. Однако после монтирования всех необходимых ФС открывается возможность «сопоставить» абсолютные пути для всех заданных объектов доступа конкретным inode/dentry на уровне ядра ОС и контролировать доступ именно к ним (а не пытаться каждый раз построить абсолютный путь по известным inode/dentry). Такой подход позволяет:

- частично избавиться от неоднозначности при изменении порядка монтирования ФС (inode/dentry будут оставаться неизменными, будет изменяться структура, определяющая точку монтирования, vfstmount);

- решить проблему с переименованием объекта (в рамках текущей работы ОС) и обращениями по символьным ссылкам (в любом случае доступ будет осуществляться в inode/dentry,

однако, дополнительно нужно занести inode-объект, а не его ссылку, в ПРД).

При всех плюсах такой метод контроля доступа необходимо сочетать с уже перечисленными механизмами контроля точек монтирования (как минимум, это требуется в самом начале для корректного «сопоставления» абсолютных путей с inode/dentry) и «пополнения»/изменения ПРД (например, для тех же объектов-ссылок или создаваемых объектов). Кроме того, должен присутствовать механизм, который будет решать, что делать с объектом (по абсолютному пути), которого в системе уже нет (но, возможно, может появиться, например, при дальнейшей загрузке или работе ОС), – в какой момент строить для него «соответствие» и строить ли вообще.

Выводы

При выборе СЗИ часто (если не всегда) не очевидно, каким образом оно идентифицирует защищаемые объекты ОС и правильно ли вообще функционирует. Кроме того, вопрос идентификации объекта доступа граничит с «доступностью» этого метода для понимания рядовым пользователем/администратором. В связи с этим, достаточно многие СЗИ строятся на базе идентификации объекта доступа по абсолютным путям (что, несомненно, является наиболее простым для понимания способом), не вводя дополнительно в ОС Linux каких-то сторонних механизмов защиты, описанных в данной статье. Если говорить про ОС семейства Windows, такие дополнительные механизмы, как контроль точек монтирования, там вообще избыточны (если не изменена конфигурация и порядок подключения носителей информации, то нумерация и обозначение разделов, а также абсолютные пути всегда будут неизменными).

Мы в ОКБ САПР стараемся учитывать особенности защищаемой среды (если говорить о данной статье – особенности ОС семейства Linux) при проектировании своих СЗИ. Механизм контроля точек монтирования изначально включен в продукт ОКБ САПР ПАК СЗИ НСД «Аккорд-Х», дополнительные механизмы постепенно внедряются и находят свое место в этом решении.

КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ В РЕШЕНИИ ПРИКЛАДНЫХ ЗАДАЧ

С.В. Конявская,
ОКБ САПР, г. Москва

Проблема века – имитация бурной деятельности – требует в качестве необходимого условия неясности предмета, позволяющей предельно «усложнять» задачи, повышая, тем самым, стоимость их решения. За счет многообразия применяемых технологий и инфраструктур дроблением объектов защиты удается сегодня мотивировать применение в любой системе любого набора средств защиты информации. Это перегружает системы, делает их плохоуправляемыми и ненадежными (растет количество возможных точек отказа, функции многократно дублируются, что ведет к неизбежным ошибкам настроек и возникновению конфликтов). В каждом конкретном случае можно доказывать, что нужно защищать – ключи или справочники сертификатов, и что лучше – отражать атаки виртуальных машин на виртуальные машины, или обеспечивать невозмож-

ность осуществления такой атаки, однако, это всякий раз будут точечные выводы, не меняющие основного подхода: выделить новую сущность и предложить новое решение для ее защиты.

Альтернативой представляется методологический прием – возведение каждого явления, предполагаемого к защите, к классификации объектов защиты информации.

Наиболее высокой степенью абстрагированности от инфраструктур различных типов характеризуется классификация, предложенная В.А. Конявским. Предельно коротко ее можно свести к следующему тезису.

В процессе информационного взаимодействия на разных его этапах заняты люди (операторы, пользователи) и используются средства информатизации – технические (ПЭВМ, ЛВС) и программные (ОС, ППО). Информация (сведения) порождается

людьми, затем преобразовывается в данные и представляется в АС в виде информационных ресурсов. Данные между компьютерами передаются по каналам связи. В процессе работы АС данные преобразовываются в соответствии с реализуемой информационной технологией.

Таким образом, объектов защиты оказывается четыре:

- компьютеры;
- данные;
- каналы;
- информационные технологии.

Задачей формирования этой классификации при ее создании было выявление и обоснование информационной технологии как отдельного объекта защиты, и эта задача была решена, сейчас сложно себе представить, что этот объект не выделяется или считается не существенным.

Однако возникло понимание необходимости уточнения этой классификации в других ее частях.

Этому и посвящены нижеследующие выкладки.

Информационная технология – это понятие, описывающее процесс изменения данных.

Тезис этот может показаться неочевидным, если исходить из определения, данного в ГОСТ «Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных». Однако обратим внимание, что это определение не касается сущности понятия, а описывает его через обстоятельства, в которых оно проявляется. Это «приемы, способы и методы» даже не выполнения перечисленного ряда действий, а используемые при их выполнении. То есть тогда, когда они выполняются. В какой еще зависимости они находятся, кроме временной, ГОСТом не определяется.

Таким образом, это определение не дает ни явного подтверждения, ни опровержения тому, что результатом действия технологии обязательно является изменение данных.

Кроме обращения к ГОСТ, можно прибегнуть к методу выведения содержания из определения понятия, родового по отношению к рассматриваемому. То есть из определения понятия «технология» (так как информационная технология – это определено технология, просто не любая).

«Технология – всегда процесс производства продукта. Информационная технология (ИТ) – процесс производства информационного продукта. Та или иная совокупность информационных продуктов называется информационным ресурсом. В процессе производства продуктов используются материалы, средства производства и технологии производства. В информационном производстве средства производства – это средства вычислительной техники (СВТ) и информационные системы (ИС) на их основе, технологии – это ИТ, а материалы – информация в том или ином виде – преимущественно в виде сообщений в электронной форме». Такая длинная цитата приведена для того, чтобы сделать акцент на следующем: у информационной технологии входные и выходные данные различны (одни являясь материалом, а вторые – продуктом), иначе, применение технологии необосновано. В процессе производства должно быть что-то произведено, иначе процесс определенно поставлен неверно.

Интуитивно – именно это обычно понимается под «обработкой» данных, и не это – под «хранением». Интуитивно, потому что общепринятого терминологического определения обработки данных на сегодняшний день нет (в техническом смысле, а не в смысле регулирования отношений граждан, как,

в частности, в ФЗ-152 – такого рода определения для классификации технической стороны вопроса неприменимы).

Итак, обработка данных – это процесс, в ходе которого они как-то меняются.

В общем случае – предсказуемо меняются. Вспомним гениальное определение Кузнецова Николая Александровича: «Информация – это то, что сохраняется при вычислимом изоморфизме». Если изоморфизм нарушен, информация утрачена.

Поэтому, как правило, результат разрушительного программного воздействия на данные «обработкой» не называется. А вот преобразование из одного формата в другой называется, хотя изменения «содержания» данных не происходят.

Таким образом, обработка данных – это процесс исполнения информационной технологии. Которая, в свою очередь, напомним, является упорядоченной последовательностью операций над данными.

Кроме обработки данных, возможно еще их хранение. В отличие от обработки, когда данные меняются, хранение – это когда данные не меняются. Это, однако, не единственная полезная для классификации характеристика хранения. Важно также то, что при хранении данные остаются там же, где были сохранены. Они не перемещаются.

Стало быть, есть третий случай – когда данные перемещаются, но не изменяются – это передача. В данном контексте невозможно игнорировать тот факт, что защищенная передача данных предполагает в качестве обязательного требования неизменность данных при передаче. То есть данные перемещаются, но не изменяются.

Логика классификации детерминирует и четвертый случай – данные одновременно и перемещаются, и изменяются. Видимо, это говорит о том, что информационная технология может включать, а может не включать в себя передачу данных между инфраструктурными элементами (на которых функционируют инструменты, выполняющие операции над данными).

Итого.

- 1) Хранение – нет изменения, нет перемещения (00).
- 2) Передача – нет изменения, есть перемещение (01).
- 3) Обработка в рамках одного инфраструктурного элемента – есть изменение, нет перемещения (10).
- 4) Обработка в рамках разных инфраструктурных элементов – есть изменение, есть перемещение (11).

Так, данные могут храниться, передаваться и обрабатываться. Отражая это на приведенную выше классификацию, получаем две точки, в которых отражение происходит не идеально:

- компьютеры;
- данные.

Казалось бы, две из четырех – это слишком много несоответствия (или слишком мало соответствия), чтобы можно было вообще говорить о сводимости классификаций.

Однако несоответствия эти имеют совершенно разную природу, что существенно снижает их критичность.

Очевидно, что «данные» выпадают из этого ряда ровно по той причине, что это предмет, общий для всех выделяемых объектов:

- каналы – это каналы передачи данных;
- информационные технологии – это технологии обработки данных;
- компьютеры – это ...

Логика классификации ведет к тому, что это средство (место) хранения данных.

Однако компьютер – это, конечно, не только место хранения. Это с тем же успехом и место (и что важнее – средство) их обработки. Он содержит и инструменты, и хранилища, и даже каналы передачи, в общем-то.

Видимо, в контексте данной классификации компьютер (или СВТ) необходимо заменить на «носитель». Это позволит избежать нарушения правила единого основания, обязательного для классификации, с одной стороны, а с другой – отражение «хранения» на «носитель» – абсолютно точно. Носитель – это средство хранения данных.

В результате, получаем следующую обобщающую классификацию объектов защиты, относящихся к предмету защиты, – «данные».

1. Носители (хранение).
2. Технологии (обработка).
3. Каналы (передача).

Отдельно данные, как самостоятельный объект защиты, не имеют смысла, поскольку защищать данные оказывается возможно только при хранении, обработке или передаче. Других состояний у них просто нет. И все это, с другой стороны, состояния именно данных.

Практическая польза этой, как и всякой другой классификации, заключается в возможности проверки ею концептуальных основ подсистем защиты тех или иных систем и

инфраструктур – как на предмет полноты, так и на предмет избыточности.

В частности, такая проверка делает предельно наглядной необоснованность тезиса о том, что в терминальных системах необходимо защищать только терминальный сервер и, в лучшем случае, каналы, а на терминальном клиенте достаточно только относительно надежно аутентифицировать пользователя, так как на терминальных клиентах не хранятся и не обрабатываются данные.

Делает возможным это утверждение именно неопределенность понятия обработки данных, которую в «бытовом» смысле очень привлекательно свести к изменению содержания.

Однако, если проверить эту логику тем, реализуют ли терминальные клиенты какую-нибудь технологию, становится очевидным, что да, реализуют: именно ОС терминального клиента поддерживает работу оборудования терминала (сетевая карта, видеокarta и так далее), именно в ней исполняется (как приложение) само ПО терминального клиента ICA или RDP, поддерживается работа протокола.

Ясно, что эти функции имеют значение с точки зрения обеспечения безопасности информации в системе, и ОС терминального клиента должна быть контролируемой.

ПРИНЦИПЫ И МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ В УСТРОЙСТВАХ С БЛОЧНОЙ ВНУТРЕННЕЙ СТРУКТУРОЙ

**В.В. Коробов,
ОКБ САПР, г. Москва**

Большой популярностью в современных персональных вычислительных средствах пользуются носители информации с блочной внутренней структурой, такие как USB Flash-накопители, SSD-диски, гибридные жесткие диски и пр. В данной работе рассмотрены особенности применения криптографических методов защиты данных в устройствах такого класса.

Традиционно основными требованиями безопасности информации является обеспечение конфиденциальности и целостности. Ниже рассматриваются проблемы обеспечения требований конфиденциальности и целостности данных, используемых в устройствах с блочной внутренней структурой.

Для обеспечения конфиденциальности данных применяется шифрование, целостность данных обеспечивается посредством использования контрольных сумм, хэш-функции, кодов аутентификации сообщений (КАС), а также аутентифицированного шифрования (семейство режимов шифрования, в которых дополнительно к обеспечению конфиденциальности обрабатываемых данных, достигается контроль целостности).

Защищая данные носителей информации с блочной внутренней структурой, необходимо определиться со следующими вопросами:

- какой режим шифрования должен использоваться?
- Каким образом обеспечить контроль целостности данных?
- Каким образом организовать ключевую систему?

Выбирая режим шифрования, необходимо понимать, каким образом будет осуществляться контроль целостности. Возможны следующие варианты:

- использование традиционных механизмов контроля целостности;

- использование аутентифицированного шифрования.

В первом случае, контроль целостности осуществляется путем вычисления и проверки криптографической контрольной суммы, вообще говоря, независимой от шифрования. Во втором случае, контроль целостности данных обеспечивается попутно самим режимом шифрования.

Режимы аутентифицированного шифрования (CCM [1], CS [2], CWC [3], XCBC [4], OCB [5], GCM [6] и подобные) в большей своей части подразумевают, что контроль целостности и обеспечение конфиденциальности будет выполняться совместно в рамках единого криптографического преобразования, что, в общем случае, не потребует выделения дополнительной памяти для сохранения значений данных, используемых при контроле целостности (значения хеш-функции или КАС). В то время, как использование традиционных режимов шифрования данных в устройствах рассматриваемого класса (подробнее см. [7]) совместно с механизмами контроля целостности (HMAC [8], режим выработки имитозащитной вставки ГОСТ 28147-89 [9], CBC-MAC [10] и другие) страдает от этого недостатка. В некоторых случаях это может привести к выделению дополнительных регионов памяти в ущерб общему полезному объему устройства.

В данном случае речь идет о внутренних данных, используемых алгоритмами шифрования/проверки целостности. Контрольные суммы, как вычисляемые внешне, независимо, так и в процессе шифрования должны вносить примерно одинаковую избыточность в шифрованный текст для обеспечения одного и того же уровня имитозащищенности. Поэтому размер шифротекста превышает размер открытого текста в обоих случаях примерно на одну и ту же величину.

Помимо этого, применение традиционного подхода с использованием КАС или хэш-функций, вообще говоря, требует более значительного, чем при аутентифицированном шифровании, увеличения времени выполнения операций вычисления/проверки контрольной суммы, что замедляет чтение/запись данных на блочном носителе.

Таким образом, актуальной следует считать задачу дополнения алгоритма шифрования ГОСТ 28147 режимом аутентифицированного шифрования.

Правильная организация ключевой системы является еще одной важной задачей, возникающей при защите данных в устройствах с блочной внутренней структурой.

Корректно спроектированная ключевая система должна учитывать то, что каждый ключ может использоваться для защиты строго ограниченного объема данных. Поэтому существует необходимость в периодической смене ключей. Существуют две основные модели использования ключей, отталкиваясь от которых принимается решение об их смене:

- ключи используются некоторое, заранее установленное время (модель с конечным временем – МКВ);
- ключи используются для обработки некоторого, заранее установленного объема данных (модель с конечным ресурсом – МКР).

Наиболее распространенными методами организации ключевой системы являются:

- использование единственного ключа шифрования (мастер-ключа), применяемого для шифрования всех блоков данных;

- использование производных ключей, применяемых для шифрования блоков данных;

- генерация случайного ключа для шифрования каждого блока данных.

Рассмотрим достоинства и недостатки каждого из методов.

Очевидно, невозможно использовать один и тот же ключ для шифрования по ГОСТ 28147 данных всего блочного устройства сколь-нибудь серьезного размера, поскольку смена ключа по времени будет происходить слишком часто. Поэтому использование единственного мастер-ключа в серьезном изделии не безопасно.

В последнем случае – использование случайных ключей – накладные расходы возрастают значительно. Для корректной реализации необходимо осуществлять контроль характеристик ДСЧ и выделять дополнительные ресурсы для организации безопасного хранения ключа шифрования конкретного блока, что приводит к необходимости выделения дополнительных регионов памяти, и сокращению общего полезного объема устройства. Кроме того, необходимо контролировать ресурс мастер-ключа, используемого в этом случае для шифрования произвольных ключей, что при использовании МКР при организации ключевой системы нивелирует преимущества этого метода относительно более простых.

К слову, вариант производных ключей не сильно отличается от случайных ключей, поскольку требует хранения открытой информации, используемой функцией вычисления ключа. Для достижения необходимой энтропии ключа шифрования эта информация должна иметь практически те же размеры, что и зашифрованные случайные ключи.

Таблица 1 – Достоинства и недостатки методов организации ключевой системы

Метод организаций ключевой системы	Достоинства	Недостатки
Использование мастер-ключа	Простота реализации. Необходимость обеспечения безопасного хранения только одного ключа шифрования	Большой объем защищаемых данных на один ключ. Необходимость перешифрования больших объемов данных при смене ключа
Использование производных ключей	Использование уникального ключа для шифрования конкретного блока данных. Необходимость обеспечения безопасного хранения только одного ключа шифрования	Сложность реализации. Необходимость дополнительных вычислений при обращении к конкретному блоку данных. Необходимость перешифрования больших объемов данных при смене ключа шифрования. Необходимость обеспечения безопасного хранения открытых данных, используемых при вычислении производного ключа
Использование произвольных ключей	Отсутствие зависимости от компрометации ключей других блоков. Необходимость перешифрования небольших объемов данных при смене ключа шифрования	Сложность реализации. Необходимость обеспечения безопасного хранения множества ключей шифрования. Необходимость периодического контроля характеристик ДСЧ

Как видно из таблицы 1, относительно использования МКВ при организации ключевой системы предпочтение тому или иному методу отдать сложно и поэтому выбор конкретного метода должен определяться индивидуально. Единственное достоинство, которое выделяет метод случайных ключей, состоит в более простой операции перешифрования при смене мастер-ключа, поскольку смена мастер-ключа требует перевычисления всех производных ключей и перешифрования всех данных носителя, а случайные ключи можно не заменять, перешифровав только сами ключи, но не данные.

При реализации конкретного метода криптографической защиты данных в устройствах с блочной внутренней структурой необходимо соблюдать компромисс между состоянием защищенности данных и удобством использования устройства, на которое накладывают отпечаток общая скорость взаимодействия с устройством (скорость чтения/записи) и разумные рекомендации по администрированию устройства (частота смены ключей, возможность автоматизации этого процесса).

Литература:

1. SP 800-38 C Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality.

2. Cipher-State (CS). W. Erik Anderson, Cheryl L. Beaver, Timothy J. Draelos, Richard C. Schroepel, Mark D. Torgerson.

3. The CWC Authenticated Encryption (Associated Data) Mode. Tadayoshi Kohno, John Viega, Doug Whiting.

4. Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes. Virgil D. Gligor, Pompiliu Donescu.

5. OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption. Phillip Rogaway, Mihir Bellare, John Black, Ted Krovetz.

6. SP 800-38 D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.

7. Коробов В.В. Шифрование данных в устройствах с блочной внутренней структурой: Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15-18 мая 2012 года. – Суздаль (Россия). 2012. – С. 151-152.

8. NIST FIPS 198 The Keyed-Hash Message Authentication Code (HMAC).

9. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

10. ISO/IEC 9797-1:1999 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher.

СТАНДАРТ X.690: BER, CER И DER

А. Красавин,
ОКБ САПР, г. Москва

X.690 – один из стандартов ASN.1, разработанных совместно организациями ISO, IEC и ITU-T для удобства представления данных при их передаче в телекоммуникационных сетях. Правила кодирования, описанные в X.690, служат для представления структур данных, описанных по правилам ASN.1, в виде последовательностей байт. Такие последовательности удобнее передавать по линиям связи или сохранять в файлы, чем делать те же операции с самими структурами.

Правила кодирования, описанные в X.690, применяют в различных протоколах передачи данных и в криптографических протоколах, как-то: SMNP и LDAP, PKCS#7 (для кодирования сообщений), X.509 (для хранения сертификатов). В частности, в стандарте CMS (RFC #5652) говорится, что сообщение должно передаваться закодированным по правилам DER (описаны в X.690). Однако единой кроссплатформенной реализации правил кодирования на каждом из языков программирования, описанных в стандарте X.690, нет. Поэтому разработчикам ПО часто приходится реализовывать библиотеки для кодирования данных в соответствии с X.690. И тут возникает следующая проблема: очень сложно найти хорошее и понятное описание стандарта и правил кодирования на русском языке.

Собственно, задача этой статьи - дать именно такое описание.

Стандарт X.690 описывает следующие правила кодирования структур данных, созданных в соответствии с ASN.1: BER (BasicEncodingRules), CER (CanonicalEncodingRules), DER (DistinguishedEncodingRules). Разберемся с этими правилами подробнее.

BasicEncodingRules

Базовые правила кодирования или BER – правила для представления структуры, описанной с помощью ASN.1, в виде последовательности байт (или «октетов»). Такую последовательность удобнее передавать по линиям связи или сохранять в файл, чем делать те же операции с самими структурами.

Для того, чтобы различные типы данных можно было описывать схожим образом, в X.690 была определена общая структура блока закодированной информации, состоящая из следующих 3 частей:

- идентификатор – один или несколько октетов, в которых содержится информация о типе закодированных данных;

- часть, содержащая информацию о длине блока, – один или несколько октетов, в которых содержится информация о длине закодированных данных (в октетах);

- часть, содержащая закодированную информацию.

Рассмотрим подробнее эти части:

Идентификатор

Формат идентификатора строго фиксирован:

- биты 8 и 7 определяют класс данных (Universal (т.е. определенный в ASN.1), Application (используемый в каком-то конкретном приложении), Context-specific (т.е. зависящий от контекста)* или Private (т.е. определенный в какой-то спецификации ASN.1));

- бит 6 определяет, являются ли данные простыми (как-то INTEGER), или могут содержать в себе другие различные наборы данных (как-то SET). При этом, в первом случае говорят

о примитивном кодировании, а во втором – о конструктивном;
– биты 5-1 определяют тэг данных (их тип).

В случае, если класс данных не определен в ASN.1, то тэг может быть больше 30. В таком случае используют несколько октетов для представления идентификатора. При этом биты 5-1 первого октета имеют значение 11111(2), а следующие октеты, кодируются следующим образом:

- бит 8 во всех октетах, кроме последнего равен 1. В последнем октете длины бит 8 равен 0;
- биты с 1 по 7 этих октетов содержат биты тэга в его двоичном представлении.

Оклеты длины закодированных данных

В случае, если длина блока закодированных данных заранее известна, оклеты длины кодируются следующим образом:

- если эта длина не превышает 31 байта, то она просто записывается в соответствующий октет длины. Такая форма представления октетов длины называется примитивной (primitive);
- если длина блока закодированных данных больше 31 байта, то:
 - в биты второго и последующих октетов записывается значение длины блока закодированной информации в ее (длины) двоичном представлении;
 - в первый октет записывается количество дополнительных блоков длины, считая со второго (не более 30); бит 8 первого октета устанавливается в 1.

Такая форма представления октетов длины называется длинной (long).

Если же длина блока закодированных данных на момент кодирования длины неизвестна, то в октет длины записывается значение 0x80h, что указывает на кодирование с неопределенной длиной. В этом случае, в конце блока закодированных данных должно стоять значение 0x0000h (2 октета), явно указывающее на его завершение.

Кодирование структур различных типов

Кодирование различных типов данных детально и доступно описано в стандарте X.690 и затруднений при использовании вызывать не должно. Куда больший интерес вызывают особенности при кодировании различных типов данных.

В зависимости от структуры и преследуемых при кодировании целей, кодирование одних и тех же данных может существенно различаться. Так, кодирование значения TRUE типа BOOLEAN может иметь как вид: 01 01 01, так и вид: 01 01 0F.

Результат кодирования типа SET может быть различным, в зависимости от того, в каком порядке мы кодируем «вложенные» типы данных: если `set ::= SET{ int, float }`; `int ::= INTEGER`; `float ::= REAL`, то для `set{-128, 0.15625}` результат кодирования может быть таким: 31 08 02 01 80 09 03 80 FB 05, и таким: 31 08 09 03 80 FB 05 02 01 80.

В зависимости от того, примитивное или конструктивное кодирование используется, его результат может также различаться. Так для значения «Test User 1» типа STRING при примитивном кодировании результат будет иметь вид: 13 0B 54 65 73 74 20 55 73 65 72 20 31, а при

конструктивном: 33 0F 13 05 54 65 73 74 20 13 06 55 73 65 72 20 31.

Другие правила кодирования стандарта X.690

Как видно из предыдущих примеров, результат кодирования по правилам BER может существенно различаться. Для того, чтобы результаты кодирования одних и тех же типов данных в разных системах были одинаковыми, были разработаны правила кодирования DER и CER.

Distinguished Encoding Rules

Особые правила кодирования или DER совпадают с BER с учетом выполнения следующих ограничений:

- 1) для кодирования данных с известной длиной количество октетов длины должно быть наименьшим;
- 2) кодирование простых типов данных (в том числе STRING, OCTETSTRING и BITARRAY) всегда примитивное;
- 3) для типа SET кодирование вложенных типов должно происходить в порядке следования их тегов (согласно ASN.1).

Canonical Encoding Rules

Канонические правила кодирования или CER совпадают с BER с учетом выполнения следующих ограничений:

- 1) для составных типов данных должно применяться кодирование с неизвестной длиной;
- 2) для примитивного кодирования количество октетов длины должно быть наименьшим;
- 3) для типа SET кодирование вложенных типов должно происходить в порядке следования их тегов (согласно ASN.1).

Сравнение BER, DER и CER

В чем же преимущество различных правил кодирования?

BER предлагает пользователю различные пути для кодирования одних и тех же данных, причем предполагается, что система, которая поддерживает стандарты ASN.1, может корректно их декодировать вне зависимости от представления, в то время как DER и CER поддерживают только конкретный вариант кодирования для каждого типа. Это отличие проявляется в быстродействии кодирования данных: согласно исследованиям, если при кодировании используется строго определенный формат данных, то системе требуется для кодирования и декодирования намного меньше операций. Проще говоря, DER и CER обеспечивают большее быстродействие, чем BER.

Основное же отличие DER от CER заключается в том, что в DER используется кодирование данных с известной длиной, а в CER в некоторых случаях (например, при кодировании данных типа STRING длиной более 1000 символов) используется кодирование с неизвестной заранее длиной. Это отличие выражается в количестве блоков, необходимых для кодирования длины зашифрованных данных. Так, для определения длины блока закодированных данных при кодировании с неизвестной длиной требуется всего 3 октета, в то время как для больших сообщений при DER кодировании их количество может достигать 32 октета. То есть целесообразно использовать DER при кодировании небольших по размеру данных и CER – для больших.

ВЫНУЖДЕННАЯ НЕБЕЗОПАСНОСТЬ ПРИ ХРАНЕНИИ ПАРОЛЕЙ

В.В. Кравец,
ОКБ САПР, г. Москва

С широким распространением социальных сетей и других популярных Интернет-сервисов многие пользователи компьютеров начали понимать необходимость надлежащим образом обеспечивать свою безопасность при работе в Интернете. Легко представить ход мыслей обычного пользователя: «Если кто-то узнает мой пароль от социальной сети, то узнает с кем я общаюсь, о чем, как долго...», «Если кто-то узнает мой пароль от почты, то узнает какие новостные рассылки мне интересны, какие товары я покупаю, мои пароли от других сервисов...». Компрометация пароля к почтовому ящику приводит, пожалуй, к самым серьезным угрозам. Сейчас почти все сервисы используют привязку к e-mail, а значит, злоумышленник, получив доступ к почте, сможет получить доступ к аккаунтам привязанных сервисов, например, через функции, аналогичные восстановлению забытых паролей. Тот, кто знает, пароль может выдать себя за реального владельца аккаунта того или иного сервиса.

Все люди любят удобство. Создатели браузеров и программ для использования сервисов не хуже других знают это. Именно для того, чтобы пользоваться продуктом было удобно, многие программы включают такие функции, как «запомнить пароль», «сохранить пароль». Что же происходит, когда пользователь нажимает соответствующую кнопку?

Большинство систем безопасности работает на одном из двух аутентификационных признаков: «Я знаю что-то уникальное» или «Я владею чем-то уникальным». Границы между этими двумя понятиями не всегда достаточно четкие, но все-таки знание пароля больше подходит под первый пункт. Поэтому, когда мы вводим пароль, то мы тем самым предъявляем «имеющееся уникальное знание», которое сервер проверяет. Мы нажали кнопку «сохранить пароль» и наше знание оцифровывается, переводится в последовательность байт и теперь это уже не «уникальное знание» у пользователя, а «владение уникальной последовательностью байт» у компьютера. Если мы попробуем зайти на сайт, для которого сохранили пароль, то теперь браузер (прозрачно для нас) предъявит серверу последовательность байт, на основе которой сервер примет решение о том, прошли ли мы процедуру аутентификации или нет.

Безопасен ли такой переход из «знания» в «последовательность байт»? Прежде, чем дать ответ на этот вопрос, стоит отметить, что для пользователя такой переход однозначно удобен. Сложно представить себе ситуацию, в которой пользователь добровольно согласится каждое свое действие подтверждать паролем, если речь, конечно, идет не об операциях с деньгами. Вернемся к безопасности – для того, чтобы понять насколько сохранение пароля безопасно, нужно рассмотреть то, как именно пароль хранится.

Для удобства восприятия я предлагаю следующую схему разделения способов хранения паролей.

Приведем короткие описания с примерами по каждому пункту.

1) Хранение пароля в открытом виде.

С одной стороны, это просто ужасно. Только представьте себе, что злоумышленник получил доступ к вашему компьютеру всего на одну минуту и этого будет достаточно, чтобы все пароли оказались у него. Так хранят пароли, например, браузеры Google Chrome и Firefox. Почему разработчики, для которых вопрос защиты информации является одним из ключевых, поступают именно так? На самом деле, причина такого решения вполне понятна: браузер не может предусмотреть все возможные способы проверки пароля, поэтому недостаточно хранить хэш или какую-то другую информацию. Всегда найдется сайт, который для аутентификации выберет новую хэш-функцию или вообще предоставит свою.

Для того, чтобы не совсем очернять указанные браузеры, стоит отметить, что в них реализована функция «Мастер-пароля». Используя мастер-пароль, все хранящиеся пароли зашифровываются и хранятся уже в зашифрованном виде. Если пользователь захочет воспользоваться паролем из базы, то ему придется ввести мастер-пароль, обычно один раз в течение сессии работы с браузером. Такое хранение более безопасно, но возможна худшая ситуация – скомпрометировав такой пароль, пользователь лишается всех своих паролей.

В качестве примера программы, которая просто хранит пароль в открытом виде – достаточно популярный Интернет-мессенджер Pidgin. В ответ на вопрос, почему пароль хранится именно так, авторы программы отвечают: «If someone else can access your files and you can't trust them not to misuse stored sensitive data, don't store the sensitive data.» («Если кто-то еще имеет доступ к вашим файлам, и вы не можете положиться на то, что он не будет использовать ваши конфиденциальные данные, то не стоит их вообще хранить»).

2) Хранение пароля в зашифрованном виде без привязки к компьютеру.

К такому методу хранения прибегает очень большое количество разработчиков программных продуктов. На самом деле, это просто ужасная практика. Пользователь считает, что его конфиденциальные данные надежно защищены, хотя на самом деле это «визуальное» шифрование. Расшифровать такие данные не составляет ровным счетом никаких проблем, поскольку чаще всего используется безключевое шифрование («шифрование Цезаря», ROT13, xor), либо симметричное шифрование с фиксированным ключом. К этому разделу очень сложно подобрать пример, по той причине, что таких программ очень много и сложно выбрать ту, пример которой будет нагляднее. Приведу такой список: Total Commander, FAR Manager, The Bat!,

Способ хранения пароля		
Пароль в открытом виде	Пароль в зашифрованном виде	
	Привязка к компьютеру	Без привязки к компьютеру
		Не хранение пароля как такового, а только производная информация

Opera, QIP. Хотя для Opera можно сделать оговорку, аналогичную той, что была в предыдущем пункте – поддерживается функция «Мастер-пароль».

3) Хранение пароля в зашифрованном виде с привязкой к компьютеру.

Редко используемый способ, но выгодно отличающийся от предыдущих двух пунктов. При выборе такого способа хранения пароль можно расшифровать только на том компьютере, на котором данные были зашифрованы. Такой механизм используют, например, встроенные программы Windows для работы с ftp. Еще один пример – программа Microsoft Office Outlook. При использовании таких программ, мы защищены от ситуации, когда злоумышленник каким-то образом завладел нашими данными, и будет пытаться расшифровать их на своих мощностях. Но, если злоумышленник имеет доступ к нашему компьютеру (аккаунту в системе), то, скорее всего, такое шифрование его не остановит.

4) Хранение не самого пароля, а некоторой производной информации.

Пожалуй, идеальный способ хранения паролей. Данным способом пользуется Skype. Сам пароль не хранится, а хранится только результат многократного хеширования с примесью системных данных. В результате, если у нарушителя даже есть доступ к компьютеру, то узнать пароль он не сможет. Как и взять с собой аутентификационные файлы, для того, чтобы попробовать осуществить доступ с их помощью со своей машины. Тут стоит сделать оговорку, что если у злоумышленника есть постоянный доступ к атакуемому компьютеру, то ему и не потребуется узнавать пароль, можно будет просто пользоваться на этом компьютере. Такие ситуации стоит решать организационными мерами.

К сожалению, такой способ применим только для узкого класса программ – те, которые узкоспециализированы и работают на одном конкретном протоколе. Поэтому, например, нельзя реализовать такое хранение паролей для браузеров, ftp-клиентов, email-клиентов, im.

Что же делать, если мы хотим уберечь свои пароли? Рассмотрим плюсы и минусы основных вариантов решения данной проблемы.

1) Не сохранять пароли. Самый простой и один из самых надежных способов обезопасить себя. Если пароль не хра-

нится, то его и не украсть. Но такой способ крайне неудобен. Начало работы за компьютером будет превращаться в длительную процедуру запуска всех интересующих программ и сервисов. После запуска нужно будет вспомнить пароль от каждого конкретного сервиса и убедиться, что он правильный. А если учитывать, что в интересах безопасности пользователя пароли должны быть разными, то получается достаточно большой объем информации, который нужно держать в памяти.

2) Использовать для доступа к каждому конкретному сервису специализированный клиент. Если программа «заточена» для работы с каким-то конкретным сервисом и не является универсальной, то в ней чаще всего сам пароль не хранится, а хранится только некоторая производная часть (хэш или что-то аналогичное). Такой способ позволит обойти вынужденную небезопасность, но имеет крайне существенный минус: не под все сервисы можно найти соответствующий клиент. А даже если такой клиент и есть, то нет гарантий, что он хранит пароль именно в требуемом нам виде.

3) Пользоваться внешними сервисами хранения паролей. Достаточно удобный способ – достаточно запомнить главный пароль и в любом месте, в любое время, указав только один пароль, получить доступ ко всем своим данным. У всех таких сервисов и программ есть одна большая проблема – при компрометации мастер-пароля, все ваши пароли перестанут быть конфиденциальными.

К последнему виду решения можно отнести функцию «Помощник авторизации» в ПО ПСКЗИ ШИПКА. Суть функции состоит в возможности сохранять используемые пароли в устройстве ШИПКА. Доступ к данным осуществляется только после ввода пин-кода. Кардинальное отличие от других сервисов состоит в том, что компрометация пин-кода сама по себе не является проблемой – устройство отчуждаемо от компьютера и для того, чтобы узнать ваши пароли, будет недостаточно подглядывать какой именно пин-код вы набираете – нужно будет еще украсть само устройство, а не просто получить его в свое распоряжение на время. Даже если злоумышленник сможет завладеть устройством, то вряд ли это останется незамеченным для владельца – он сможет оперативно поменять все сохраненные пароли.

ОРГАНИЗАЦИЯ ОДНОНАПРАВЛЕННОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ НА БАЗЕ ЗАЩИЩЕННОГО СЛУЖЕБНОГО НОСИТЕЛЯ ИНФОРМАЦИИ

С.С. Лыдин,
ОКБ САПР, г. Москва

Защита автономных компьютеров или сетей от нежелательного и неавторизованного раскрытия обрабатываемой, хранимой и передаваемой с их помощью информации конфиденциального характера составляет извечную проблему в области обеспечения безопасности информации. Эта проблема воспринимается особенно остро, если речь идет о компьютерных системах, используемых правительственными органами или органами безопасности коммерческих структур, которые, в силу высокого уровня критичности размещаемых в них данных, нуждаются в обеспечении повышенного уровня безопасности.

При этом традиционные средства защиты, включая средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, при типовом конфигурировании, как правило, контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их передачи. Подобный подход оставляет возможность обмена информацией посредством т. н. скрытых каналов, (СК) не предусмотренных разработчиком информационной технологии (ИТ) или автоматизированной системы (АС) коммуникационных

каналов, которые могут быть использованы для нарушения политики безопасности [1].

Классическим примером, иллюстрирующим суть скрытых каналов, является возможность отображения на уровне сегмента сети, для которого требуется обеспечение низкого уровня безопасности, названий каталогов и файлов, созданных на уровне сегмента сети, для которого требуется обеспечение высокого уровня безопасности. При этом информация может передаваться в неявном закодированном виде в сформированных определенным условным способом именах файлов, атрибутах, даже размерах и датах изменения файлов и т. д. Наконец, сам факт существования файла с определенным названием содержит в себе один бит информации, передаваемый с высокого уровня на низкий.

Другой пример связан с тем, что в настоящее время Интернет, равно как и большинство действующих сетей, все еще функционирует на основе протоколов TCP и IP. Данные протоколы, хотя и являются достаточно эффективными, характеризуются отсутствием необходимых элементов защиты [2].

Основной протокол TCP/IP специфицирован в RFC 793 [3] и RFC 791 [4], однако, существуют также его расширения (например, расширения TCP для обеспечения высокой производительности, в RFC 1323 [5]), которые определяют дополнительные параметры заголовка, оставляющие некоторые возможности для стеганографического кодирования и использующие тот факт, что некоторые заголовки изменяются в процессе передачи (потенциальные возможности для использования в злоумышленных целях полей заголовка TCP/IP рассмотрены, например, в работах [6], [7], [8], [9] и др.).

В общем случае угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

- внедрение вредоносных программ и данных;
- передача злоумышленником команд для выполнения внедренному в систему программному агенту;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

Для удовлетворения потребности в обеспечении безопасности надлежащего уровня, позволяющего блокировать угрозы безопасности, возникающие вследствие наличия возможности несанкционированных воздействий с помощью СК, проектируются и разрабатываются специальные методы и механизмы защиты.

В ГОСТ Р 53113.1-2008 определены следующие средства и методы противодействия опасным СК [1]:

- построение архитектуры ИТ или АС, позволяющей перекрыть СК или сделать их пропускную способность настолько низкой, что каналы становятся неопасными;
- использование технических средств, позволяющих перекрывать СК или снижать их пропускную способность ниже заданного уровня;
- использование программно-технических средств, позволяющих выявлять работу опасных СК в процессе эксплуатации системы;
- применение организационно-технических мер, позволяющих ликвидировать СК или уменьшить их пропускную способность до безопасного значения.

Одним из наиболее очевидных методов противодействия опасным СК является использование однонаправленной сети (ОНС), или диода данных (data diode) – механизма, позволяющего в целях обеспечения безопасности инфор-

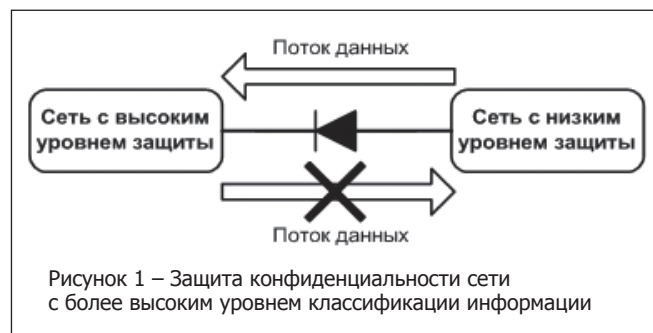
мации осуществлять передачу данных только в одном направлении. В средах с повышенными требованиями к безопасности информации, диод данных используется при соединении между двумя или более сетями с различающимися уровнями критичности информации и, соответственно, различающимися уровнями защиты (рисунок 1).

Преимущества для пользователей сети с высоким уровнем защиты заключаются в том, что их данные остаются конфиденциальными, в то время как они могут получать доступ к данным стороны с низким уровнем защиты. Подобная функциональность может быть востребована потребителем, например, в том случае, если чувствительные данные хранятся в сети, которой требуется подключение к сети Интернет.

Однако в то время, как односторонний канал данных обеспечивает исключительно высокий уровень защиты данных, размещенных в защищенном сегменте сети, его применение обуславливает возникновение дилеммы, связанной с потребностью в верификации данных, которая, можно предположить, является критичной в большинстве систем передачи данных. В частности, протоколы, обычно используемые в сетевых соединениях, такие как TCP/IP, не могут использоваться в ОНС, поскольку предполагают подтверждение приема. Это также служит препятствием для возможности функционирования в таких сетях большого числа прикладных приложений.

Можно констатировать, что в тривиальной односторонней системе передачи данных узел-отправитель не может получить от узла-получателя статус и информацию о целостности отправленных данных без отказа от односторонности потока данных и, как следствие, компрометации защиты, предоставляемой за счет использования односторонних каналов передачи данных.

Попытки преодоления указанной сложности отличаются широким многообразием применяемых подходов и порождают весьма экзотические решения. Например, в патенте США № 5703562 «Методы передачи данных от незащищенного к защищенному компьютеру» предлагается схема верификации данных для систем передачи, основанных на одностороннем канале данных, в которой используется некое «сигнальное устройство», подсоединенное к защищенному компьютеру и «испускающее сигнал предупреждения» в момент обнаружения ошибки в передаваемых данных. В качестве сигнала предупреждения об обнаружении ошибки в патенте предлагается использовать «одиночный продолжительный звук». Очевидно, предложенное решение не позволяет обеспечить передачу результата вычислений, выполненных в рамках обнаружения ошибок, от узла-получателя к узлу-отправителю, так, чтобы



последний мог сравнить результаты и вывести на экран статус и информацию о целостности переданных данных из этого сравнения.

Существуют также решения, которые предусматривают использование для организации подтверждения приема дополнительных средств вычислительной техники, реализующих функции узла обратной связи.

Кроме того, в ряде подходов рассматривается возможность построения IP-архитектур, в которых используются традиционные межсетевые экраны или маршрутизаторы, сконфигурированные таким образом, чтобы разрешать исключительно одностороннюю передачу данных между двумя доменами или узлами сети. Следует отметить, что, к сожалению, подобные подходы, будучи относительно простыми и привлекательными для реализации, в то же время в значительной степени подвержены атакам, связанным с несанкционированным изменением конфигурации системы защиты в целях нарушения однонаправленности передачи данных.

Наличие известных трудностей способствует рассмотрению в качестве основы для построения однонаправленных каналов передачи данных альтернативных решений. Одним из таких альтернативных механизмов является организация однонаправленного канала передачи данных на базе защищенного служебного носителя информации.

Обобщенная схема защищенного служебного носителя информации приведена на рисунке 2.

Носитель информации, показанный на рисунке 2, представляет собой запоминающее устройство, содержащее пользовательские данные и удовлетворяющее спецификации для USB-устройств класса Mass Storage. Исполнительный механизм для ограничения доступа к носителю информации реализован в блоке ограничения доступа. При этом блок ограничения доступа получает управляющие воздействия со стороны вычислителя, который реализован в виде микропроцессорного устройства, также выполняющего операции, связанные с идентификацией и аутентификацией пользователя при доступе к пользовательским данным, содержащимся на носителе информации. Безопасность хранения ключей в энергонезависимой памяти вычислителя базируется на отсутствии доступных для злоумышленника процедур, позволяющих получить значения ключей аутентификации.

Определяющим механизмом, положенным в основу

концепции рассматриваемой архитектуры защищенного служебного носителя информации является процедура регистрации. При этом различаются процедуры первичной и повторной регистрации. Первичная регистрация позволяет ему функционировать на обособленном компьютере или в заданном сегменте сети (в зависимости от модификации защищенного служебного носителя информации, определяющей возможность его сопоставления либо с выделенным компьютером, либо с сегментом сети). Повторная регистрация предназначена для расширения области его функционирования за счет дополнительных «дружественных» обособленных рабочих станций или сегментов сети.

В целях реализации однонаправленного канала передачи данных процедура регистрации должна быть параметризована таким образом, чтобы предусматривать возможность задания режима доступа («только чтение», «только запись», «чтение и запись») к носителю информации на обособленном компьютере или в сегменте сети. В этом случае при регистрации защищенного служебного носителя информации администратором безопасности в сегменте сети с низким уровнем защищенности для него должен быть установлен режим «чтение и запись» или «только запись», а при регистрации в сегменте сети с высоким уровнем защищенности «только чтение». Информация о заданных режимах доступа сохраняется во внутренней энергонезависимой памяти вычислителя. Реализация данного подхода принципиально возможна, поскольку механизм для ограничения доступа к носителю информации реализован в блоке ограничения доступа, в свою очередь управляемом программой, также записанной во внутренней энергонезависимой памяти вычислителя.

Таким образом, общий алгоритм работы защищенного служебного носителя информации, реализующего односторонний канал передачи данных, выглядит следующим образом:

1) после подключения к соответствующему разъему компьютера вычислитель начинает исполнять программу, записанную в его внутренней энергонезависимой памяти (при этом блок ограничения доступа запрещает обращение к носителю информации со стороны интерфейса USB);

2) вычислитель, как USB-устройство, выполняет функции подключения к интерфейсу USB в соответствии с технологией Plug and Play, в результате чего операционная система компьютера распознает устройство и загружает его драйвер;

3) вычислитель получает необходимые данные для проведения:

- идентификации и аутентификации пользователя;

- определения, производилась ли ранее регистрация на данной рабочей станции (относится ли она к числу рабочих станций, на которых разрешается получение доступа к пользовательским данным, содержащимся на носителе информации; в ходе проверки выполняется процедура криптографической взаимной аутентификации защищенно-

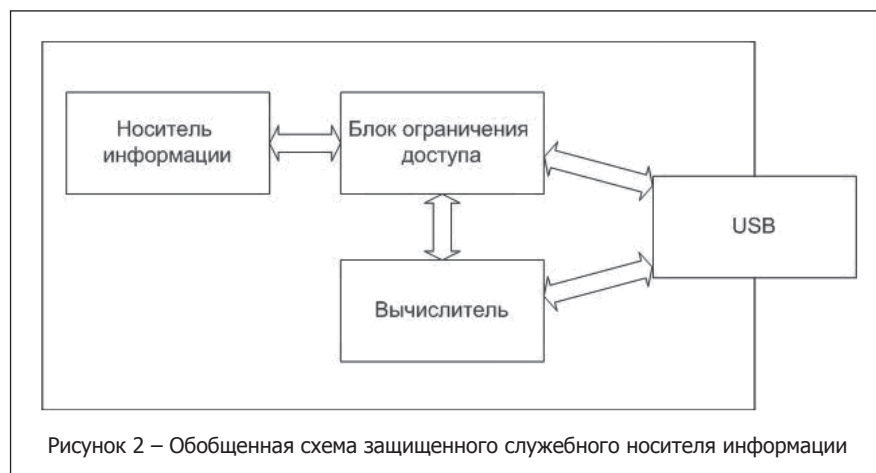


Рисунок 2 – Обобщенная схема защищенного служебного носителя информации

го служебного носителя информации и системы);

– определения заданного режима доступа к пользовательским данным, заданного на этапе регистрации в зависимости от уровня защищенности сегмента сети;

4) вычислитель после получения необходимых данных выполняет вычисления, результатом которых является принятие решения об открытии доступа к носителю информации с учетом заданного режима доступа;

5) если проверки не увенчались успехом, то в доступе будет отказано, вычислитель не направит в блок ограничения доступа команду, разрешающую обращение к носителю информации со стороны интерфейса USB; таким образом, доступ к носителю информации будет по-прежнему запрещен, а вычислитель возвращается в состояние ожидания необходимых данных;

6) если проверки выполнены успешно, вычислитель посылает в блок ограничения доступа команду, разрешающую обращение к носителю информации со стороны интерфейса USB в рамках заданного режима доступа, и поддерживает его в таком состоянии до отключения питания.

Приведенный алгоритм позволяет на физическом уровне блокировать попытки записи данных при подключении устройства к сегменту с высоким уровнем защиты, тем самым неизбежно перекрывая как СК, основанные на наличии памяти, в которую передающий субъект мог бы записывать информацию, а принимающий – считывать ее, так и статистические СК, использующие для несанкционированной передачи информации изменение параметров распределений вероятностей каких-либо случайных характеристик системы. Использование скрытых каналов по времени, основанных на том, что субъект, передающий информацию со стороны с высоким уровнем защищенности, модулирует с ее помощью некоторый изменяющийся во времени процесс, а субъект, принимающий информацию на стороне с низким уровнем защищенности, имеет возможность демодулировать передаваемый сигнал, анализируя несущий информацию процесс во времени, представляется затруднительным уже в силу самой физической природы служебного носителя информации, предполагающей асинхронность передачи порций данных.

Любопытно, что описанный односторонний канал передачи данных может быть направлен и в обратную сторо-

ну – в целях формирования доверенной стороны как источника информации с повышенным уровнем обеспечения целостности и доступности. Для этого достаточно выполнить регистрацию защищенного служебного носителя информации в сегменте с высоким (с точки зрения требований, предъявляемых к целостности и доступности) уровнем защищенности, определив для него режим доступа «только запись» или «чтение и запись», а далее выполнить его регистрацию в сегменте с низким уровнем защищенности в режиме «только чтение». При этом алгоритм функционирования такого канала передачи полностью аналогичен описанному выше.

Литература:

1. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
2. Steven J. Murdoch. Covert channel vulnerabilities in anonymity systems. – Technical Report, 2007.
3. J. Postel. Transmission Control Protocol. RFC 793, IETF, September 1981.
4. J. Postel. Internet Protocol. RFC 791, IETF, September 1981.
5. V. Jacobson, R. Braden, and D. Borman. TCP extensions for high performance. RFC 1323, IETF, May 1992.
6. T. Handel and M. Sandford. Hiding data in the OSI network model. In R. Anderson, editor, Information Hiding Workshop (IH 1996), volume 1174 of LNCS, pages 23–38, Cambridge, UK, May/June 1996. Springer.
7. K. Ahsan and D. Kundur. Practical data hiding in TCP/IP. In ACM Workshop on Multimedia and Security, Juan-les-Pins, France, December 2002. ACM Press.
8. J. Rutkowska. The implementation of passive covert channels in the Linux kernel. In 21st Chaos Communication Congress, Berlin, Germany, December 2004. Chaos Computer Club e.V.
9. J. Giffin, R. Greenstadt, P. Litwack, and R. Tibbetts. Covert messaging in TCP. In R. Dingledine and P. Syverson, editors, Privacy Enhancing Technologies (PET), volume 2482 of LNCS, pages 194–208, San Francisco, CA, US, April 2002. Springer.

КРИТЕРИИ СРАВНЕНИЯ ЗАЩИЩЕННЫХ СЛУЖЕБНЫХ НОСИТЕЛЕЙ

**Е.А. Мареникова,
ОКБ САПР, г. Москва**

В современном обществе использование съемных носителей в корпоративной среде приобрело большую популярность. Однако использование съемных носителей внутри организации связано с риском возникновения различных угроз, таких, как утечка корпоративной информации вследствие потери или кражи съемного носителя, уничтожение служебной информации мотивированным инсайдером, привнесение вредоносного программного обеспечения, а также вирусов в систему, блокирование и уничтожение корпоративной информации [1].

Чтобы снизить риск кражи или потери информации конфиденциального характера (в силу использования не-

защищенных съемных носителей), компании принимают ряд организационных мер [2], например, использование в организации служебных носителей [3] (портативных запоминающих устройств, подключаемых к инфраструктуре информационной системы организации (компьютерам или иным считывающим устройствам) по интерфейсу USB с целью обработки (хранения, переноса и обмена) корпоративной информации) [4]. При этом предполагается, что служебные носители должны использоваться только в организации и нигде больше.

Однако такая мера не способствует увеличению уровня защищенности системы (т.к. служебные носители зачастую

используются сотрудниками как на работе, так и за ее пределами), если служебные носители не защищены с помощью специальных технических решений.

Как выбрать надежный защищенный носитель среди многообразия носителей, представленных на рынке? Чтобы дать ответ на этот вопрос, необходимо выполнить следующее:

- определить понятие защищенного служебного носителя;
- определить основные характеристики, которыми может обладать защищенный служебный носитель;
- на основе определенных характеристик сформировать критерии сравнения защищенных служебных носителей.

Понятие «защищенный служебный носитель»

Защищенный служебный носитель информации (ЗСНИ) – это служебный носитель, предназначенный для защиты размещаемых на нем пользовательских данных конфиденциального характера от доступа со стороны посторонних лиц. ЗСНИ надежно защищает пользовательскую информацию в случае потери или кражи устройства.

ЗСНИ должен использоваться только внутри системы согласно ее внутренним правилам. Очевидно, что ЗСНИ, по меньшей мере, должен:

- исключать хищение, несанкционированную модификацию информации;
- препятствовать утечке информации в результате кражи или потери ЗСНИ;
- препятствовать блокированию или уничтожению обрабатываемой информации в результате привнесения вредоносного ПО в систему;
- препятствовать несанкционированному привнесению в систему информации извне.

Характеристики ЗСНИ

В качестве средства защиты информации любой ЗСНИ обладает набором характеристик безопасности; кроме того, подобно любой другой продукции, ЗСНИ обладает набором потребительских характеристик.

Анализ рынка защищенных носителей показывает, что в общем случае в ЗСНИ могут быть реализованы следующие функции безопасности [5-7]:

- 1) возможность удаленного управления устройством;
- 2) возможность настройки общих политик доступа к ЗСНИ: управление длиной пароля, количеством попыток ввода пароля и т. д.;
- 3) возможность настройки политики доступа к ЗСНИ на рабочих станциях (РС): ограничение доступа к РС по доменам, именам РС, серийному номеру материнской платы компьютера, серийному номеру дистрибутива ОС и др.;
- 4) шифрование данных;
- 5) аутентификация пользователя по паролю, PIN-коду, с использованием биометрических характеристик и др.;
- 6) защита от исследований (активного (контактного) несанкционированного доступа к информации);
- 7) возможность фильтрации USB-устройств, позволяющей использовать на РС только разрешенные USB-носители и блокировать использование неразрешенных USB-устройств (обеспечение защиты от утечки информации и привнесения вредоносного программного обеспечения (ПО));

- 8) ведение журнала событий;
- 9) защита от вирусов;
- 10) резервное копирование данных.

К потребительским характеристикам ЗСНИ целесообразно отнести следующие [8]:

- 1) наличие/отсутствие встроенных прикладных пользовательских приложений (Web-браузер, почтовая программа и пр.);
- 2) емкость устройства, скорость чтения, скорость записи, поддерживаемые операционные системы;
- 3) наличие эксплуатационной документации в комплекте поставки;
- 4) особенности дизайна;
- 5) цена.

Критерии сравнения ЗСНИ

Основываясь на определенных выше характеристиках ЗСНИ, можно сформировать критерии сравнения ЗСНИ, с помощью которых можно определить, соответствует ли тот или иной продукт понятию и требованиям безопасности, предъявляемым к защищенному служебному носителю: защищает ли продукт информацию от доступа к ней посторонних лиц, препятствует ли устройство проникновению вредоносного ПО в систему, исключает ли продукт возможность выноса корпоративной информации за пределы системы, препятствует ли продукт несанкционированному привнесению в систему информацию извне.

Базовые критерии сравнения ЗСНИ:

- 1) возможность настройки общих политик доступа к ЗН;
- 2) возможность настройки политики доступа к ЗН на РС;
- 3) ведение аппаратного журнала событий ЗН;
- 4) шифрование данных;
- 5) парольная аутентификация пользователя;
- 6) защита от исследований (активного (контактного) несанкционированного доступа к информации);
- 7) защита от вирусов;
- 8) наличие фильтра USB-устройств;
- 9) возможность удаленного управления устройством;
- 10) наличие возможности разделения ролей эксплуатирующего персонала.

ЗСНИ, удовлетворяющий описанным критериям, надежно защищает корпоративную информацию конфиденциального характера и не снижает общего уровня защищенности системы даже при физическом выносе устройства за ее периметр.

Примерами ЗСНИ, удовлетворяющих большинству заданных критериев, являются устройства линейки «Секрет» (ПАК «Секрет Особого Назначения», ПАК «Личный Секрет», ПАК «Секрет Фирмы»), а также продукт Kanguru Defender Elite.

Литература:

1. The threats posed by portable storage devices. GFI White Paper [Электронный ресурс]. Режим доступа: <http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf>.
2. The State of USB Drive Security, Ponemon Institute Research Report [Электронный ресурс]. Режим доступа: http://media.kingston.com/images/usb/pdf/MKP_272_Ponemon_WP.pdf.
3. Seven Steps to Secure USB Drives. Sandisk White Paper [Электронный ресурс]. Режим доступа:

http://www.sandisk.com/assets/File_pdf/Seven_Steps_to_Secure_USB_Drives.pdf.

4. Лыдин С.С. «Подходы к построению системы защищенного применения служебных носителей информации» // Комплексная защита информации. – Материалы 17 Международной конференции, 2012.

5. Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers [Электронный ресурс]. Режим доступа: <http://www.sans.org/critical-security-controls/control.php?id=3>.

6. Secure USB Flash Drives. European Network and Information Security Agency (ENISA) [Электронный ресурс]. Режим доступа: <http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2008/secure-usb-flash-drives-en>.

7. About Kanguru Central Remote Management [Электронный ресурс]. Режим доступа: <https://kanguru.com/remote-management/about-remote-management.shtml>.

8. Петрищев Ф.А. Теоретические основы товароведения и экспертизы непродовольственных товаров. – М., 2007.

ПРИМЕНЕНИЕ DYNAMIC BINARY INSTRUMENTATION В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

М. Перов,
ОКБ САПР, г. Москва

В деятельности специалистов по защите информации возникают ситуации, когда требуется изучить ПО без исходного кода. Например, нужно исследовать malware, проверить коммерческое ПО, которое не поставляется с исходным кодом на предмет недеklarированных возможностей (НДВ), провести сертификацию предоставленного софта. Для решения конкретной задачи необходимо подобрать определенный инструмент, который может в лучшем случае оказаться платным, в худшем – вообще не существовать. Поэтому специалистам в области защиты информации время от времени приходится создавать собственные инструменты. Отсюда вытекают две существенные проблемы: время и сложность написания средств.

Вообще, для изучения ПО без исходного кода применяются инструменты двух классов: инструменты статического и динамического анализа. Статический анализ – это анализ ПО, проводимый без выполнения исследуемой программы, а динамический анализ – анализ, который осуществляется в отношении ПО, выполняющегося в момент проведения анализа на реальном или виртуальном процессоре. Нельзя сказать, что один способ анализа лучше другого, так как каждый применяется в тех случаях, когда это необходимо. Например, статический анализ эффективен, если код программы не запутан и не меняется во время выполнения, а в случае самомодифицирующегося кода динамический анализ не заменим.

Для реализации динамического анализа существует технология, название которой Dynamic Binary Instrumentation (DBI). Основной принцип DBI заключается во вставке дополнительных внешних процедур в исследуемый бинарный код. Данные процедуры вставляются единожды, а вызываются столько раз, сколько выполняется участок кода, в который была произведена вставка. Например, можно перехватывать и обрабатывать события возникновения исключений, запуск системных вызовов, порождение потоков и многое другое.

Поскольку ручной анализ – это весьма трудоемкая задача, поэтому были созданы различные фреймворки для DBI, которые позволяют достаточно просто и быстро создавать динамические бинарные анализаторы. Один из самых знаменитых фреймворков – PIN, разработанный в

Intel, речь о котором пойдет далее. Однако существуют и другие библиотеки, например, DynInst и DynamoRIO. Помимо инструментов анализа, упомянутые выше фреймворки позволяют создавать отладчики, инструменты измерения производительности и симуляторы, примером является потактовый симулятор The Sniper, который базируется на PIN.

Как говорилось ранее, PIN – это фреймворк динамической двоичной инструментации, поддерживающий такие архитектуры, как IA-32 и x86-64. В то же время, PIN – кроссплатформенный, позволяет создавать инструменты под Linux и Windows. Библиотека дает исследователю возможность вставить произвольную процедуру, написанную на Си или Си++, в произвольный участок бинарного кода. Перед выполнением вставленного кода полностью сохраняются все данные выполняемого процесса, такие как состояние регистров, таким образом, работа программы не нарушается.

Одной из отличительных особенностей PIN является вполне обширный API, примеры использования которого поставляются вместе с библиотекой. На сайте Intel имеется подробное описание всех примеров. Все это делает PIN достаточно простым фреймворком, которым легко научиться пользоваться. А из недостатков стоит отметить то, что PIN – проприетарное приложение. Однако распространяется бесплатно для некоммерческих проектов.

Среди существующих проектов, использующих PIN, стоит отметить те, которые относятся к безопасности. Итак, VERA – инструмент, визуализирующий работу программы; Kerckhoffs детектируют криптографические примитивы; Tripoux – анализатор упаковщиков; Privacy Score ищет утечки критичной информации. И это далеко не полный список. Упомянутые проекты с открытым исходным кодом, что позволяет их изучить и написать собственные инструменты.

Таким образом, DBI довольно удобная технология, для которой существуют мощные фреймворки, позволяющие достаточно быстро и легко создавать инструменты динамического анализа, без которых не обойтись для быстрого и качественного исследования ПО без исходного кода, что является одной из важнейших задач в области защиты информации.

АНАЛИЗ ЗАЩИТЫ ОБРАЗОВ ДИСКОВ ВИРТУАЛЬНЫХ МАШИН И СНАПШОТОВ

Д. Постоев,
ОКБ САПР, г. Москва

Системы виртуализации сейчас широко и повсеместно распространены в организациях по всему миру. Виртуализация позволяет консолидировать аппаратные средства и запускать несколько виртуальных машин, каждая со своей операционной системой, на одной физической, тем самым, оптимизируя ресурсы.

Однако внедрение технологий виртуализации требует пересмотра вопросов безопасности. Виртуализация добавляет новые уровни (гипервизор, виртуальная машина), которые также нуждаются в дополнительной защите и контроле. В данной статье рассмотрен один из вопросов защиты виртуальных машин на платформе виртуализации VMware vSphere. Это решение было выбрано в силу его большой распространенности и широких возможностей.

Виртуальная машина – это полностью изолированный программный контейнер, представленный в виде совокупности файлов различного назначения, основными из которых являются:

1) .vmx – файл конфигурации виртуальной машины, он содержит информацию о гостевой системе, количестве ядер процессора, выделенной оперативной памяти или подключенных устройствах;

2) .vmdk – файл образа диска виртуальной машины, содержащий файлы гостевой системы и метаданные о жестком диске (размер, файловая система);

Остановимся подробнее на последнем и рассмотрим связанные с ним угрозы.

1 Получение доступа к конфиденциальным данным внутри гостевых систем

Образы виртуальных машин и снапшоты могут хранить конфиденциальную информацию, в том числе состояние оперативной памяти (в файле конфигурации снапшотов – .vmsn). Единственный способ защититься от несанкционированного доступа на чтение к этим данным – запретить доступ к хранилищу виртуальных машин всем, кроме администратора безопасности информации и администратора СХД (систем хранения данных).

2 Внесение вредоносного кода внутрь виртуальной машины

Для организации защиты от подобного рода атак необходимо контролировать целостность, во-первых, загрузочного раздела диска, во-вторых, критических системных файлов (kernel32.dll, ntdll.dll,...), в-третьих, использовать антивирусные решения для виртуальных сред для индикации и предотвращения вредоносной активности.

3 Получение доступа к гипервизору

Эта угроза является наиболее опасной, так как компрометация гипервизора делает уязвимой все имеющиеся

на нем виртуальные машины, поэтому остановимся на ней подробнее. На сегодняшний день известна одна успешная атака, позволяющая использовать данную угрозу с применением vmdk-файлов. Чтобы понять, как она работает, и как от нее защититься, рассмотрим подробнее устройство образа виртуальной машины.

Сам образ, как и снапшот, состоит из двух частей: файла дескриптора и файла с данными. Файл данных хранит непосредственно файлы гостевой ОС. В файле дескрипторе содержится информация о размере виртуального жесткого диска, ссылка на родителя в дереве снапшотов, уникальный идентификатор и пути к файлу с данными. Основным, интересующим нас, моментом является именно этот путь. Если его подменить, например, на файл логов ESXi – /scratch/log/vmkernel.0.gz, то мы получим доступ к файлу гипервизора, таким же образом можно получить доступ к бэкапу папки /etc/ или даже физическим дискам хоста. Эта угроза особо актуальна при использовании облачных сервисов, когда используется виртуальная машина, а, следовательно, и сам .vmdk-файл предоставляется облачному провайдеру пользователем.

Как же защититься от подобного рода атак? В первую очередь, надо ограничить доступ к хранилищу виртуальных машин, во вторую, надо контролировать целостность не только отдельных файлов внутри виртуальной машины, но и самого файла дескриптора. Для облачных систем необходимо проверять соответствие предоставляемых файлов дескрипторов и файлов данных.

Общепринятые стандарты (PCI-DSS, NISTSP800-125) тоже не обходят этот вопрос стороной, призывая защищать образы виртуальных машин и снапшоты. Это также нашло отражение и в проекте приказа ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», где предусматривается «контроль целостности конфигураций компонентов виртуальной инфраструктуры и самих компонентов».

Виртуальные технологии имеют много различных приложений и применений, и системы защиты, используемые в одних, могут быть нереализуемы для других. В виртуальных системах изначально существуют компоненты, которые при неправильной настройке и управлении могут привести к атакам.

В данной статье был рассмотрен только один из видов угроз, возникающий в виртуальной среде. При проектировании конкретной системы должны учитываться ее индивидуальные особенности и риски. Если защита виртуальной инфраструктуры построена и функционирует правильно, то это позволяет использовать все плюсы виртуализации без ущерба для безопасности.

ОСОБЕННОСТИ СОВМЕСТИМОСТИ АККОРД-АМДЗ И СОВРЕМЕННЫХ СВТ

С.А. Синякин,
ОКБ САПР, г. Москва

Термин «совместимость» в области вычислительной техники имеет, как минимум, три различных толкования – аппаратная совместимость, программная совместимость и совместимость программ. Поскольку Аккорд-АМДЗ является программно-аппаратным комплексом, то стоит рассмотреть 2 вида совместимости – аппаратную и программную.

В рамках данной статьи под аппаратной совместимостью мы будем понимать способность аппаратной части (платы контроллера АМДЗ) работать на различных компьютерах как PCI/PCIe-устройство, без учета функционального назначения, а под программной – способность ПО АМДЗ выполнять свои функции на различных компьютерах.

Поскольку ПО Аккорд-АМДЗ на данный момент, к сожалению, абсолютно несовместимо с архитектурами, отличными от x86/x86-64, то под «различными компьютерами» мы будем понимать «IBM PC-совместимые» СВТ в современном понимании. Т.е. предполагается, что при построении такого компьютера используется определенный набор стандартов – архитектура микропроцессора x86 (IA-32) или x86-64 (AMD64), наличие шин PCI и/или PCI-Express (стандарты PCI 2.x-3.x и PCI-Express 1.x-3.x), встроенное ПО типа PC BIOS (стандарт de facto, расширенный стандартами BIOS Boot Specification, Plug and Play BIOS Specification, BIOS Enhanced Disk Drive Specification, «El Torito» Bootable CD-ROM Format Specification и др.) или UEFI (стандарт Unified Extensible Firmware Interface Specification версий от 2.0 и выше).

Складывается впечатление, что никаких проблем не должно быть – следуй стандартам и все должно работать. Тем не менее, практика показывает, что проблемы есть, и мы попытаемся выяснить, почему.

В первую очередь, рассмотрим проблемы аппаратной совместимости. Физически контроллеры Аккорд-АМДЗ вставляются в разъем шины PCI или PCI-Express (miniPCI-Express), поэтому аппаратная совместимость – это совместимость с шиной. Здесь можно выделить 2 уровня:

- физический (разъем, размеры, питание, временные параметры сигналов);
- логический (логика работы интерфейса шины).

Стандарты PCI/PCI-Express достаточно подробно описывают параметры устройства (как физические, так и логические). Но реально существуют как допуски и диапазоны, определенные стандартом, так и отклонения, вызываемые разбросом параметров микросхем или особенностями разводки печатной платы. Иногда в конкретной модели или даже конкретной системе происходит сложение погрешностей. Например, на промышленных компьютерах производства Advantech для работы контроллера Аккорд-5MX через переходник CompactPCI-PCI потребовалась доработка (установка конденсатора по линии CLK).

Иногда производители банально нарушают стандарты. Достаточно ярким примером служит некий вполне серийный ноутбук, на разъеме miniPCIe которого отсутствует напряжение питания 1,5 V.

Примером логической несовместимости может служить история с сигналом четности шины PCI. Первая версия про-

шивки контроллера Аккорд-5MX не синхронизировала вывод данных от микропроцессора на шину PCI с тактированием шины. Что интересно, оказалось, что большинство СВТ не проверяют четность на шине как минимум при установках по умолчанию, проблема проявилась на серверах. Еще один пример – ранние версии Аккорд-5.5 PCI-Express использовали микросхему моста PCI-PCI-Express PLX PEX-8111. Оказалось, что в PCI-конфигурации моста по умолчанию производителем микросхемы была допущена ошибка, которая вызывала BSOD на ОС от Vista и новее при загрузке драйвера шины PCI (pci.sys). PLX выпустила Errata с рекомендациями по конфигурированию моста и, как минимум, несколько сотен плат пришлось дорабатывать путем прошивки EEPROM с конфигурацией моста. Современные Аккорд-5.5 PCI-Express выпускаются с мостом PEX-8112, который не имеет этой проблемы.

Особенно остро стоят вопросы аппаратной совместимости с ноутбуками. Обычно ноутбук имеет 1 слот miniPCIe (причем, очень часто формата half-size), предназначенный для установки Wi-Fi-карты. Список Wi-Fi-карт, официально совместимых с конкретной моделью, как правило, невелик, да и зачастую известен только самому производителю. Кроме того, фактически до старта ОС Wi-Fi-карта не нужна, поэтому для ускорения загрузки встроенное ПО (PC BIOS или UEFI) ноутбука может не полностью инициализировать плату в слоте miniPCIe (например, игнорировать наличие на плате расширения BIOS).

С точки зрения физической совместимости – ОКБ САПР единственная, насколько известно, компания в России, производящая «электронные замки» в формате miniPCIe half-size.

Некоторые производители ноутбуков и моноблоков практикуют использование т.н. white-list (списка разрешенных устройств) и при установке платы, параметров которой нет в этом списке, на этапе старта ноутбука мы получаем сообщение «установлено недопустимое устройство» и дальнейшая загрузка системы блокируется.

Происходит также развитие стандартов, но как раз здесь все складывается удачно. При разработке новых версий шин обеспечивается совместимость с прошлыми версиями. Так, достаточно незаметно произошли смены версии шины PCI от 2.0 к 3.0, развитие PCI-Express от 1.0 до 3.0 тоже пока не приносит проблем. К слову сказать, контроллеры Аккорд 5.0, созданные более 10-ти лет назад вполне успешно работают в современных материнских платах.

Проблемы аппаратной совместимости – это проблемы не только Аккорд-АМДЗ. Ведь не зря серьезные производители (IBM, HP и др.) публикуют списки совместимого оборудования, даже производители обычных материнских плат публикуют списки протестированных модулей памяти. В сети Интернет можно найти ставшие уже классическими примеры аппаратной несовместимости:

- проблемы с AGP-видеокартами Nvidia на чипсетах VIA и Ali;
- проблемы инициализации HDD с интерфейсом SATA-II микросхемой VIA VT8237;

– проблемы со звуковыми картами Live! на чипсетах VIA и др.

Какие-то из этих проблем решались обновлениями BIOS/прошивок/драйверов, а какие-то так и ушли в историю нерешенными.

Перейдем к вопросу программной совместимости. Учитывая принципы работы ПО АМДЗ, мы выделим 3 основных момента, в которых важна программная совместимость:

1. Совместимость принципа перехвата управления;
2. Совместимость при работе встроенной ОС и ПО АМДЗ (DOS- и Linux-версии);
3. Совместимость принципа продолжения загрузки основной ОС.

1 Совместимость принципа перехвата управления

Принцип перехвата управления АМДЗ заключается в установке собственного обработчика для отладочного прерывания аппаратной контрольной точки при передаче управления адресу памяти 0000:7C00H (именно на этот адрес передается управление из BIOS после считывания загрузочного сектора с какого-либо носителя). Таким образом, перехват момента загрузки операционной системы происходит в два этапа. Во время исполнения процедуры инициализации происходит установка аппаратной контрольной точки на передачу управления адресу 0000:7C00H и установка в качестве обработчика прерывания по контрольной точке процедуры, расположенной в Аккорд-BIOS. Далее происходит возврат из процедуры инициализации. После считывания загрузочного сектора с какого-либо загрузочного носителя в память по адресу 0000:7C00H и успешной проверки сигнатуры загрузочного сектора происходит передача управления на этот адрес. При этом при передаче управления коду загрузчика возникнет прерывание по аппаратной контрольной точке и будет вызван ранее установленный обработчик этого прерывания, расположенный в Аккорд-BIOS. Таким образом, будет получено управление непосредственно перед загрузкой операционной системы.

Практика показала, что этот принцип достаточно надежен и универсален для PC BIOS. Тем не менее, детали реализации не раз уточнялись. Например, встречаются BIOS, которые в процессе работы затирают отладочные регистры CPU (используемые для установки контрольной точки) и сейчас для таких BIOS работает алгоритм восстановления нужного состояния регистров.

Известной проблемой является несовместимость этого принципа с UEFI. Спецификация UEFI не предполагает заранее известного фиксированного адреса, на который можно установить контрольную точку. На данный момент совместимость достигается тем, что в состав UEFI входит Compatibility Support Module (CSM), который при определенных условиях обеспечивает процесс загрузки ОС в режиме Legacy. Над разработкой совместимого с UEFI принципа перехвата ОКБ САПР ведет работы.

2 Совместимость при работе встроенной ОС и ПО АМДЗ

После получения управления перед загрузкой операционной системы из flash-памяти контроллера загружается встроенная ОС (DOS или Linux), в которой запускается ПО АМДЗ. В принципе, DOS-версия ПО АМДЗ является 32-раз-

рядной надстройкой над простейшим DOS (AcDOS), который обеспечивает только загрузку и запуск исполняемых файлов в определенной последовательности. Здесь как раз минимум проблем совместимости, т.к. практически весь процесс идет под полным контролем ПО АМДЗ в замкнутой среде. Единственным потенциально проблемным местом является разбор файловой системы, т.к. при этом происходит взаимодействие с сервисами BIOS и анализ структур файловой системы.

И снова вспоминаем про UEFI. Работа DOS-версии основана на вызовах сервисов BIOS (ввод информации, вывод изображения, чтение накопителей), и в случае UEFI работа возможна только в том случае, если при работе UEFI был запущен CSM. Кроме того, замечена тенденция не уделять большого внимания правильности реализации программных Legacy-интерфейсов BIOS, что объяснимо – современным ОС они практически не нужны.

В случае Linux-версии ПО АМДЗ, в первую очередь, стоит проблема совместимости собственно нашей сборки ОС Linux с широким кругом различных конфигураций компьютеров. Разработчиками ОС Linux очень много сделано для повышения стабильности и совместимости, но все же задачи запуска ядра, графической оболочки и работы с дисковой подсистемой имеют проблемы с совместимостью. Для минимизации проблем ядро собрано с минимальной поддержкой не нужных для выполнения основных функций АМДЗ опций (отключена поддержка многопроцессорности, ACPI и т.п.). При возможности используются универсальные драйверы (видеодрайвер VESA, драйвера IDE и AHCI). Но сложность практически полноценной ОС несравнима со сложностью простейшей версии DOS, поэтому все же могут возникать проблемы совместимости именно ОС с определенными конфигурациями СБТ.

Тем не менее, на данный момент Linux-версия в целом стабильно работает практически на любых конфигурациях обычных офисных компьютеров. Из проблем совместимости актуальными остаются:

- работа с дисковой подсистемой на серверных конфигурациях, в которых обычно используются RAID-контроллеры;
- невозможность работы с USB-устройствами (клавиатурой, мышью) от момента завершения работы ОС АМДЗ и до загрузки драйверов USB-стека основной ОС;
- невозможность продолжения загрузки с USB-устройств (при входе администратором).

Над решением этих проблем ведутся работы.

Возвращаясь к вопросу совместимости с UEFI надо сказать, что Linux-версия более готова к работе в среде UEFI, хотя доработки, конечно же, потребуются.

3 Совместимость принципа продолжения загрузки

В случае DOS-версии корни возможных проявлений несовместимости в том, что алгоритм определения загрузочного устройства для продолжения загрузки основан на информации, предоставляемой сервисами PC BIOS. При входе пользователем загрузчик ОС в АМДЗ должен проверить, не является ли первый жесткий диск съемным устройством, при входе администратором – правильно определить устройство, с которого началась загрузка до перехвата управления. Но производители встроенного ПО довольно вольно обходятся со спецификациями в этой области (в частности, BIOS

Enhanced Disk Drive Specification и «El Torito» Bootable CD-ROM Format Specification), что может приводить к ошибкам при работе загрузчика. В частности, этим «грешит» встроенное ПО фирмы Fujitsu, не менее 3-х исправлений в загрузчике было связано с необъяснимой, с точки зрения логики работы сервисов BIOS в части Bootable CD-ROM Specification.

В случае Linux-версии загрузчик ОС тоже использует сервисы PC BIOS. И здесь есть известные проблемы, связанные с тем, что после работы полноценной ОС со своими драйверами устройств (USB-стека и дисковой подсистемы), работа этих сервисов нарушается или может быть нарушена.

В частности, это проблема невозможности загрузки с USB-устройств и загрузки с некоторых типов RAID-контроллеров.

Надо отметить, что как раз в случае продолжения загрузки будущая совместимость с UEFI может практически решить эти вопросы.

ОКБ САПР ведет непрерывную работу по обеспечению наиболее полной совместимости своих изделий с современными средствами ВТ. Чтобы «держать руку на пульсе», мы постоянно проводим тестирования с новыми моделями серверов, ноутбуков, моноблоков, стараемся выявить возможные проблемы и решить их.

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМЫ МОНИТОРИНГА И УПРАВЛЕНИЯ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С.В. Сухарева, ОКБ САПР, г. Москва

Системы мониторинга и управления информационной безопасностью (ИБ) контролируют функционирование информационных систем (ИС), систем передачи данных, средств и механизмов защиты.

В процессе функционирования система мониторинга и управления осуществляет сбор первичных данных мониторинга информационной безопасности с наблюдаемых подконтрольных объектов (ПКО) и их анализ. При этом мониторинг информационной безопасности может быть как активным, так и пассивным.

Активный мониторинг характеризуется тем, что на события, которые нарушают заданную политику безопасности, заранее определено воздействие, которое, как ожидается, должно привести к решению возникшей проблемы.

Пассивный мониторинг предполагает сбор информации с удаленных источников в режиме чтения. В случае выходов значений параметров за пределы, определенные как «нормальные», оператор предпринимает соответствующие шаги для устранения возникшей ситуации и нормализации параметров. Такой вид аудита наиболее прост в реализации, но обеспечивает менее высокий уровень защиты по сравнению с активными методами.

Системы мониторинга ИБ также могут быть классифицированы по типу объектов воздействия и в соответствии с этим признаком разделены на системы, предназначенные для мониторинга и управления ресурсами, событиями, активностью.

К числу представителей систем мониторинга и управления ресурсами вычислительных устройств являются системы MRTG и CACTI. Системы данного типа не позволяют в режиме реального времени отслеживать какие-либо показатели, но имеют возможность сохранять статистику и отображать ее в виде графиков.

В рамках мониторинга и управления событиями, как правило, ставится задача отслеживания как событий уровня ОС, так и событий на аппаратном уровне. При этом в отличие от случая использования систем мониторинга и управления ресурсами, возможна настройка срабатывания при наступлении определенных событий. Для отслеживания и реагирования на события могут быть использованы, например, системы Nagios и Zabbix.

Примерами систем мониторинга и управления активностью

являются HP OpenView и IBM Tivoli. Это комплексные системы, которые в зависимости от возникновения событий активности генерируют ответные действия для восстановления требуемых показателей [1].

Системы мониторинга и управления ИБ являются естественным развитием систем мониторинга ИБ и могут быть условно разделены на три класса:

- SIM (Security Information Management) предназначены для сбора событий преимущественно с сетевого оборудования. Основной задачей SEM-решения является анализ событий ИБ и отправка уведомлений о нарушениях в масштабе времени, близком к реальному;

- SEM (Security Event Management) позволяют консолидировать и долгосрочно хранить события от систем информационной безопасности и приложений, осуществляют ретроспективный анализ и расследование инцидентов ИБ, анализ пользовательской активности, а также контроль над соблюдением политик и требований по ИБ [2];

- SIEM (Security Information and Event Management) – решения, которые обрабатывают события безопасности, поступающие как от оборудования, так и от приложений различного уровня. Они обеспечивают соответствие нормативным стандартам и стандартам безопасности на предприятиях (COBIT, FISMA, GLBA, HIPAA, ISO 17799, PCI DSS, SOX и др.), обладают достаточной гибкостью и могут быть адаптированы к особенностям структуры компании и используемой ИТ-инфраструктуры.

- SIM- и SEM-системы по отдельности служат для решения лишь части задач. В полноценной системе ИБ необходимо фиксировать и анализировать с максимально возможной оперативностью событий всех типов. Поэтому на практике внедряются преимущественно комбинированные SIEM-решения, такие как:

- CA Security Command Center;
- Cisco MARS;
- Arcsight Enterprise Security Manager;
- Novell Sentinel;
- Symantec Security Information Manager;
- NetForensics nFX One;
- IBM Tivoli Security Operations Manager;
- Checkpoint Eventia, Checkpoint SmartDefence;
- GFI LANguard, GFI EventsManager.

Частным случаем систем мониторинга и управления информационной безопасностью являются системы управления и мониторинга средствами защиты информации от несанкционированного доступа (СЗИ от НСД), обеспечивающие возможность централизованного управления, конфигурирования и мониторинга функционирования СЗИ от НСД, установленных на подконтрольных объектах системы.

Система мониторинга и управления СЗИ от НСД, в общем случае, может предоставлять следующие возможности:

- управление техническими средствами, доступом к коммутационным портам и периферийным устройствам;
- управление пользователями;
- управление оперативным оповещением о критических событиях и журналами событий ИБ подконтрольных объектов;
- защита от НСД и контроль целостности собственного ПО.

Требования к системе мониторинга и управления СЗИ от НСД, как правило, достаточно высоки: полнота спектра выявляемых атак, высокий уровень производительности, минимальная доля ложных срабатываний, предварительная диагностика причин возникновения нештатной ситуации, наличие подсистемы собственной безопасности, максимально возможная степень автоматизации мер по реагированию и пр.

Также основополагающим требованием является необходимость консолидации всей информации, связанной с функционированием СЗИ от НСД, и возможность на основании результатов работы системы прийти к адекватному выводу относительно того, «что происходит на самом деле» и «как должно быть». К сожалению, на данный момент не существует универсального продукта, полностью удовлетворяющего данному требованию.

Рассмотрим, какие дополнительные функции системы управления и мониторинга СЗИ от НСД могут быть реализованы для обеспечения получения наиболее полной информации о событиях, происходящих в защищаемой системе:

- фиксация в оперативном журнале результатов контроля целостности компонентов на подконтрольном объекте, а также фиксация в собственном журнале фактов изменения настроек и попыток несанкционированного доступа к ПО системы мониторинга и управления. При этом контроль целостности собственного программного обеспечения и настроек, а также программного обеспечения, указанного как «объекты контроля» системы, обеспечивается с помощью возможностей СЗИ от НСД, функционирующих в составе подконтрольных объектов, в том числе, серверного оборудования системы управления и мониторинга СЗИ от НСД;

- возможность просмотра настроек СЗИ от НСД на подконтрольных объектах средствами ПО системы;
- удаленное управление процессами контроля целостности файловой системы ПКО средствами СЗИ от НСД;
- доставка и обновление ПО в соответствии с заданными политиками или по запросу пользователей. С использованием данного функционала администратор может:

1) задавать требуемые политики для различных приложений, которые необходимо в дальнейшем будет

рассылать на ПКО с возможностью получения от ПКО информации о версии установленных на них СЗИ от НСД;

2) составлять расписание рассылки ПО (например, ежедневно/еженедельно/в фиксированное время/по изменению и т. д.);

3) задавать каталог на ПКО, в который необходимо установить или откуда следует загрузить комплект ПО;

4) задавать политику, применяемую в случае неудачной установки/доставки ПО на ПКО;

5) использование механизмов виртуализации ПО. В этом случае ПО, необходимое для установки на ПКО, упаковывается в виртуальные программные пакеты и доставляется пользователю. Виртуальные пакеты содержат все файлы, требуемые данные и параметры реестра приложений, они записываются и устанавливаются в определенный раздел на жестком диске ПКО. После активации любое приложение из виртуального пакета может быть сразу запущено и никаких дополнительных настроек и инсталляций не требуется;

6) удаленный рабочий стол и сопутствующие механизмы для подключения к ПКО при устранении проблем (может быть полезно в случае реализации задач, связанных с сетевым управлением);

7) дедупликация (технология, при помощи которой обнаруживаются и исключаются избыточные данные в дисковом хранилище) при осуществлении резервного копирования. Эта функция может быть полезна, но ее функционирование во многом зависит от типа данных, которые сохраняются при резервном копировании;

8) повышение удобства использования системы мониторинга и управления СЗИ от НСД для ее персонала в части;

9) возможности назначения различных типов оповещений для разных видов событий ИБ. Система мониторинга и управления СЗИ от НСД должна предусматривать возможность задания приоритетов для обнаруживаемых атак или уязвимостей;

10) возможность индивидуальной настройки эксплуатирующим персоналом системы параметров отображения оперативных журналов, получаемых от подконтрольных объектов.

Таким образом, на данный момент не существует системы мониторинга и управления СЗИ от НСД, позволяющей объединить все данные, связанные с функционированием СЗИ от НСД, на основании результатов работы которой можно было бы сделать вывод, «что происходит на самом деле» и «как должно быть». Обычно такие системы служат для решения лишь части задач, связанных с информационной безопасностью. Реализация перечисленных выше функций системы управления и мониторинга СЗИ от НСД позволит получить более полную информацию о событиях, происходящих в защищаемой системе.

Литература:

1. Сильнов, Д.С. Современные системы удаленного мониторинга вычислительных ресурсов: состояние, проблемы, перспективы // Безопасность информационных технологий. М., 2011. – № 3. – С. 57–60.

2. Башлыков, М.А. Мониторинг, анализ и управление ИБ // Information Security/ Информационная безопасность. – М., 2008. – № 1. – С. 50–51.

ПЕРСПЕКТИВЫ РАЗВИТИЯ СРЕДСТВ ЗАЩИТЫ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

Д.В. Угаров,
ОКБ САПР, г. Москва

На дворе 2013 год, виртуализация применяется повсеместно, однако, при этом в статьях почему-то не перестают упоминать, что люди все еще сомневаются в безопасности перехода к данному типу инфраструктуры. Однако даже поверхностный взгляд позволяет понять, что представленных средств защиты для виртуальных инфраструктур уже более, чем достаточно. К сожалению, в связи с этим назревает другая проблема – отсутствие четкого понимания, что именно нужно из представленных продуктов в каждом конкретном случае. Результатом этого непонимания становятся решения с чуть ли не десятками одновременно установленных продуктов, обеспечивающих безопасность. Естественно, при таком «ответственном» подходе производительность системы проседает в разы, а об удобстве управления вообще говорить не приходится.

Причина непонимания заключается в том, что в настоящее время невозможно в полной мере решить все вопросы одновременно с использованием всего лишь одного продукта. Это ведет к необходимости использования нескольких решений, а это, в большинстве случаев, – к дублированию функционала. Помимо этого, не стоит забывать, что часть решений повторяет функционал, предоставляемый самими средствами виртуализации, что окончательно лишает возможности разобраться в данном вопросе.

Т.к. отчет Gartner в очередной раз подтвердил лидерство решения VMware vSphere, то рассмотрение данной проблемы и пути ее решения имеет смысл рассматривать именно на этом продукте. Однако стоит отметить, что большинство идей применимо, в целом, к защите виртуальных инфраструктур, вне зависимости от производителя.

Для того, чтобы выявить узкие места, появляющиеся на стыке используемых решений, обобщим имеющиеся технологии в текущих продуктах по защите информации для виртуальных инфраструктур.

I. В первую очередь, это контроль обращения к файлам операционных систем (ОС) виртуальных машин (ВМ). Данная техника подразделяется на два типа решений.

1. Множество антивирусных продуктов, использующих технологию VMware Endpoint security (EPSEC). Она позволяет обеспечивать контроль обращения к файлам ОС вне этой ОС. Для ее использования необходимы установленные гостевые дополнения внутри ВМ и наличие специальной ВМ на каждом гипервизоре (посредством которой и будет осуществляться контроль). Такой подход, в свою очередь, позволяет значительно снизить нагрузку на инфраструктуру и упростить управление для администраторов за счет отказа от установки дополнительных агентов в каждую ВМ.

2. Продукты, обеспечивающие разграничение доступа к файлам за счет перехвата системных вызовов на уровне ядра. На текущий момент, данная технология работы идентична как для физических машин, так и для виртуальных. Модули безопасности при этом в отличие от EPSEC находятся внутри самой ОС. Т.е. для виртуальных машин контроль происходит не снаружи ОС, а изнутри.

II. Следующим, но не менее важным подходом являются решения, обеспечивающие контроль управления объектами виртуальной инфраструктуры за счет добавления промежуточного звена, выступающего в роли шлюза. В большинстве случаев, для этого на гипервизор добавляется специальная ВМ с фаерволом. Такой подход позволяет вклиниться в сетевые соединения и фильтровать необходимые запросы (т.е. запрещать управляющие команды или блокировать доступ к определенным объектам).

III. Завершают список модули доверенной загрузки. Здесь так же имеет место разделение на 2 подтипа:

1. «Физическая» имплементация необходима для серверов с гипервизорами и серверов управления (для VMware – vCenter).

2. «Программная» имплементация – для ВМ. Необходимость данного элемента связана с тем, что работа EPSEC возможна лишь после того, как включатся гостевые дополнения, а это примерно +10 секунд от включения ОС (образуя таким образом брешь, т.к. контроль не осуществляется непрерывно). Хотя данный модуль нет необходимости реализовывать в виде физического устройства по причине его работы на более высоком уровне, он обязательно должен использоваться в связке со своим «старшим» собратом.

При одновременном использовании антивирусов и решений по разграничению доступа узким местом становится дублирование контроля обращения к файлам – внутри ОС ядром безопасности, а так же из ВМ, находящейся снаружи по отношению к данной ОС. Очевидно, что контролировать доступ из вне – является более правильным решением, кроме того, дающим выигрыш в скорости и простоте управления. Поэтому необходимым шагом в развитии этого направления является интеграция между собой антивирусного ПО, использующего EPSEC, и решений, обеспечивающих разграничение доступа (по аналогии взаимодействия для антивирусов и средств разграничения для физических машин).

Использование шлюзов вместе с модулем доверенной загрузки (МДЗ) ВМ приводит к дублированию контроля состояния виртуальной машины (например, попытку включения ВМ сначала перехватывает фаервол, а затем МДЗ). Поэтому логично снизить избыточность за счет передачи управления к МДЗ ВМ сразу после выявления сигнала фаерволом.

Аппаратные модули доверенной загрузки, в свою очередь, обособлены от предыдущих подходов по двум причинам: во-первых, они обязательно должны использоваться как опорная точка для защищаемой системы (т.е. для них не встает вопрос «а нужно ли?»). Во-вторых, по причине того, что они не дают перекрытия по функционалу с другими продуктами, и как следствие, могут использоваться в системе в своем текущем исполнении. Однако их так же есть, куда развивать.

1. В связи со спецификой виртуализации, все чаще при построении виртуальной инфраструктуры предпочтение отдается blade-серверам, которые не подразумевают воз-

возможности установки PCI-решений. Поэтому, в первую очередь, необходимо озаботиться возможностью перехода на альтернативные интерфейсы, например, USB.

2. За счет того, что в большинстве случаев сервера управляются удаленно, встает вопрос организации И/А при их загрузке. Решить эту проблему можно двумя путями: добавить возможность удаленной И/А или оставить необходимость И/А лишь на случай обнаружения инцидентов при загрузке. Хотя второй вариант предпочтительнее (т.к. ведет к упрощению системы), он требует дополнительного обоснования для принятия со стороны регуляторов, что может занять достаточно продолжительное время. Поэтому выбор в пользу одного из них не очевиден.

3. Существуют комплексы, предоставляющие АМДЗ как «опцию», что показывает не связанность всей системы. Однако просто добавить АМДЗ в систему недостаточно. Чтобы обеспечить непрерывную цепочку защиты, требуется взаимная увязка данного модуля с модулем, находящимся на уровень выше. Таким образом, необходимо, чтобы АМДЗ проверял целостность ПО и драйверов в ОС, ПО, стоящее выше, в свою очередь, проверяло наличие и работоспособность АМДЗ, а так же хранило в нем все необходимые данные.

По отдельности все предлагаемые решения – более чем достойны внимания. С другой стороны, в «полевых» усло-

виях они чаще всего используются в связке. В результате возникает две задачи: не допустить дублирование функционала и тесно интегрировать решения с возможностью централизованного управления ими.

Выход же из данной ситуации возможен двумя путями.

1) Использование программно-аппаратных комплексов от одной компании. Такой подход позволит избавиться от наложения функционала и снизит количество элементов управления. Однако над сведением управления в действительно централизованное решение компаниям еще необходимо работать.

2) Выработать унифицированные API, позволяющие делать связки решений между собой, чтобы, тем самым, минимизировать накладные расходы и упростить управление. Примером такого подхода может служить выпущенный компанией VMware продукт vCenter Multi-Hypervisor Manager, который помимо управления ESXi гипервизорами может управлять и Hyper-V.

Скорее всего, функционал средств защиты виртуальных инфраструктур (в особенности сертифицированных) в самом ближайшем будущем будет идти вровень, а основу выбора в пользу одного из них будут составлять взаимосвязанность компонент и удобство использования. Поэтому, чтобы новые решения были действительно «новыми», компаниям стоит сосредоточиться именно на этих аспектах.

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ПРОТОКОЛА CCID В АППАРАТНЫХ СЗИ

**В.М. Елькин,
ОКБ САПР, г. Москва**

При разработке нового аппаратного СЗИ важным вопросом является выбор стандартов, которые данное устройство будет поддерживать. Выбор определяется удобством для разработчика аппаратуры СЗИ, для разработчика программной составляющей системы защиты, а так же для технической поддержки уже разработанного устройства.

В первую очередь, важны стандарты взаимодействия аппаратного СЗИ с ПК пользователя. Ни для кого не секрет, что одним из наиболее распространенных интерфейсов передачи данных на данный момент является USB. О стандартах работы с USB и хотелось бы поговорить. В первую очередь о стандарте CCID.

CCID (integrated circuit card interface device) – это стандарт USB, созданный для работы с контактными смарт-картами, описанный ГОСТ Р ИСО/МЭК 7816 (аналог зарубежного ISO/IEC 7816). Данный стандарт используется для работы как с USB-ридерами смарт-карт, так и со смарт-картами с USB интерфейсом.

Стандарт CCID является альтернативой таким стандартам USB, как MSC (Mass Storage Class) и HID (Human Interface Device). Примером устройства, поддерживающего стандарт MSC, можно назвать обычный флеш-накопитель. Примером HID-устройства может послужить стандартная клавиатура.

Чем же CCID выгодно отличается от двух других стандартов и почему его стоит использовать при создании аппаратного СЗИ? Попробуем разобраться.

Во-первых, все три стандарта поддерживают передачу данных массивами информации, что обеспечивает высокую

скорость обмена информацией между устройством и ПК. Однако структура пакетов данных в стандартах MSC и HID, по сути, не документирована и остается на совести разработчика, что осложняет поддержку данных стандартов на специфических встраиваемых системах. Что касается стандарта CCID, то структура команд, пакетов данных и ответов описана в ГОСТ Р ИСО/МЭК 7816, что облегчает поддержание данного стандарта на нестандартных устройствах. Это облегчает поддержку корректной работы СЗИ в составе конечной системы, а следовательно и разработку программной части этой системы.

Во-вторых, очевидно, что аппаратное СЗИ должно обладать внутренней памятью. Стандарты MSC и HID не выдвигают никаких требований относительно специфики устройства оной. В CCID же наоборот, структура внутренней памяти целиком и полностью описана ГОСТом, там же описаны возможные свойства файлов и папок, их атрибуты безопасности, порядок их создания, удаления, чтения и записи. Данная особенность позволяет с большей вероятностью восстановить информацию из поврежденного устройства (при известном PIN-коде). Это облегчает дальнейшее обслуживание СЗИ и техническую поддержку клиента.

В-третьих, одной из наиболее важных особенностей стандарта CCID состоит в том, что он, как и стандарт HID, в отличие от MSC, не требует установки дополнительных драйверов. В подавляющем большинстве операционных систем драйвер CCID интегрирован в ядро системы, что обеспечивает работу аппаратного средства защиты информации «из коробки». Казалось бы, нет особых проблем поставить дополнительные

драйвера, однако, что если речь идет о UNIX-подобной системе, да еще и не о стандартной сборке, а разработанной для специфической встраиваемой системы (например, «умный дом»)? Задача сразу многократно усложняется. Со стандартом CCID таких проблем нет, так как драйвер для работы с таким классом устройств интегрирован в ядро системы. Данная особенность облегчает работу как самого разработчика СЗИ, так и разработчиков программной составляющей системы (не требуется написание собственных драйверов).

В-четвертых, стандарт CCID изначально проектировался как стандарт с поддержкой криптографических систем и

алгоритмов. Это заранее увеличивает доверие к системе, поддерживающей данный стандарт, так как криптография поддерживается не как отдельный модуль, а как интегрированная на уровне файловой системы составляющая. Эта особенность облегчает разработку самого СЗИ – разработчику не требуется придумывать алгоритмы работы с криптографией, что исключает ошибки и уязвимости, а следовательно, и повышает надежность системы в целом.

Перечисленные выше плюсы стандарта CCID дают ему неоспоримое преимущество при разработке аппаратного средства защиты информации.

СИНТЕЗ РЕЧЕПОДОБНЫХ СИГНАЛОВ НЕПОСРЕДСТВЕННО ИЗ РЕЧИ ДИКТОРОВ ДЛЯ СИСТЕМ АКУСТИЧЕСКОЙ МАСКИРОВКИ

О.Б. Зельманский, В.В. Мирончик,
БГУИР, г. Минск

Задача защиты речевой информации от утечки по акустическим и виброакустическим каналам представляется довольно сложной и дорогостоящей в виду того, что речь является самой естественной формой взаимодействия для человека и, следовательно, именно по средствам речи передается большая часть конфиденциальной информации. Для ее решения наиболее эффективным является активная маскировка разговора [1]. В настоящей работе предлагается методика синтеза маскирующих речеподобных сигналов (РПС) непосредственно из защищаемой речи [2].

В основе методики лежит метод компиляции участков естественной речевой волны по псевдотексту, генерируемому вероятностными методами. Такой подход требует заранее сформированных баз аллофонов. Процесс формирования подобных баз является достаточно трудоемким. Причем для каждого диктора должна быть сформирована своя индивидуальная база, которая должна периодически обновляться, например, в связи с простудой или охриплостью диктора. В противном случае характеристики формируемых РПС будут отличаться от характеристик речи участников, что может снизить надежность защиты акустической информации. Это, в свою очередь, затрудняет широкое использование систем, реализующих данный метод. Данную проблему предлагается решить путем формирования баз аллофонов непосредственно из речи, участвующих в защищаемом разговоре, дикторов. Это позволит формировать РПС максимально подобные маскируемому речевому сигналу.

Методика формирования баз аллофонов непосредственно из речи дикторов включает в себя следующие этапы: детектирование речи, верификацию диктора, сегментацию речи на фонетические единицы, их классификацию и сохранение в базу.

Детектирование речи заключается в обнаружении и выделении речи из акустической обстановки. Методика детектирования речи заключается в сравнении классификационных параметров сигнала с соответствующими пороговыми значениями, при этом для определения пороговых значений применяется отслеживание статистического минимума данных параметров. В качестве классификационных параметров используются параметры как во временной, так и в частотной областях. Временными характеристиками сигнала являются кратковременное среднеквадратическое значение сигнала и кратковременная функция среднего числа переходов сигнала

через нуль. А частотной характеристикой является спектральная оценка сигнала, объем вычислений которой уменьшается при использовании быстрого преобразования Фурье и свойства симметрии преобразования Фурье [3].

Верификация диктора [4] позволяет отделить речь одного участника разговора от речи другого, с целью формирования базы аллофонов диктора из произнесенной именно им речи. Кроме того, в результате верификации может быть установлено, что для данного диктора уже имеется ранее сформированная база аллофонов и нет необходимости в формировании новой.

В процессе сегментации выделенная при детектировании речь разбивается на участки однородных колебаний, соответствующие фонетическим единицам, путем нахождения межфонемных переходов. В методике сегментации речи используется анализ функции изменения спектра, как меры корреляции между последовательными окнами анализируемого сигнала. При этом в качестве меры корреляции используется расстояние между векторами параметров, описывающими окна сигнала [5].

При классификации фонетических единиц устанавливается, к какому классу фонем относится каждая из них. Методика классификации речи состоит в вычислении коэффициентов различия между анализируемой фонетической единицей и базой образцов вариантов реализации фонем, обусловленных конкретным фонетическим окружением этих фонем, представленных кепстральными коэффициентами, на основе корреляционной матрицы. Принятие решения о принадлежности анализируемой фонетической единицы к той или иной группе фонем, а так же ее классификация, как определенной фонемы, осуществляется путем нахождения образца с наиболее близкой анализируемой фонетической единице длительностью, которому соответствует наименьшее значение коэффициента различия. В результате создается база аллофонов диктора, говорящего на определенном языке, содержащая звуковые реализации фонетических единиц и информацию о них.

Тем не менее, формирование РПС непосредственно из речи дикторов, участвующих в переговорах требует наличия как минимум одной, заранее сформированной базы аллофонов, которая будет использоваться в начале разговора, пока еще не сформированы базы аллофонов участников

этого разговора. Возможно также использование заранее сформированных неполных баз аллофонов каждого из дикторов, которые будут дополняться в процесс разговора. Такая необходимость позволяет предложить многофункциональную объединенную методику компиляционного синтеза РПС, сочетающую в себе способность формирования РПС на основе уже имеющихся, заранее сформированных баз аллофонов, а также добавления к ним РПС генерируемых непосредственно из речи участников разговора. Применение данной методики позволит начать синтез РПС в необходимый момент времени благодаря использованию заранее сформированных баз аллофонов из речи произвольных дикторов и аллофонов, выделяемых непосредственно из речи участников разговора.

Таким образом, была разработана методика компиляционного синтеза РПС непосредственно из речи участников разговора с использованием заранее сформированных баз аллофонов с одновременным подмешиванием РПС, который формируется непосредственно из речи участников переговоров. Данная методика включает детектирование речи, верификацию диктора, сегментацию и классификацию речи и может использоваться для защиты акустической информации от утечки по техническим каналам путем ее маскирования.

Литература:

1. Активные и пассивные методы и средства защиты информации от утечки по техническим каналам / Аль-Хатми М.О., Зельманский О.Б., Лыньков Л.М., Петров С.Н. – Минск: Бестпринт, 2011. – 275 с.
2. Информационные технологии. Средства защиты речевой информации виброакустические. Классификация и общие технические требования : СТБ П 34.101.28–2007. – Введ. 01.04.2008. – Минск: НП РУП «Научно-исследовательский институт технической защиты информации», 2008. – 8 с.
3. Зельманский, О.Б. Построение программного модуля детектирования речи на основе классификационных параметров аудиосигнала / О.Б.Зельманский // Доклады БГУИР. – 2008. – № 7(37). – С. 72–76.
4. Зельманский, О.Б. Программные средства текстозависимой верификации диктора по голосу / О.Б.Зельманский // Доклады БГУИР. – 2009. – № 4(42). – С. 37–41.
5. Зельманский, О.Б. Модуль сегментации речи для систем синтеза речеподобных сигналов / О.Б. Зельманский, А.Г. Давыдов // «Milex 2011»: материалы V Междунар. науч.-техн. конф. по военно-техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения. – Минск, 2011. – С. 386.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОФИЛИАЛЬНОГО ТЕЛЕКОММУНИКАЦИОННОГО ПРЕДПРИЯТИЯ

**В.А. Бойправ, О.В. Бойправ, Л.М. Лыньков,
БГУИР, г. Минск**

В настоящее время большинство предприятий стремится к усовершенствованию процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации. Это явление должно сопровождаться изменениями и дополнениями в системе информационной безопасности (СИБ) предприятия, базирующимися на изменениях и дополнениях в стандартах и нормативно-правовых актах в области информационной безопасности. Для того, чтобы усовершенствования носили своевременный характер, наряду с СИБ на предприятии должна существовать система менеджмента информационной безопасности (СМИБ). Последняя является частью системы менеджмента предприятия, следовательно, ее структура зависит от структуры предприятия. В то же время политика, деятельность по планированию, обязанности, практика, процедуры, процессы и ресурсы СИБ определяются стратегическими целями, отраслью, спецификой и конечным результатом деятельности предприятия. Например, стратегической целью телекоммуникационного предприятия (предприятия отрасли связи) является своевременное удовлетворение спроса со стороны населения и организаций на конечный результат его деятельности – услуги телеграфа, телефонии, сети Интернет и другие. Чем шире спектр оказываемых услуг, тем масштабнее предприятие и сложнее схема его управления.

В Республике Беларусь одним из крупнейших телекоммуникационных предприятий является республиканское

унитарное предприятие (РУП) «Белтелеком», которое включает в себя десять филиалов, расположенных в областных центрах и столице страны, а также два структурных подразделения в составе аппарата управления. Количество абонентов РУП «Белтелеком» составляет более 4,5 миллионов физических и юридических лиц. Они являются потребителями услуг телефонии, сети Интернет, проводного вещания, хостинга и цифрового интерактивного телевидения. Каждый из филиалов РУП «Белтелеком» занимается обслуживанием и эксплуатацией определенного набора телекоммуникационного оборудования, необходимого для предоставления ряда из перечисленных услуг. Следовательно, каждому филиалу РУП «Белтелеком» целесообразно поддерживать свою СМИБ, являющуюся частью общих СМИБ и системы менеджмента предприятия.

Согласно ISO/IEC IS 27001 процесс менеджмента информационной безопасности (МИБ) должен носить циклический характер и включать в себя стадии планирования, реализации, проверки и совершенствования. Эти четыре стадии можно назвать жизненным циклом СМИБ.

Стадия планирования в РУП «Белтелеком» должна быть связана с обсуждением и установлением дополнений и изменений для стратегической (общей) и тактических (для каждого из филиалов) политик информационной безопасности (ПИБ). При этом комиссия по обсуждению возглавляется генеральным директором предприятия, членами комиссии являются заместители генерального директора и представи-

тели каждого из филиалов либо структурных подразделений (директора, главные инженеры). Обсуждение дополнений и изменений в ПИБ проводится с учетом результатов текущего анкетирования начальников отделов филиалов (структурных подразделений) предприятия по вопросам обеспечения информационной безопасности на вверенных им объектах. Отчет о результатах проведения данного анкетирования по каждому из филиалов (структурных подразделений) должен представляться их директорами. Кроме того, на стадии планирования для каждого из филиалов (структурных подразделений) из списка его сотрудников должны выбираться лица, ответственные за контроль выполнения положений стратегической и тактической ПИБ.

Стадия реализации должна быть связана с осуществлением, внедрением и поддержкой стратегической и тактических ПИБ. На данной стадии с внесенными комиссиями изменениями и дополнениями в стратегическую ПИБ предприятия и тактическую ПИБ филиала должен быть под роспись ознакомлен каждый сотрудник, имеющий доступ к информационной системе данного предприятия. Дополнительно на данной стадии лицами, назначенными ответственными за контроль выполнения положений стратегической и тактической ПИБ, должен по согласованию с директором и главным инженером филиала (структурного подразделения) разрабатываться перечень мер, которые будут предприниматься по отношению к сотрудникам, допускающим нарушения положения ПИБ. С утвержденным перечнем так же, как и с принятыми изменениями и дополнениями ПИБ, должен быть своевременно ознакомлен каждый сотрудник.

На стадии проверки оценивается и, если необходимо, измеряется эффективность процессов МИБ организации на соответствие требованиям ПИБ, а также подготавливаются отчеты генеральному директору о результатах проведения соответствующего анализа. Повысить уровень объективности результатов измерения эффективности процессов МИБ возможно путем проведения независимого аудита системы информационной безопасности филиала (структурного под-

разделения), при котором в состав аудиторской группы не входят сотрудники филиалов (структурных подразделений) РУП «Белтелеком». При этом отчет генеральному директору о результатах проведения данного измерения представляется руководителем аудиторской группы. Предварительно положения этого отчета должны быть обсуждены с директором филиала (структурного подразделения), в котором был проведен аудит.

Результаты стадии проверки определяют необходимость внеочередного заседания комиссии по обсуждению и установлению дополнений и изменений в ПИБ и, как следствие, комплекс мероприятий для стадии совершенствования СМИБ. В случае, если принимается отрицательное решение по вопросу проведения внеочередного заседания комиссии, то перечень мер, корректирующих и совершенствующих СМИБ филиала (структурного подразделения), разрабатывается его директором и главным инженером, и согласуется с руководителем аудиторской группы. Наряду с результатами аудита системы информационной безопасности филиала (структурного подразделения), при составлении данного перечня мер следует учитывать данные о планируемых сроках проведения очередного заседания комиссии по обсуждению и установлению дополнений и изменений в ПИБ. По факту принятия и реализации мер, корректирующих и совершенствующих СМИБ филиала (структурного подразделения), его директор должен представить отчет генеральному директору предприятия. Завершающими мероприятиями стадии совершенствования СМИБ должны являться анкетирование начальников отделов филиалов (структурных подразделений) по вопросам обеспечения информационной безопасности на вверенных им объектах и составление отчетов по результатам данного анкетирования.

Таким образом, продолжительность и комплекс мероприятий каждой последующей стадии жизненного цикла СМИБ филиалов (структурных подразделений) многофилиального предприятия определяется результатами комплекса мероприятий его предыдущих стадий.

К ВОПРОСУ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ САРТСНА ДЛЯ ЗАЩИТЫ СЕТЕВЫХ РЕСУРСОВ

Н.Н. Кузьмицкий, С.С. Дереченник, Д.А. Костюк,
БрГТУ, г. Брест

Введение

История использования графических изображений в качестве основы теста Тьюринга (Completely Automated Public Turing tests to tell Computers and Humans Apart или CAPTCHA), призванного предотвратить массовую автоматизированную эксплуатацию сервисов, предоставляемых посетителям сетевого ресурса для единичного использования, насчитывает более 10 лет [1]. Исходная сфера применения CAPTCHA-тестов – развлекательные веб-сайты и цифровые медиа, окупаемость которых построена на периодическом показе посетителям рекламы и предложении более комфортных платных вариантов сервиса – предполагала незначительный ущерб в случае обхода данного вида защиты. Однако по мере внедрения веб-сервисов государственными и иными

учреждениями (например, услуг сетевой регистрации) возможный ущерб становится гораздо более серьезным, меняясь от сравнительно небольших коммерческих убытков и издержек массовой рассылки несанкционированной рекламы к возможности затруднить либо полностью парализовать работу медицинских учреждений, банков и др. организаций. Показателен пример блокирования электронной регистрации в консульствах Республики Польша, осуществляемого злоумышленниками для перехвата и последующей перепродажи мест в очереди на собеседование, в результате чего для граждан Беларуси оказался практически недоступен установленный порядок получения визы [2].

Подход к защите от подобных вредоносных программ построен на применении тестов, легко выполнимых че-

ловеком и непреодолимыми автоматизированными системами. При этом в настоящее время подавляющая часть CAPTCHA-тестов основана на вводе субъектом строки текста, в полной мере (порядок символов, регистр) соответствующей образам графических изображений (см. примеры на рисунке 1).

Рукописный текст имеет ряд принципиальных отличий от машинописного (разнообразие стилей письма, геометрических, топологических свойств символов др.). Кроме того, затруднено решение большинства задач в его автоматическом анализе (распознавание символов, сегментация). Поэтому изображения рукописных слов являются наиболее подходящими для создания CAPTCHA-тестов.

Хотя для обхода нередко применяются и не прямые способы (поиск уязвимостей веб-сайта, привлечение массового человеческого ресурса), судить о принципиальной эффективности защиты CAPTCHA-тестами можно только на основе возможности прохождения теста с помощью технологий искусственного интеллекта. Разнообразие сфер практического применения систем OCR (Optical Character Recognition) приводит к постоянному совершенствованию имеющихся и разработке новых методик распознавания текста. В связи с незначительными изменениями типов искаженных изображений, используемых для защиты, и расширением сфер их применения до критически важных, становится актуальным вопрос, насколько надежны на текущий момент CAPTCHA-тесты для блокирования автоматизированных атак. В русле данного исследования и находится представленная работа. При этом основное внимание уделяется оценке возможности созданию универсального классификатора цифровых образов на основе нейросетевого подхода, который является одним из наи-

более гибких механизмов, перспективных для работы с искаженными образами символов.

Классификатор цифровых образов

Под универсальностью классификатора будем понимать его способность сохранять высокую точность распознавания на произвольной выборке входных данных. В зависимости от способа получения рассмотрим три типа текстовых образов: машинописные, рукописные и синтезированные. Изображения последнего типа подобны символам CAPTCHA, т. к. являются результатом применения пространственных преобразований к образам первых двух. Для их генерации была разработана методика, основанная на технике «волновых искажений», позволяющих имитировать эффекты от воздействия неблагоприятных окружающих условий или дефектов аппаратуры [3]. Примеры изображений выделенных типов приведены на рисунке 2.

В качестве базовой для решения задачи распознавания нами выбрана представленная на рисунке 3 сверточная нейросетевая архитектура (CNN), особенностями которой являются:

- 1) локальные рецептивные поля (нейроны получают входной сигнал от окрестностей нейронов предыдущего слоя, за счет чего сеть обучается двумерной структуре входного образа);
- 2) разделяемые веса (нейроны слоя объединены картами, в которых они обладают общими весами, при этом карты генерируют различные признаки и сокращают количество параметров, настраиваемых в ходе обучения);
- 3) пространственные подвыборки (локальное усреднение откликов карт приводит к синтезу высокоуровневых признаков и повышает инвариантность сети к искажениям) [4].

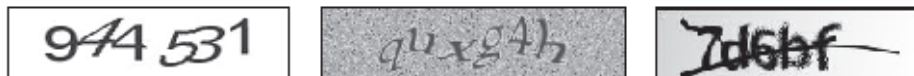


Рисунок 1 – Примеры графических CAPTCHA-тестов

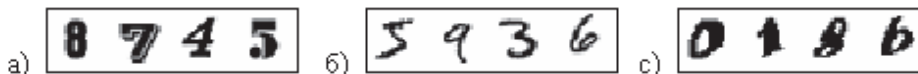


Рисунок 2 – Примеры машинописных (а), рукописных (б) и синтезированных (с) образов

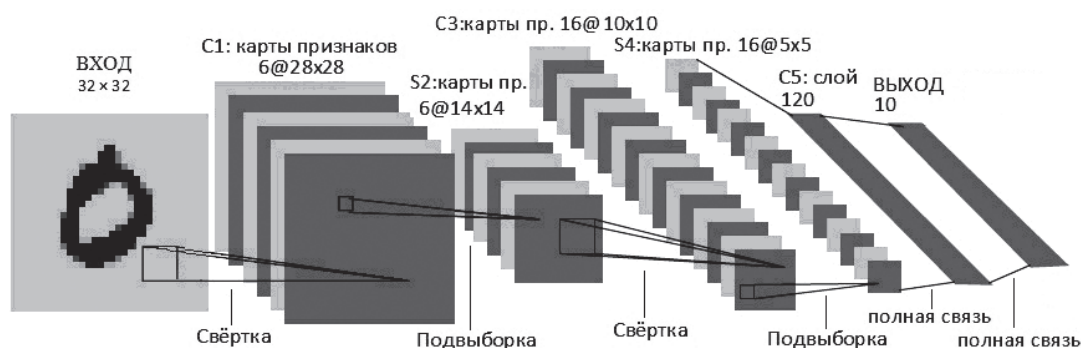


Рисунок 3 – Сверточная нейросетевая архитектура (CNN)

Таблица 1 – Точность распознавания (в %) CNN-экспертами образов

CNN эксперт	MNIST_train	FONT_train	KNI_train	Среднее для 3-х	MNIST_test	FONT_test	KNI_test	Среднее для 3-х
CNN_MNIST	99.68	96.75	85.21	93.88	99.39	95.23	85.06	93.22
CNN_FONT	86.68	99.88	88.34	91.63	87.23	99.58	88.06	91.62
CNN_KNI	86.48	94.54	99.38	93.46	86.52	92.97	99.29	92.92
Среднее	90.94	97.05	90.97	92.99	91.04	95.92	90.80	92.58

Таблица 2 – Точность распознавания (в %) комитетами образов тестовых частей баз

Комитет CNN	MNIST_test	FONT_test	KNI_test	Среднее для 3-х
MAX_COM	98.23	98.62	98.56	98.47
AVER_COM	97.64	99.11	98.10	98.28
MAJOR_COM	93.82	98.50	98.86	97.06
MKF	99.15	99.56	99.86	99.52
KADMOS	95.84	98.68	84.95	93.15

Выделенные типы изображений послужили прообразами к созданию трех видов экспертов, под которыми понимаются CNN, специализирующиеся в распознавании изображений одного из типов. Для построения экспертов использовалась рукописная (MNIST, 60000/10000 образов в тренировочной/тестовой части), машинописная (FONT, 20000/5000 образов) и синтезированная (KNI, 60000/10000 образов) базы данных. Результаты тестирования экспертов представлены в таблице 1, на основании данных которой можно отметить:

1) использованная архитектура CNN и методика ее обучения позволили достичь более 99% точности распознавания экспертами образов своих баз;

2) максимальный уровень ошибок был показан экспертами на множестве KNI_train, соответствующем символам CAPTCHA;

3) эксперт, обученный на основе MNIST, обладал лучшей средней точностью как на тренировочных (93.88%), так и на тестовых (93.22%) частях баз;

4) средняя точность экспертов (92.58%) на тестовых множествах показала низкую универсальность нейросетевой модели (аналогичное замечание справедливо и для других методов машинного обучения, в частности, метода опорных векторов (SVM)).

Для повышения обобщающих характеристик CNN использовались технологии коллективного распознавания, представленные двумя подходами:

– эксперты объединены в три комитета, названия которых соответствуют применяемой ими схеме голосования членов: MAX_COM, AVER_COM, MAJOR_COM;

– базы образов объединены в одну смешанную (по 20 000 примеров из каждой типовой), на основе которой с использованием процедуры «регулярного масштабирования» [5] построены несколько CNN, сформировавших комитет MKF, имеющий усредняющую схему голосования.

Результаты тестирования полученных комитетов и системы KADMOS (коммерческий продукт, специализирующийся в решении OCR задач) представлены в таблице 2. Отметим, что с помощью второго подхода также был создан комитет для заглавных букв английского языка, средняя точность распознавания которого на трех типовых базах составила 98,44%.

Анализ данных таблицы приводит к следующим выводам:

1) интеграция знаний CNN в комитеты позволяет существенно повысить точность распознавания (минимум – на 4,48%, максимум – на 6,94%);

2) наиболее эффективным оказался комитет, CNN в котором были обучены на смешанной базе образов, что позволило им сформировать более информативные признаки классов;

3) средняя точность комитета MKF (99,52%) показывает его высокую универсальность и стабильность характеристик, в отличие от модуля KADMOS (особенно на синтезированной базе символов, подобных CAPTCHA (84,95%)).

Заключение

Результаты проведенных исследований показали, что современные технологии искусственного интеллекта способны приблизиться к созданию универсального классификатора алфавитно-цифровых данных, что помимо своей безусловной практической пользы может привести к необходимости разработки новых путей выявления автоматизированных атак.

Литература:

1. L. von Ahn, M. Blum, J. Langford. Telling humans and computers apart automatically // Communications of the ACM. Vol. 47, No. 2. – 2004. – P. 57–60.
2. Посол Польши признал наличие проблем с электронной регистрацией на получение визы. // Новости Беларуси. Белорусское телеграфное агентство. 14 ноября 2012 г. <http://tinyurl.com/bq3vsxc>
3. N. Kuzmitsky, S. Derechennik. The problem of «brittleness» of convolutional neural networks in recognition of digit patterns with different writing styles // Proceedings of the 7th International Conference Neural Networks and Artificial Intelligence (ICNNAI). – 2012. – P. 235–238.
4. Y. LeCun, L. Bottou, Y. Bengio and P. Haffner. Gradient-Based Learning Applied to Document Recognition // Proceedings of the IEEE, 86(11). – 1998. – P. 2278–2324.
5. Н.Н Кузьмицкий. Об одном значимом результате в распознавании образов рукописных цифр // Материалы Международной научной конференции «Информационные технологии и системы». – 2012. – С. 228–229.

ПРИМЕНЕНИЕ ДИОДОВ-ГЕНЕРАТОРОВ ШУМА В СРЕДСТВАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. Буслюк, БрГТУ, г. Брест;

В.А. Тюнин, П.Н. Лаптев, ОКБ САПР, г. Пенза;

С.И. Ворончук, И.В. Лешкевич, Частное научно-исследовательское предприятие «СКБ «Запад», г. Брест

Введение

Физические источники шума находят применение в различных областях техники, в том числе в программно-аппаратных средствах защиты информации.

Шум, генерируемый физическими источниками, может быть использован, например, для маскирования информативных побочных электромагнитных излучений и наводок (ПЭМИН) от средств вычислительной техники, исключающего возможность перехвата ПЭМИН за пределами контролируемой зоны путем создания помех в широкой полосе частот.

Другое возможное применение физического шума в средствах защиты информации – использование случайных битовых последовательностей для генерации ключевой информации в средствах криптографической защиты информации. Поскольку в современной криптографии алгоритмы шифрования считаются общеизвестными, а безопасность информации основывается на правильном выборе ключа шифрования (принцип Керкгоффса), то задача качественной генерации ключевой информации является очень важной.

1 Аппаратная реализация

Схема включения шумовых диодов, приведенная на рисунке 1, соответствует рекомендуемой в [1]. В качестве источника опорного напряжения $U_{оп}$ величиной $15,5 \pm 0,5$ мВ был выбран интегральный источник напряжения (DA2), с установленным на его выходе резистивным делителем (R4, R6). Использование интегральной микро-

схемы, прецизионных резисторов, низкое выходное сопротивление полученного источника опорного напряжения (при высоком входном сопротивлении компаратора) позволяют добиться достаточной стабильности параметров, высокой помехоустойчивости, низкой стоимости и хорошей повторяемости схемы в целом.

2 Оценка качества случайных битовых последовательностей

Для получения случайных цифровых последовательностей сигнал $U_{цифр}$ с выхода компаратора (рисунок 1) подавался на микроконтроллер Atmel ATSAM3U, после чего полученный поток битов сохранялся в файл с целью дальнейшей оценки качества случайной последовательности.

В настоящее время наибольшей популярностью пользуются два набора тестов оценки качества случайных последовательностей – пакет NIST американского Национального института стандартов и технологий (http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html) и тест DIEHARD Джорджа Марсальи (<http://stat.fsu.edu/pub/diehard/>).

Оценка качества цифрового шума выполнялась путем анализа сравнительно длинных (более 1 Мбит) последовательностей набором тестов NIST.

Пакет NIST состоит из 15 статистических тестов, целью которых является определение меры случайности двоичных последовательностей, порожденных генераторами случайных (псевдослучайных) чисел. Эти тесты основаны на различных

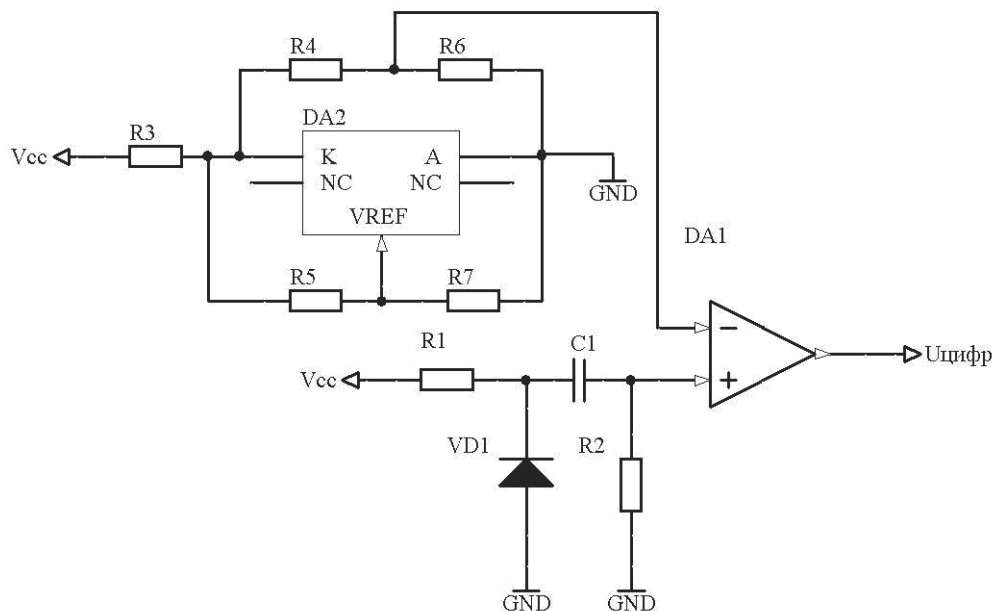


Рисунок 1 – Практическая схема включения шумовых диодов

статистических свойствах, присущих только случайным последовательностям. Обзор тестов приведен в [2], подробное описание в [3]. Пользователю доступна возможность настройки отдельных тестов, однако, в данном эксперименте пакет тестов был использован с настройками «по умолчанию».

Проведенные тесты дали следующие результаты – случайная последовательность успешно прошла 13 тестов, однако два теста не были пройдены. Тесты, выявившие отклонение исследуемой последовательности от случайной, – тест кумулятивных сумм (Cumulative Sums (Cusum) Test) и частотный побитовый тест (Frequency (Monobit) Test). На основании описаний данных тестов можно сделать вывод о том, что неуспешный результат вызван дисбалансом количества единиц и нулей в исследуемой последовательности. Эта гипотеза легко проверяется простым подсчетом микроконтроллером количества нулей и единиц в исследуемой последовательности, который действительно выявляет отличие математического ожидания от 0,5 в последовательности, которая предположительно должна быть случайной (и, соответственно, содержать в идеальном случае равное количество единиц и нулей). Такое отклонение от ожидаемого результата не является необычным и его можно объяснить неидеальностью элементов электрической схемы – самих шумовых диодов, резисторов, источника опорного напряжения.

3 Пути повышения качества случайных цифровых последовательностей

Для того, чтобы улучшить качество случайной последовательности (добиться равномерного распределения), необходимо провести некоторые дополнительные преобразования. В простейшем случае можно, например, складывать по модулю 2 (xor) соседние биты в исходной последовательности. Если входные данные независимы, и имеют отклонение от равномерного распределения ϵ , то последовательность на выходе будет иметь отклонение 2ϵ . Также возможно использование схемы фон Неймана (von Neumann's debiasing scheme) [4], суть работы которой состоит в том, что из исходной последовательности берется пара битов и, если биты различаются, в выходную последовательность добавляется первый из них, а если биты одинаковы, то они отбрасываются. Если исходная последовательность является стационарной, то последовательность на выходе схемы фон Неймана характеризуется дискретным равномерным распределением, однако, следует помнить о том, что корректор фон Неймана генерирует последовательность с неравномерным распределением, если внутри исходной последовательности существуют циклы с

периодом 2. Поэтому при практической реализации датчиков случайных чисел (ДСЧ) последовательность с выхода корректора рекомендуется подавать на вход криптографической хэш-функции, которая вносит в данную последовательность дополнительную энтропию.

Dan Boneh (Stanford University) в своих лекциях по криптографии (<https://class.coursera.org/crypto-preview/class/index>) рекомендует использовать для обработки «сырой» случайной последовательности с неравномерным распределением сеть Фейстеля [5]. Учитывая, что многие стандартизированные блочные шифры (DES, ГОСТ 28147-89) построены на основе сети Фейстеля, а разработчики программных (программно-аппаратных) средств защиты информации очень часто уже имеют в своем распоряжении библиотеки (модули, IP-ядра), реализующие указанные алгоритмы шифрования, видится разумным использование блочных шифров для улучшения характеристик последовательностей, полученных от физических ДСЧ.

Выводы

На основе рекомендаций [1] разработчиков шумовых диодов, рассмотрены возможности применения этих приборов в практических схемах средств защиты информации. Дальнейшего исследования требуют варианты обработки случайных цифровых последовательностей – сравнение эффективности этих методов (получение максимально качественного шума) и их быстроты действия.

Литература:

1. Буслюк, В.В. Режимы применения кремниевых генераторных диодов для создания широкополосного шума / В.В.Буслюк, С.И. Ворончук, И.В. Лешкевич // Материалы и структуры современной электроники: сб. науч. тр. 5-й Междунар. науч. конф., Минск, 10-11 окт. 2012 г. – Минск: БГУ, 2012. – С. 24-27.
2. Soto, J. Statistical Testing of Random Number Generators / J.Soto // [Electronic resource]. – Mode of access: <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf>
3. Rukhin, A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A.Rukhin, et al. // [Electronic resource]. – Mode of access: <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf>
4. Entropy Key // [Electronic resource]. – Mode of access: <http://www.entropykey.co.uk/res/download/diagram-explanation.pdf>
5. Feistel cipher / From Wikipedia, the free encyclopedia // [Electronic resource]. – Mode of access: http://en.wikipedia.org/wiki/Feistel_cipher

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ПРОТОКОЛОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В EDI СИСТЕМАХ НА ПРИМЕРЕ ОНТОЛОГИИ ПРОТОКОЛА AS2

А.В. Агафонов, О.В. Линич, Научно-инженерное республиканское унитарное предприятие «Межотраслевой научно-практический центр систем идентификации и электронных деловых операций»

В настоящее время при проектировании информационных систем все чаще находят применение новейшие технологии и разработанные специально для них инстру-

ментальные средства. Одной из таких технологий является технология семантического Web и созданный язык OWL (Web Ontology Language) – язык описания онтологий для

описания классов и отношений между ними, присущих Web-документам и Web-ориентированным приложениям.

Данный язык может являться основным инструментом проектировщика, выполняющего бизнес-анализ проблемной области, определяющего классы (концепты) их отношения, свойства объектов и структуры данных.

Исключительным свойством разработки онтологии для конкретной задачи является получаемый результат – готовый тезаурус, описывающий проблемную область в формате XML, который можно применять для создания методических рекомендаций по разработке программного обеспечения или напрямую использовать на информационных ресурсах посвященных конкретной тематике.

В докладе приводится пример реализации онтологии, описывающей все аспекты протокола AS2 (Applicability Statement 2), на основе которой создана методология разработки программного обеспечения для сервера гарантированной доставки сообщений (EDI-сервера).

Электронный обмен данными (Electronic Data Interchange – EDI) – это электронная передача данных в виде структурированных сообщений в согласованном формате между компьютерными системами при минимальном участии человека.

Сервер EDI осуществляет электронный обмен данными между участниками бизнес-процесса. Клиент подключается к серверу EDI и может выполнять коммерческие транзакции с любым из подключенных партнеров. Клиент формирует электронный документ, который передается на сервер. Сервер проверяет правильность поступившего сообщения. Если документ имеет правильную структуру и допустимые данные, сервер регистрирует сообщение, определяет получателя сообщения и отправляет ему сообщение. Если сообщение не прошло проверку, клиент получает уведомление об ошибке в документе.

Для надежной и безопасной передачи данных EDI и XML документов по Интернету через HTTP используется стандарт AS2. Безопасность и безопасная передача данных по стандарту AS2 через Интернет обеспечиваются следующими технологиями:

- конфиденциальность обеспечивает безопасность передачи информации, содержащейся в сообщении, шифруя данные;
- аутентификация – удостоверение подлинности происходит через проверку электронной подписи отправителя;
- достоверность сообщения достигается через использование MDN (оповещений о местонахождении сообщений) для контрольных сумм и полностью исключает возможность изменения документа без ведома получателя;

– невозможность отрицать получение сообщения – получатель подписывает оповещение о местонахождении документа, направляет его назад отправителю и, таким образом, уже не может заявить, что не получал его.

Для любого электронного обмена сообщениями требуется отправитель и получатель. Сервер коммуникации получателя настроен на «прослушивание» сообщений в Интернете, которые обращаются к нему.



Рисунок 1 – Онтология протокола AS2

Для AS2 используется асинхронный или синхронный режим передачи MDN (Message Disposition Notification). Существуют потенциальные проблемы с синхронным и с асинхронным режимами передачи MDN, поэтому существует необходимость в совместном определении торговыми партнерами, какая опция лучше всего подходит к их операционным средам и характеристикам сообщения.

Обычно для AS2 используется транспортный протокол HTTP. Однако, если есть необходимость в обеспечении безопасности AS2-To и AS2-From адреса и другой информации заголовка AS2, может быть использован протокол HTTPS в дополнение к кодированию информации AS2. Кодирование, используемое HTTPS, обеспечивает только тип связи точка-точка непосредственно между клиентом и сервером.

Цифровые сертификаты могут быть от доверенной третьей стороны или самостоятельно подписаны, если данный подход согласован обеими сторонами. Если используются свидетельства от третьего лица, трастовый уровень должен быть как минимум «Class 2», который гарантирует, что была сделана проверка подлинности человека и организации.

Для кодирования и подписи может использоваться единый цифровой сертификат, однако, если есть необходимость, допускается использование двух отдельных сертификатов.

Получение сообщений AS2 на единственном порту (для каждого протокола) значительно минимизирует операционные сложности, такие как установка файервола и потенциальная незащищенность для отсылки и получения.

Для реализации полноценного в функциональном плане протокола AS2 в сервере EDI необходимо обеспечить имплементацию группы стандартов, определяющих составляющие протокола, объединив всю информацию в методические рекомендации по разработке.

Для этого была разработана онтология полноценного в функциональном плане протокола AS2, с учетом всех его составляющих. Для разработки использовался программный продукт Protégé версии 4.2.0. (Build 256).

Все элементы онтологии имеют детальное описание URI на конкретные стандарты, определены атрибуты концептов, их отношения и базовые данные, необходимые для реализации AS2.

«Consortium». Созданием и стандартизацией данного протокола занимались несколько международных ассоциаций, среди которых можно выделить:

- Internet Engineering Task Force. Группа ответственна за ведение RFC документов Request For Comments (серии пронумерованных информационных документов, размещаемых в Internet по техническим спецификациям и стандартам;
- Word Wide Web Consortium.

«Protocols». В составе онтологии определен ряд современных протоколов, относящихся к протоколам Application Statement:

- AS1 – электронная почта на базе SMTP;
- AS2 – обмен сообщениями на базе HTTP/HTTPS;
- AS3 – обмен файлами на базе FTP;
- AS4 – функционально расширенный AS2.

AS2 подразделяется по своему функциональному наполнению на четыре вида обмена по отношению к сообщению MDN:

- AS2 по MDN – сообщение MDN не передается отправителю;

- AS2 Synch MDN – возврат синхронного MDN через HTTP(S) отправителю в рамках одного сеанса. Это достаточно быстрый режим, но при больших размерах передаваемого AS2 сообщения возможна ситуация тайм-аута;

- AS2 Email MDN – возврат асинхронного MDN уведомления через Email. Редко используемый режим;

- AS2 Asynch MDN – возврат асинхронного MDN через HTTP(S) отправителю. Этот режим позволяет возвратить MDN в другом сеансе. Особенно приемлем для передачи больших файлов.

«Standards» – все стандарты, влияющие на разработку AS2.

RFC 4130 является комплексным стандартом, ратифицированный IETF для всех MIME-based EDINT (a.k.a. AS2) протоколов обмена.

MIME-based стандарты показаны в онтологии и определяют следующие составляющие разрабатываемого протокола:

- RFC 2616 – протокол передачи гипертекстовой информации (HTTP);
- RFC 1767 – формирование содержимого электронных сообщений (EDI Content Type);
- RFC 3023 – формирование медиа информации (XML Media Types);
- RFC 1847 – алгоритмы безопасности для MIME (Security Multiparts for MIME);
- RFC 3462 – формирование отчетов о доставке (Multipart/Report);
- RFC 2045 to 2049 MIME RFCs – описание MIME;
- RFC 3798 – описание сообщения MDN (Message Disposition Notification). Данный стандарт для разработчиков описывает сообщение MDN и регламенты его обработки и является основой для реализации;
- RFC 3851, 3852 – спецификации S/MIME v3.1 Specification.

«Messages». Стандарты определяют следующие сообщения:

- EDI message – оригинальное сообщение EDI условно любого формата, описанное в онтологии как концепты «Formats»;
- MDN-сообщение – Message Disposition Notification обеспечивает уведомление о диспозиции (месте) сообщения, указывая к примеру, где сообщение было прочитано реципиентом или отвергнуто после прочтения и т.д. Определяется стандартом RFC 3798;

- Reply ответ на EDI-сообщение в соответствии с установленной «хореографией» обмена сообщениями;

- Receipt – функциональное сообщение, посылаемое от получателя к отправителю, как подтверждение выполненного обмена. В определенных случаях трактуется как эквивалент MDN или им же является.

«Formats». Сообщения для информационного обмена в торговых операциях могут представляться в следующих форматах:

- EANCOM – формат сообщений, регламентированный стандартами UN/CEFACT (электронные сообщения в администрации, транспорте и логистике). Подмножеством являются сообщения EANCOM 2003;

- ANSI X12 – американский стандарт обмена сообщениями ANSI X12;

– GS1 XML – форматы обмена сообщениями в XML, определяемые в настоящее время GS1 XML (эквивалентные по составу сообщениями EANCOM 2003);

– ECR-ru – формат электронных сообщений, разработанный ассоциацией ECR-rus, используемый EDI-провайдерами в России и по составу совпадающий с EANCOM 2003.

«Subjects». Основными субъектами, участвующими в информационном обмене, определены два следующих субъекта:

– User Agent – приложение, которое формирует и обрабатывает AS2 запросы;

– Requested_URI URI-обработчика получаемых сообщений (к примеру сервера).

«Languages». В качестве применяемых языков стандартами регламентированы языки HTML и XML.

«Algorithms». Основные алгоритмы, применяемые в данной технологии, следующие:

– SHA-1 – однократный алгоритм шифрования, используемый в сочетании с ЭЦП. Основной алгоритм, рекомендуемый для работы протокола AS2;

– MD5 – однократный алгоритм шифрования, используемый в сочетании с ЭЦП. Возможно использование для AS2;

– MIC – Message Integrity Check – это протокол проверки целостности пакетов. Протокол позволяет отбрасывать пакеты, которые были «вставлены» в канал третьим лицом.

На рисунке 1 приведен фрагмент онтологии, элементы (концепты) которой отражают все составляющие протокола AS2 и отношения между ними.

Разработанная для конкретной задачи онтология позволяет получить готовый тезаурус, описывающий проблемную область в формате XML, который можно применять для создания методических рекомендаций по разработке программного обеспечения или напрямую использовать на информационных ресурсах посвященных конкретной тематике.

КОНЦЕПЦИЯ СОЗДАНИЯ И ТЕКУЩЕЕ СОСТОЯНИЕ СЕРВИСОВ ДОВЕРЕННОЙ ТРЕТЬЕЙ СТОРОНЫ, РАЗВЕРНУТЫХ В ПРОСТРАНСТВЕ РОССИЯ – БЕЛАРУСЬ

В.Н. Кустов, С.А. Кирюшкин, Т.Л. Станкевич,
ООО «УЦ ГИС», г. Санкт-Петербург

В связи с интенсивным развитием электронного документооборота на корпоративном, государственном и межгосударственном уровне задача обеспечения юридической силы электронных документов (ЭД) приобрела особую актуальность. Традиционной технологией обеспечения юридической силы электронных документов, закрепленной национальными и международными нормативами является криптографическая электронная подпись, обеспечиваемая инфраструктурой открытых ключей (PKI) на основе системы сервисов доверенной третьей стороны (ДТС).

Наиболее широко рассматриваемым в настоящее время в контексте трансграничного юридически-значимого документооборота является сервис DVCS (Data Validation and Certification Server) – сервис в составе ДТС, который предоставляется удостоверяющим центром (УЦ), и обеспечивает проверку электронной подписи (ЭП) документа, инвариантно по отношению к использованным для ЭП средствам криптографической защиты информации (СКЗИ) и правовому полю, в котором подписан ЭД. В настоящее время данный сервис развернут силами ООО «ГАЗИНФОРМ-СЕРВИС» (Санкт-Петербург) и ЗАО «Белтим СБ» (Минск) на пространстве Россия – Беларусь.

Основными факторами, повышающими интерес к данной технологии и ее нормативному и организационному обеспечению, являются:

1) глобализация мировой экономики;

2) наличие выстроенной правовой модели, являющейся правовой основой технологии (совокупность международных документов в масштабе ЕврАзЭК) и гармоничное сочетание с ней национальных законодательств России, Беларуси и Казахстана, а так же проекта общеевропейского «Положения...», приходящего на смену Директиве ЕС 1999/93;

3) жесткая позиция национальных регуляторов в части, касающейся применения национальных криптографических стандартов;

4) наличие международных стандартов и рекомендаций на данную технологию;

5) положительный опыт практической эксплуатации;

6) широкое использование технологий на базе PKI.

Вот лишь некоторые заметки по вопросу об ориентации законодательства РФ в направлении формирования единого пространства доверия.

– Ст.13 п. 9 Федерального закона от 06 апреля 2011 года №63-ФЗ «Об электронной подписи» определяет, что УЦ «осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей», то есть, эту услугу должен оказывать любой УЦ, независимо от того, каким УЦ был изготовлен сертификат и какое использовано СКЗИ.

– Приказ Минкомсвязи РФ № 221 2 сентября 2011 г. N 221 г. «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения», п.15: Для проверки аутентичности, целостности и достоверности электронных документов СЭД ФОИВ должна хранить результат проверки электронной подписи в виде метаданных электронного документа.

– Государственный стандарт об электронном документообороте – ГОСТ Р /ISO/TR 15801:2009 (Системы электронного документооборота) устанавливает, что в случае применения электронной подписи (или иных методов электронного подписания) в составе контрольной информации следует сохранять следующие сведения:

- 1) идентифицирующие данные файла;
- 2) подтверждение личности подписанта (certification of identification);
- 3) идентифицирующие данные удостоверяющего органа (authenticating authority);
- 4) дату и время подписания;
- 5) квитанцию/подтверждение получения;
- 6) доказательство проверки подписи.

Изменения в международном нормативном регулировании в области электронного документооборота отражены в Проекте «Положения европейского парламента и совета об электронной идентификации и сервисам доверия для электронных транзакций на внутреннем рынке». Этот проект, в частности, устанавливает:

- 1) правила электронной идентификации и электронных сервисов доверия для электронных транзакций;
- 2) условия, на которых Государства-участники должны признавать и принимать средства электронной идентификации физических и юридических лиц;
- 3) правовую основу для электронных подписей, электронных печатей, электронных штампов времени, электронных документов, электронных сервисов доставки и аутентификации веб-сайтов;
- 4) гарантирует, что доверенные услуги и товары разрешены к свободному обороту на внутреннем рынке ЕС.

Сервис DVCS, в соответствии с RFC 3029, реализует 4 вида запросов: vkrc, cpd, cspd, vsd. По результатам обработки запроса формируется квитанция, которая отправляется пользователю, сформировавшему запрос.

Ядром сервиса является библиотека, реализующая базовые криптографические функции клиентских и серверных приложений.

Сервис DVCS обеспечивает функциональность, представленную на рисунке 1.



В настоящее время в России идет активное развертывание общедоступного сервиса ДТС по проверке ЭП, сформированной с использованием стандартизированных в РФ СКЗИ, и ЭП, сформированной с применением СКЗИ Республики Беларусь. В ближайшем будущем планируется провести эту же работу на пространстве Россия – Казахстан, что станет следующим шагом в развитии трансграничного электронного взаимодействия.

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

Н.Г. Киевец, БГУИР,

А.И. Корзун, ЗАО «Центр новых интеллектуальных интегрированных систем», г. Минск

Электронная пластиковая карта (ЭПК) является наиболее защищенным средством личной идентификации, в котором содержится физический генератор случайных чисел (ГСЧ), необходимый для выработки ключевой информации. Эта информация может использоваться как для шифрования данных, так и для идентификации и электронной цифровой подписи.

Для оценки качества ГСЧ ЭПК разработан аппаратно-программный комплекс (АПК) (рисунок 1), который решает следующие задачи:

1. Формирование массивов данных, получаемых из ГСЧ ЭПК.
2. Статистическое тестирование данных на основе выбранных методик.

Структурная схема АПК для исследования ГСЧ ЭПК имеет вид, представленный на рисунке 1. АПК содержит карту, ридер, подключенный по USB 2.0, и персональный компьютер (ПК) с соответствующим программным обеспечением.

АПК работает следующим образом. После того, как карта вставлена в ридер, по запросу программы BCR MFC Application ридер взаимодействует с ЭПК по командам ISO 7816 [1] и пере-

дает данные в ПК. Для извлечения случайного числа из ЭПК в программу BCR встроена подпрограмма getRND.txt. В результате многократного обращения к ЭПК в BCR формируются данные, содержащие ключевую информацию.



Таблица 1 – Расчетные данные для последовательности длиной 1 000 192 бит

Номер серии, i	1	2	3	4	5	6	7	8
Серия	0000	0001	0010	0011	0100	0101	0110	0111
n_i	0,0624	0,0623	0,0626	0,0619	0,0638	0,0623	0,0628	0,0628
Номер серии, i	9	10	11	12	13	14	15	16
Серия	1000	1001	1010	1011	1100	1101	1110	1111
n_i	0,0631	0,0614	0,0620	0,0629	0,0632	0,0629	0,0620	0,0620
p	0,00625							
χ^2	22,0084							
P	0,1076							

Дальнейшая обработка данных зависит от средства, с помощью которого осуществляется тестирование. В качестве средства тестирования можно использовать пакеты статистического тестирования, например, DIEHARD, NIST, TestU01 и др. Недостатками этого подхода являются ограниченные наборы тестов без обоснования их достаточности, невозможность изменения ряда параметров тестирования и получения промежуточных результатов. Другой способ тестирования – тестирование с использованием одной из систем компьютерной математики. Это дает возможность пользоваться всеми возможностями, предоставляемыми системой.

В качестве средства вычислений была взята система MATLAB [2]. Для того, чтобы данные файла программы BCR можно было обработать в MATLAB, необходимо сделать предварительные преобразования. Данные файла программы BCR копируются в файл программы Microsoft Word. Далее в полученном документе с помощью функции замены удаляются все данные, кроме данных ключей генератора. В результате получается последовательность символов 0, 1, ..., 9, A, B, ..., F, которая переносится в MATLAB. Для большинства тестов требуется бинарное представление последовательности. Для вычислений в системе MATLAB составлен алгоритм, по которому каждый символ 0, 1, ..., 9, A, B, ..., F преобразуется в четырехразрядный двоичный код:

0 → 0 0 0 0;
 1 → 0 0 0 1;

 F → 1 1 1 1.

Полученная битовая последовательность может тестироваться в соответствии с разработанными алгоритмами, используемыми системой MATLAB. MATLAB позволяет осуществлять тестирование практически по любым известным тестам, задавать требуемые параметры тестирования и получать желаемые промежуточные данные. Система MATLAB позволяет представить результаты тестов различными способами – в числовом виде и графическом виде с использованием 2D- и 3D-графики.

В качестве примера использования АПК сделана проверка гипотезы о том, что непересекающиеся серии длиной 4 бита в последовательности ключей, полученной из ЭПК, распределены равномерно.

Для установления степени соответствия эмпирического закона распределения четырехбитных серий равномерному распределению применяется критерий «хи-квадрат», для чего вычисляется случайная величина [3]:

$$\chi^2 = \sum_{i=1}^{16} \frac{(n_i - p)^2}{p}, \quad (1)$$

где n_i – относительная частота появления i -го вида четырехбитной серии, p – вероятность появления четырехбитной серии. Учитывая, что возможно появление 16 различных четырехбитных серий, то вероятность появления каждой из них $p = 1/16 \approx 0,0625$.

Для принятия или опровержения гипотезы о законе распределения вычисляется вероятность χ^2 – вероятность того, что при принятой гипотезе случайная величина будет не менее значения, полученного по формуле (1) [3]:

$$P = \frac{\int_0^{\chi^2/2} t^{\frac{K}{2}-1} e^{-t} dt}{\int_0^{\infty} t^{\frac{K}{2}-1} e^{-t} dt}, \quad (2)$$

где K – число степеней свободы распределения. В данном случае $K = 15$.

Значение P сравнивается с уровнем значимости α , который выбирается исследователем. Для принятия гипотезы о законе распределения должно выполняться условие: $P > \alpha$.

С помощью АПК из ЭПК CNIIS-SC было получено 3907 32-битных ключей, из которых была сформирована битовая последовательность длиной 1000192 бит.

Для системы MATLAB был составлен алгоритм, по которому определяются относительные частоты появления непересекающихся четырехбитных серий n_i , величины χ^2 и P . Результаты, полученные для последовательности длиной 1000192 бит, представлены в таблице 1. С учетом полученного значения $P = 0,1076$ при уровне значимости $\alpha = 0,01$ принимаем гипотезу о том, что непересекающиеся четырехбитные серии последовательности длиной 1000192 бит, сформированной из ключей карты CNIIS-SC, распределены равномерно.

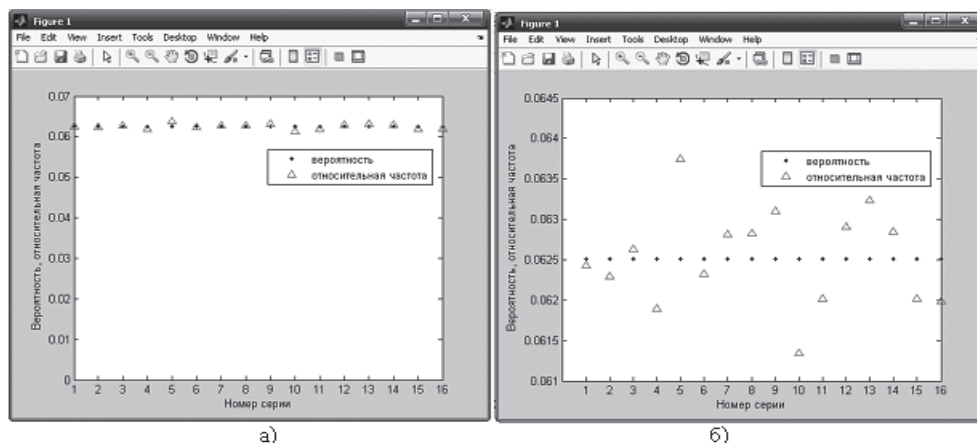


Рисунок 2 – Теоретический и эмпирический законы распределения непересекающихся четырехбитных серий последовательности длины 1000192 бит, сформированной из ключей карты CNIIS-SC

Для наглядности на рисунке 2 представлены диаграммы, полученные с использованием MATLAB. Рисунок 2а) позволяет увидеть соответствие распределения непересекающихся четырехбитных серий последовательности 1000192 бит равномерному распределению. Рисунок 2б) позволяет увидеть отклонения относительных частот появления серий, указанных в таблице 1, от теоретического значения.

Вывод

Создан АПК для исследования ГСЧ ЭПК. С помощью данного АПК исследовано распределение непересекающихся четырехбитных серий последовательности длины

1000192 бит, сформированной из ключей ЭПК.

Литература:

1. ISO/IEC 78116-3. Identification Cards – Integrated Cards – Integrated circuit(s) cards with contacts. Part 3. – Electronic signals and transmission protocols. – 1997.
2. Бондаренко В.Ф., Дубовец В.Д. MatLab. Основы работы и программирования, компьютерная математика. – Минск: Харвест, 2010. – 256 с.
3. Справочник по вероятностным расчетам / Г.Г. Абезгауз, А.П. Тронь, Ю.Н. Копенкин, И.А. Коровина. – М., Воениздат, 1970. – 536 с.

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ПО СОСУДИСТОМУ РУСЛУ РУКИ И АСПЕКТЫ ЕЕ ПРИМЕНЕНИЯ В СИСТЕМЕ ПАСПОРТНО-ВИЗОВЫХ ДОКУМЕНТОВ НОВОГО ПОКОЛЕНИЯ

Д.В. Грунтович,
ОКБ САПР, г. Москва

Постоянный рост объемов воздушных перевозок заставил государство задуматься над необходимостью рационализировать процедуры проверки пассажиров с применением технологий электронного обмена данными и использования централизованных баз данных. Кроме того, рост международной преступности и незаконной миграции потребовал выработки рекомендаций относительно методов и средств повышения уровня защищенности проездных документов от мошенничества или злоупотребления. Комплекс предпринимаемых мер был реализован в виде создания системы паспортно-визовых документов нового поколения (ПВДНП) [1], предоставляющей преимущества в части:

- повышения уровня защищенности от несанкционированного внесения изменений, подлога или подделки документов за счет изменения физических характеристик самих документов и повышения надежности элементов их защиты;
- упрощения для законного владельца документа процедур получения виз для поездок и прохождения через системы по-

граничного контроля и, как следствие, повышения пропускной способности систем пограничного контроля за счет сокращения очередей при прохождении контроля;

– сведения к минимуму потребности в бумажных документах (например, в пассажирских ведомостях и регистрационных карточках при прилете и вылете);

– сокращения административных расходов, связанных с выполнением соответствующих неавтоматизированных процедур.

Однако принципиальное повышение уровня защищенности от мошенничества было достигнуто за счет введения процедуры биометрической идентификации с использованием данных, хранящихся на бесконтактной интегральной схеме. Это объясняется тем, что биометрические характеристики человека крайне сложно похитить или подделать.

В настоящее время Международной организацией гражданской авиации (ИКАО) рекомендовано в качестве первичного механизма идентификации личности в проездных документах использование распознавания лица: анализ

геометрии лица, в отличие от большинства методов биометрической идентификации, не требует дорогостоящего оборудования. Немаловажную роль в выборе данного параметра в качестве основного сыграл психологический фактор: исторически сложилось так, что в процессе повседневного общения люди отличают друг друга по геометрическим особенностям лица, поэтому данная технология не доставляет существенных неудобств в психологическом плане.

Следует отметить, что этот метод характеризуется рядом существенных недостатков:

- низкая статистическая достоверность;
- существенные трудности для многих алгоритмов такого анализа представляют какие-либо внешние помехи (например, очки, борода, некоторые элементы прически);
- многие алгоритмы не учитывают возможные изменения мимики лица, то есть выражение должно быть нейтральным, а человек не всегда в силах владеть выражением своего лица;
- применение данного метода в полностью автоматических системах аутентификации, не требующих обязательного присутствия оператора, влечет за собой их низкую защищенность, которая связана также с простотой подделки биометрического шаблона (для этого часто достаточно использовать двумерную фотографию).

Помимо геометрии лица как основного параметра идентификации личности, в качестве дополнительных биометрических характеристик ИКАО определены к использованию радужная оболочка глаза и отпечатки пальцев. Использование последних получило наибольшее распространение в области электронных паспортов.

Анализ папиллярного рисунка на пальцах является наиболее зрелой технологией биометрической идентификации пользователей, использование которой обладает рядом преимуществ, включая распространенность технологии и разнообразие методик и алгоритмов. Однако существуют и факторы, значительно снижающие возможность интеграции технологии аутентификации по отпечаткам пальцев в систему ПВДНП:

- дактилоскопические системы вызывают у многих неприятие и снижение лояльности, поскольку исторически широко применяются в криминалистической практике;
- использование контактных датчиков отпечатков пальцев любого типа влечет за собой необходимость соблюдения санитарных норм и гигиены контактных площадок;
- эталонный образец пальца имеет достаточно большой размер (порядка 3 килобайт на один палец), а, в памяти ПВДНП необходимо хранить эталоны нескольких пальцев для одного пользователя.

Анализ рисунка радужной оболочки глаза и сетчатки глаза характеризуется высокой статистической надёжностью алгоритма, не требует физического контакта человека со считывающим устройством. Кроме того, радужная оболочка защищена от повреждений – а значит, не будет изменяться во времени. Однако данный метод также обладает рядом существенных недостатков:

- для получения биометрических образцов радужной оболочки глаза и сетчатки глаза требуется дорогостоящее оборудование;
- процедура получения изображения сетчатки глаза является болезненной, имеет медицинские ограничения и может вызвать ряд побочных эффектов (например, эпилептический приступ);

– психологический фактор: глаз человека – это важнейший орган чувств, поэтому многие люди считают процедуру сбора образцов опасной.

В настоящее время все большую популярность на рынке биометрических технологий приобретает анализ биометрических особенностей ладони человека, основанных на венозной системе, суть которого состоит в инфракрасном сканировании рисунка кровеносных сосудов ладони [2].

В технологии идентификации по сосудистому руслу руки используется сеть подкожных сосудов на тыльной стороне ладони для идентификации личности в биометрических приложениях. Принцип этой технологии основан на том, что структура кровеносных сосудов является уникальной для каждого человека, включая идентичных близнецов [3]. Таким образом, структура кровеносных сосудов руки является высокоэффективной отличительной особенностью, которая может использоваться для идентификации личности человека. Биометрическая технология применения сосудистого русла руки является относительно новой и находится в процессе непрерывного развития.

По сравнению с другими биометрическими параметрами, эта технология обладает рядом достоинств, таких как более высокая точность аутентификации и более удобное использование. Кроме того, поскольку сосудистая структура находится под кожей, она не зависит от неблагоприятного влияния окружающей среды. Благодаря этим функциям технология сосудистого русла внедряется в различные решения аутентификации для использования в общественных местах; большое количество решений было развернуто во многих приложениях, таких как контроль доступа, учет рабочего времени, безопасность и распознавание в медицинских учреждениях. Рынок использования технологии шаблонов сосудистого русла быстро развивается.

Процесс идентификации происходит следующим образом. Для получения шаблона сосудистого русла тыльной стороны ладони в системе используется инфракрасная (ИК) камера. Ближние ИК-лучи от камеры освещают тыльную сторону ладони. Раскисленный гемоглобин в кровеносных сосудах поглощает инфракрасные лучи, уровень отражения снижается, вследствие чего сосудистая структура ладони в распознающем устройстве приобретает вид черной схемы. Извлеченный рисунок сосудистого рисунка затем сравнивается с предварительно зарегистрированным шаблоном, хранящимся в базе данных, для проверки подлинности личности [4]. Данная технология обладает рядом неоспоримых преимуществ:

- высокая уникальность и стабильность биометрических образцов;
- относительно невысокая стоимость конечного решения;
- бесконтактность технологии – пользователи не касаются чувствительной поверхности, что выступает в пользу соблюдения гигиены и повышает приемлемость для пользователя;
- время сканирования составляет порядка секунды;
- изображение сосудистого русла руки трудно подделать, поскольку оно находится внутри руки и в некоторых подходах для регистрации изображения кровь должна течь;
- высокая точность, предоставляемая этими устройствами с завидным ложным принятием и ложным отказом.

Таким образом, в силу своих преимуществ перед другими биометрическими характеристиками, технологию идентификации по сосудистому руслу ладони вполне можно рассматривать в качестве перспективной для применения в системе ПВДНП.

Таблица 1 – Аспекты, связанные с применением технологии биометрической идентификации по сосудистому руслу руки

Аспект	Ожидания ИКАО	Степень соответствия технологии биометрической идентификации по сосудистому руслу руки ожиданиям ИКАО
Универсальность	Характеристика должна быть свойственна каждому человеку	Наличие сосудистого русла на тыльной стороне ладони свойственно каждому человеку
Уникальность (отличительность)	Любые два человека должны быть достаточно различимыми относительно данной характеристики	Доказано, что сосудистое русло уникально для каждого отдельно взятого индивидуума
Неизменность	Биометрическая характеристика должна быть инвариантной во времени	Сосудистое русло находится под кожным покровом и меньше подвержено влиянию окружающей среды с течением времени, чем многие другие биометрические характеристики
Измеримость	Должна быть возможность собирать и оцифровывать биометрическую характеристику с помощью соответствующих устройств, которые не причиняли бы существенных неудобств человеку. Кроме того, приобретенные исходные данные должны поддаваться обработке для извлечения отличительных особенностей	В настоящее время на рынке представлено множество устройств идентификации по сосудистому руслу руки. При этом сам процесс аутентификации является бесконтактным и безболезненным
Производительность	Достижимая точность и скорость распознавания, а также ресурсы, необходимые для их достижения, эксплуатационные и экологические факторы, влияющие на точность и скорость, должны соответствовать требованиям приложения	Технология идентификации по сосудистому руслу руки уже получила значительное внимание в биометрических сообществах, несмотря на то, что она является относительно новой. В последние годы проводится большое количество исследований по совершенствованию технологии и разработке новых устройств, позволяющих проводить идентификацию с высокой точностью и в течение относительно короткого промежутка времени
Приемлемость	Физические лица в целевой группе населения должны быть психологически готовы предоставить системе идентификации данные об указанной биометрической характеристике	Поскольку биометрические системы используют чувствительные характеристики для распознавания человека, социальные, культурные и правовые факторы являются критически важными и должны быть приняты во внимание в процессе проектирования, разработки и внедрения биометрических систем распознавания
Действия в обход системы защиты	Легкость, с которой биометрическая характеристика может быть воспроизведена с использованием мошеннических методов (например, поддельные пальцы или мимика), должна соответствовать требованиям безопасности приложения	Конечно, сложно представить, каким образом можно подделать инфракрасное изображение сосудистого русла, находящегося под кожным покровом руки человека, однако не стоит полагаться на «неизобретательность» современных мошенников, поэтому при разработке системы необходимо принять все меры по недопущению мошеннических действий в обход системы защиты в процессе биометрической идентификации

Однако прежде чем говорить о внедрении технологии идентификации по сосудистому руслу руки в систему ПВДНП, следует выяснить, удовлетворяет ли данная технология критериям, которыми руководствуются международные организации при выборе технологии идентификации в ПВДНП.

Сведения о составе аспектов [5], ожиданиях ИКАО как организации, которая организует разработку форматов, протоколов и процедур функционирования машиносчитываемых паспортов, виз и других официальных документов (именно в ее документах нашли отражение основные идеи обеспечения безопасности ПВДНП), и степени соответствия ожиданиям ИКАО технологии биометрической идентификации по сосудистому руслу ладони приведены в Таблице 1.

Таким образом, процесс оформления технологии в качестве рекомендованной ИКАО сопряжен со значительными организационными сложностями, отличается высокой инерцией, осложнен незначительным уровнем зрелости и принятия технологии обществом. Однако перспективы представляются благоприятными в виду неоспоримых технических преимуществ данной технологии.

Литература:

1. ICAO Doc 9303 Part 1, «Machine Readable Passports».
2. Счастный, Д.Ю. Расширение средств идентификации в СЗИ НСД / Д.Ю. Счастный // Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15–18 мая 2012 года, Суздаль (Россия). – 2012. – С. 231–232.
3. Coultas, L. Endothelial cells and VEGF in vascular development / L. Coultas, K. Chawengsaksophak, J. Rossant // Nature 1438. – 2005. – № 7070. – P. 937–945.
4. Alex Hwansoo Choi, Chung Nguyen Tran. Hand Vascular Pattern Technology // Department of Information Engineering, Myongji University, San 38-2 Namdong. Yongin, Kyunggido, Bangbae, Seocho, Seoul, Korea.
5. Jain, A.K. An introduction to biometric recognition / A.K. Jain, A. Ross, S. Prabhakar // IEEE Transactions on Circuits Syst. Video Techn 14(1) (2004) 4–20.
6. Pato, Josef N. Biometric recognition: challenges and opportunities / Josef N. Pato, Lynette I. Millet, editors; Whither Biometrics Committee; National Research Council. – 2010.

ТРЕБОВАНИЯ К НАУЧНЫМ СТАТЬЯМ, ПУБЛИКУЕМЫМ В РАЗДЕЛЕ «РЕЦЕНЗИРУЕМЫЕ СТАТЬИ»

1. Научная статья – законченное и логически цельное произведение по раскрываемой теме – должна соответствовать одному из следующих научных направлений: информационные технологии и системы, оптоэлектроника, микро- и нанoeлектроника, приборостроение.

2. Объем научной статьи не должен превышать 0,35 авторского листа (14 тысяч печатных знаков, включая пробелы между словами, знаки препинания, цифры и другие), что соответствует 8 страницам текста, напечатанного через 2 интервала между строками (5,5 страницы в случае печати через 1,5 интервала).

3. Статьи в редакцию представляются в двух экземплярах на бумаге формата А4 (220х15, г. Минск, пр. Пушкина, 29Б), а также в электронном виде (e-mail: sadov@bsu.by). К статье прилагаются сопроводительное письмо организации за подписью руководителя и акт экспертизы. Статья должна быть подписана всеми авторами.

Статьи принимаются в формате doc, rtf, pdf, набранные в текстовом редакторе word, включая символы латинского и греческого алфавитов вместе с индексами. Каждая иллюстрация (фотографии, рисунки, графики, таблицы и др.) должна быть представлена отдельным файлом и названа таким образом, чтобы была понятна последовательность ее размещения. Фотографии принимаются в форматах tif или jpg (300 dpi). Рисунки, графики, диаграммы принимаются в форматах tif, cdr, eps или jpg (300 dpi, текст в кривых). Таблицы принимаются в форматах doc, rtf или Excel.

4. Научные статьи должны включать следующие элементы: аннотацию; фамилию и инициалы автора (авторов) статьи, ее название; введение; основную часть, включающую графики и другой иллюстративный материал (при их наличии); заключение; список цитированных источников;

индекс УДК;

аннотацию на английском языке.

5. Название статьи должно отражать основную идею выполненного исследования, быть по возможности кратким, содержать ключевые слова, позволяющие индексировать данную статью.

6. Аннотация (100–150 слов) должна ясно излагать содержание статьи и быть пригодной для опубликования в аннотациях к журналам отдельно от статьи.

В разделе «Введение» должен быть дан краткий обзор литературы по данной проблеме, указаны не решенные ранее вопросы, сформулирована и обоснована цель работы.

Основная часть статьи должна содержать описание методики, аппаратуры, объектов исследования и подробно освещать содержание исследований. Полученные результаты должны быть обсуждены с точки зрения их научной новизны и сопоставлены с соответствующими известными данными. Основная часть статьи может делиться на подразделы (с разяснительными заголовками).

Иллюстрации, формулы, уравнения и сноски, встречающиеся в статье, должны быть пронумерованы в соответствии с порядком цитирования в тексте.

В разделе «Заключение» должны быть в сжатом виде сформулированы основные полученные результаты с указанием их новизны, преимуществ и возможностей применения.

Список цитированных источников располагается в конце текста, ссылки нумеруются согласно порядку цитирования в тексте. Порядковые номера ссылок должны быть написаны внутри квадратных скобок (например: [1], [2]).

В соответствии с рекомендациями ВАК Республики Беларусь от 29.12.2007г. №29/13/15 научные статьи аспирантов последнего года обучения публикуются вне очереди при условии их полного соответствия требованиям, предъявляемым к рецензируемым научным публикациям.

ИДЕНТИФИКАЦИЯ УГРОЗ ПРИМЕНЕНИЯ ЗАКЛАДНЫХ УСТРОЙСТВ В ТЕХНИЧЕСКИХ СРЕДСТВАХ ОБРАБОТКИ ИНФОРМАЦИИ

УДК 002:004.056

О.К. Барановский,

Государственное предприятие «НИИ ТЗИ», г. Минск

Аннотация

Идентификация и корректный учет факторов угроз информационной безопасности систем обработки информации определяет эффективность процедур управления рисками организации. Одним из недостаточно проработанных вопросов является идентификация угроз применения недеklarированных возможностей технических средств обработки информации. Предложена система классификационных признаков, позволяющая формировать классы и семейства угроз, связанных с внедрением устройств и аппаратных недеklarированных функций, в целях принятия групповых мер защиты на объекте информатизации. Приведен пример выработки классов и семейств угроз для конкретного объекта.

Введение

Инновационные информационные технологии являются неотъемлемым атрибутом своевременного и эффективного решения задач во всех сферах деятельности государства и общества. Вместе с тем, использование технических средств и автоматизированных систем импортного производства для обработки конфиденциальной и критической информации делает эти процессы потенциально уязвимыми по отношению к внешним агрессивным информационным воздействиям, внутренним сбоям и отказам, обусловленным явлениями антропогенного и природного характера.

Безопасность эксплуатации объектов информатизации (ОИ) определяется своевременным выявлением угроз и оценкой рисков их реализации. Одна из установленных практик управления информационной безопасностью зафиксирована в международном стандарте ISO/IEC 27001:2005, идентичный отечественный аналог которому введен в действие в Республике Беларусь [1].

В рамках указанного подхода идентификация рисков проводится на основании учета следующих факторов:

- активы;
- угрозы (неразрешенные воздействия), направленные на активы;
- уязвимости активов, которые могут возникнуть при наличии угроз;
- характеристики активов, подлежащие защите от угроз.

Например, в критериях оценки безопасности информационных технологий [2] угроза формулируется в понятиях: «источник угрозы» (например, субъект или группа, информационный процесс) с описанием его возможностей, применяемый «метод атаки» (вредное, деструктивное действие) на актив, подвергаемые угрозе «характеристики актива».

Другой способ описания угроз приведен в [3], в рамках которого, например, угроза несанкционированного доступа к активам есть: «источник угрозы», «уязвимость программ-

ного или аппаратного обеспечения», «способ реализации угрозы», «объект воздействия», «деструктивное действие».

Анализ источников информации показывает, что для каждого типа источников угроз можно определить необходимый и достаточный набор классификационных признаков.

Определение объекта

Отличительной особенностью технических средств и автоматизированных систем обработки информации импортного производства является наличие в них недеklarированных (неизвестных) возможностей.

Для идентификации источника угроз выделим два понятия: закладное устройство (ЗУ) и недеklarированные функции (НФ).

Под ЗУ будем понимать электронное устройство, несанкционированно и скрытно устанавливаемое или подключаемое к техническому средству обработки информации (ТСОИ) (включая штатные соединительные кабели и периферийные устройства, входящие в его состав) и предназначенное для несанкционированного доступа и/или воздействия на активы ТСОИ и/или ОИ.

К НФ будем относить специально вносимые недокументированные возможности ТСОИ, которые могут быть использованы для несанкционированного доступа и/или воздействия на активы ТСОИ и/или ОИ.

Разработка классификации

Выявление и учет угроз применения ЗУ и НФ в ТСОИ является неотъемлемой частью процессов планирования и проведения мероприятий, направленных на создание ТСОИ и/или ОИ с требуемым уровнем защищенности в рамках выделенного бюджета.

Перечень и содержание потенциальных угроз применения ЗУ и НФ в ТСОИ определяется системой условий и факторов, создающих опасность несанкционированного доступа и воздействия на активы ТСОИ.

В свою очередь, выявление системы условий и факторов, создающих опасность несанкционированного доступа и/или воздействия на активы, проводится с учетом характеристик ТСОИ (при необходимости характеристик ОИ), характеристик и/или функций защищаемых активов, обстоятельств реализации угроз.

Эффективность выявления обобщенного перечня угроз применения ЗУ и НФ в ТСОИ определяется следующими принципами:

- достаточностью классификации, позволяющей формировать полное множество угроз;
- гибкостью классификации, позволяющей расширять множества угроз, а также вносить необходимые изменения без нарушения структуры классификации.

При определении классификационных признаков угроз безопасности целесообразно их разделить на:

– классификационные признаки угроз применения ЗУ и НФ без учета характеристик ЗУ и НФ, которые описывают активы, характеристики активов, типы вредных воздействий на характеристики активов, условия и обстоятельства реализации угроз;

– классификационные признаки ЗУ и НФ, которые описывают их физические характеристики, место установки, способ управления и передачи информации и т.п.

В данной работе рассматриваются классификационные признаки угроз применения ЗУ и НФ.

При классификации угроз выделяют основные и вспомогательные признаки.

Основные признаки предназначены для классификации угроз применения ЗУ и НФ в ТСОИ по целевому признаку.

Вспомогательные признаки предназначены для описания механизмов реализации угроз применения ЗУ в ТСОИ посредством выявления и использования характеристик и уязвимостей защищаемого объекта.

Основными классификационными признаками угроз применения ЗУ и НФ в ТСОИ являются:

– тип актива ТСОИ, на который направлена угроза безопасности;

– характеристика актива, на нарушение безопасности которой направлена угроза.

В качестве вспомогательных классификационных признаков целесообразно выделить признаки, описывающие такие условия и факторы, как:

– наличие субъекта (злоумышленника или информационного процесса), являющегося источником события реализации угрозы;

– вид мер защиты, уязвимости которых использует ЗУ или НФ;

– масштаб реализации угрозы (направленность угрозы на ТСОИ, в котором установлены ЗУ и НФ, либо на другие элементы ОИ, в состав которого входит ТСОИ с внедренными ЗУ и НФ);

– этап жизненного цикла ТСОИ, на котором происходит внедрение ЗУ и НФ в ТСОИ;

– этап жизненного цикла ТСОИ, на котором осуществляется реализация угрозы применения ЗУ и НФ.

Угрозы применения ЗУ и НФ в ТСОИ подразделяются на подклассы с учетом значений классификационных признаков.

По типу актива ТСОИ:

– угрозы безопасности информации (обрабатываемой, технологической, механизмов защиты);

– угрозы безопасности ресурсов (программных, технических, аппаратно-программных).

По типу характеристики актива ТСОИ:

– угрозы, направленные на нарушение свойств (конфиденциальности, целостности и доступности информации, целостности ресурсов);

– угрозы, направленные на изменение выполняемых функций;

– угрозы, направленные на нарушение производительности (программных, технических, аппаратно-программных ресурсов) или доступности (сбой и отказ технических, аппаратно-программных ресурсов).

По наличию субъекта:

– угрозы, реализуемые посредством воздействия от

субъекта (сигналом управления из-за пределов ТСОИ, путем непосредственного физического доступа к ТСОИ);

– угрозы, реализуемые без вмешательства субъекта (изменение логического состояния или режима работы ТСОИ при обработке информации, изменение физических параметров ТСОИ, изменение параметров внешней среды).

По виду мер защиты, уязвимости которых использует ЗУ или НФ:

– угрозы, использующие уязвимости правовых мер защиты;

– угрозы, использующие уязвимости организационных мер защиты (несанкционированный доступ на ОИ лиц либо несанкционированный пронос технических средств на ОИ, несоблюдение политик безопасной эксплуатации ОИ);

– угрозы, использующие уязвимости технических мер защиты (использование уязвимостей в настройке технических средств защиты или их отсутствие, использование нетрадиционных каналов связи).

По направлению воздействия (масштабу реализации):

– угрозы, направленные на нарушение характеристик активов ТСОИ;

– угрозы, направленные на нарушение характеристик активов, принадлежащих другим ТСОИ.

По этапу жизненного цикла ТСОИ или ОИ, на котором осуществляется внедрение ЗУ или НФ:

– угрозы, возникающие в результате внедрения ЗУ или НФ на этапе разработки и создания ТСОИ (внесение в конструкторскую документацию или при технологическом процессе производства ТСОИ);

– угрозы, возникающие в результате внедрения ЗУ или НФ на этапе поставки и установки ТСОИ (при транспортировке, установке или настройке ТСОИ);

– угрозы, возникающие в результате внедрения ЗУ или НФ на этапе эксплуатации и сопровождения ТСОИ (в том числе при обслуживании или модернизации ТСОИ).

По этапу жизненного цикла ТСОИ или ОИ, на котором осуществляется реализация угроз:

– угрозы, реализуемые на этапе создания ТСОИ;

– угрозы, реализуемые на этапе поставки и установки ТСОИ;

– угрозы, реализуемые на этапе эксплуатации и сопровождения ТСОИ;

– угрозы, реализуемые на этапе вывода из эксплуатации ТСОИ.

Сформированные на основе основных признаков подклассы угроз используют для составления классов угроз применения ЗУ и НФ в ТСОИ.

Сформированные на основе вспомогательных признаков подклассы угроз используют для составления семейств угроз применения ЗУ и НФ в ТСОИ. Каждому классу угроз соответствует набор семейств угроз, сформированный с учетом вспомогательных признаков.

Пример формирования классов и семейств угроз

В качестве ТСОИ выберем цифровое копирующее средство. На ТСОИ предполагается обрабатывать информацию, отнесенную к категории «служебная информация ограниченного распространения».

ТСОИ предполагается эксплуатировать как отдельно стоящее, не подключенное к другим ТСОИ.

В соответствии с категорией ОИ, на котором предполагается эксплуатировать ТСОИ, защищаемым активом является: обрабатываемая информация.

Сделаем допущение, что риски нарушения свойств технологической информации и информации механизмов защиты, функций программных и аппаратных средств приемлемы в связи с возможностью оперативной замены ТСОИ. Поэтому указанные типы активов не являются критичными для выполнения ОИ своих функций.

Теми же соображениями будем руководствоваться при установлении типа характеристик активов, на которые направлены угрозы: конфиденциальность.

Обеспечение доступности информации реализуется путем замены ТСОИ, а ее целостности – визуальным сравнением исходного документа и его копии.

Относительно источника происхождения и условий поставки известно следующее. Производитель копировально-множительного средства является разработчиком используемых в нем технических решений. Модель цифрового копировально-множительного средства является широко продаваемым продуктом, имеет соответствующие заключения (сертификаты) по требованиям безопасности информации в других странах. ТСОИ предполагается установить и эксплуатировать с привлечением штатных, прошедших соответствующую проверку, сотрудников, в случае его выхода из строя ремонт будет производиться доверенными подрядчиками, имеющими соответствующие разрешения (лицензии). Поставка осуществляется фирмой, имеющей соответствующие разрешения (лицензии), однако, закупка происходит не у компании-производителя, а у посредника, находящегося за рубежом. В этом случае актуальны угрозы внедрения ЗУ в процессе поставки.

Формируем класс угроз:

– «Угрозы нарушения конфиденциальности обрабатываемой информации ТСОИ».

Классу «Угрозы нарушения конфиденциальности обрабатываемой информации ТСОИ» соответствует семейство «Угрозы нарушения конфиденциальности обрабатываемой информации, реализуемые как посредством воздействия от субъекта, так и без его вмешательства, в результате внедрения ЗУ на этапе поставки, использующие уязвимости правовых, организационных или технических мер защиты, реализуемые на этапах эксплуатации и сопровождения или вывода из эксплуатации ТСОИ».

Для конкретизации угроз используют параметры модели ЗУ, соответствующие заданному классу ОИ, уточняют имеющиеся уязвимости мер защиты.

К мерам защиты (включающим правовые, организационные, технические и криптографические) от угроз применения ЗУ и НФ относят:

- 1) предупреждение внедрения ЗУ и НФ в ТСОИ;
- 2) обнаружение ЗУ и НФ в ТСОИ;
- 3) противодействие реализации угроз ЗУ и НФ.

Заключение

Предложена система классификационных признаков, позволяющая сформировать классы и семейства угроз, определяемые защищаемыми активами и факторами жизненного цикла ТСОИ.

Конкретизация угроз осуществляется с учетом модели ЗУ и НФ для заданного класса ОИ, принятых мер защиты.

По результатам исследований подготовлен проект технического нормативного правового акта, который планируется ввести в качестве государственного стандарта Республики Беларусь СТБ «Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. Классификация угроз применения закладных устройств».

Литература:

1. Информационные технологии. Методы обеспечения информационной безопасности. Системы менеджмента информационной безопасности. Требования: СТБ ISO/IEC 27001–2011. – Введ. 01.01.2012. – Минск: Белорус. гос. ин-т стандартизации и сертификации, 2011. – 36 с.

2. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model: ISO/IEC 15408-1:2009. – 15.12.2009. – International Organization for Standardization, 2009. – 72 p.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Федеральная служба по техническому и экспортному контролю. – М., 2008. – 74 с.

Abstract

Identification and correct accounting of information security threat factors for information processing systems determines the efficiency of risk management procedures for an organization. Undeclared features of information processing hardware means are not clear topic. The described classification attributes system is assigned for threat classes and sets development in case of undeclared hardware means and function presence for further group protective action planning and realization. As a example, threat classes and sets for the object is introduced.

Поступила в редакцию 18.05.2013 г.

ПТСС ЗАО «Промтехсервисснаб»

г. Минск, ул. Богдановича, 120 Б, ком. 6,
e-mail: uslugi@zapservis.by,
www.zapservis.by

Тел.: 266-23-94; 266-23-92,
моб.: (029) 676-02-56,
моб.: (044) 773-72-04,
факс: 266-23-94.

Контрактное производство РЭА:

- ✓ Автоматизированный монтаж SMD-компонентов любой сложности.
- ✓ Комбинированный монтаж с использованием компонентов DIP (выводных), а также SMD (планарных).
- ✓ Сборка корпусных деталей и узлов.
- ✓ Ультразвуковая отмывка печатных плат и узлов высококачественными импортными растворами.
- ✓ Нанесение влагозащитных покрытий.

**Высокотехническое импортное оборудование обеспечивает высокое качество производимой продукции.*

Продажа неликвидов ПК для РЭА:

- ✓ Резисторы, конденсаторы, транзисторы, микросхемы и т.д.

КОМПЛЕКСНЫЙ ПОДХОД К ВЫЯВЛЕНИЮ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ТЕХНИЧЕСКИХ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ

УДК 002:004.056

О.К. Барановский,

Государственное предприятие «НИИ ТЗИ», г. Минск

Аннотация

Применение продуктов и систем информационных технологий, не прошедших процедуры подтверждения соответствия требованиям защиты информации, несет угрозы безопасности обрабатываемой информации и штатному режиму функционирования объектов информатизации. Предложен комплексный подход к обнаружению и локализации недеklarированных возможностей средств обработки информации. В рамках предложенного подхода контрольные проверки подразделяются на три группы объектов исследования: генерируемые физические поля, технические и аппаратно-программные ресурсы, внешние проводные линии средств обработки информации. Каждая контрольная проверка реализуется путем выбора методов измерений и анализа с учетом применяемых в средстве обработки информации технологий.

Введение

Применение доверенных продуктов и систем обработки информации позволяет минимизировать количество и последствия инцидентов информационной безопасности. Объекты информационных технологий, прошедшие процедуры подтверждения соответствия требованиям защиты информации, более устойчивы к угрозам информационной безопасности. Одним из источников угроз являются недеklarированные возможности технических, программных и аппаратно-программных средств обработки информации (СОИ). Среди практических методов поиска недеklarированных возможностей СОИ традиционно выделяют два направления:

- 1) методы поиска в программных средствах [1–3];
- 2) методы поиска в технических и аппаратно-программных средствах [4–6].

Ранее описанные в литературе методы предназначены для поиска узкого класса недеklarированных возможностей. В связи с этим необходим комплексный подход для исследования недоверенных СОИ в условиях крайне ограниченного объема априорной информации.

Постановка задачи

Данная работа посвящена вопросам поиска двух классов недеklarированных возможностей в технических и аппаратно-программных средствах обработки информации: «закладное устройство» (ЗУ) и «недеklarированные функции» (НФ).

Под ЗУ будем понимать электронное устройство, несанкционированно и скрытно устанавливаемое или подключаемое к СОИ (включая штатные соединительные кабели и периферийные устройства, входящие в его состав) и предназначенное для несанкционированного доступа и/или воздействия на активы СОИ.

К НФ будем относить специально вносимые дополнения или изменения в технические или аппаратно-программные ресурсы СОИ, которые могут быть использованы для организации несанкционированного доступа и/или воздействия на активы СОИ. К НФ относят также закладные схемы – составные элементы интегральных микросхем, несанкционированно и скрытно изменяемые и/или внедряемые, и предназначенные для несанкционированного доступа и/или воздействия на активы интегральной схемы и/или СОИ.

Поиск ЗУ и НФ реализуется путем выполнения набора контрольных проверок, которые определяются следующими факторами:

- типом (функциональным назначением) ЗУ или НФ и способом реализации вредоносного действия;
- применяемыми в ЗУ или НФ технологиями.

Полнота априорной информации, комбинация значений перечисленных факторов позволяют выбрать набор контрольных проверок в целях максимально эффективного выявления ЗУ и НФ по их демаскирующим признакам.

Исходя из опыта, трудоемкость и строгость выполнения контрольных проверок определяются важностью информации:

- степенью конфиденциальности обрабатываемой информации;
- параметрами целостности и доступности обрабатываемой информации, определяемых степенью критической важности объекта информатизации (ОИ), на котором планируется эксплуатировать СОИ.

Основная часть

С учетом применяемых в СОИ технологий проверки подразделяются:

- 1) контроль физических полей, генерируемых СОИ;
- 2) контроль технических и аппаратно-программных ресурсов (структуры и характеристик составных элементов);
- 3) контроль проводных линий.

В зависимости от важности обрабатываемой информации (соответственно, в среднем затрачиваемому владельцем бюджету на реализацию мер защиты информации) злоумышленник, например, для организации канала утечки информации может применить как широко используемые средства беспроводной связи wi-fi, Bluetooth, 3G, так и установить почти не описанные в открытых источниках «температурные» каналы передачи данных [7]. В связи с этим, до проведения контрольных проверок необходима оценка рисков угроз применения различных типов полей для создания каналов передачи информации.

Назначением отдельных типов ЗУ и НФ является вывод СОИ из штатного режима функционирования по

некоторому событию. В этом случае для определенных категорий объектов информатизации необходимо проводить контрольные проверки по выявлению ЗУ и НФ на основе исследования их физических характеристик (например, наличия нежелательных типовых элементов или незажеланных изменений) и циркулирующих в них сигналов.

Для распределенных СОИ и систем на их основе актуальным является контроль проводных линий, особенно проходящих в местах, не находящихся под постоянным наблюдением. В рамках выполнения контрольных проверок проводится анализ физических параметров проводных линий, специальная проверка, исследование передаваемых сигналов.

Для реализации контрольных проверок выбираются методы измерения физических величин и обработки данных измерений, в соответствии с параметрами модели ЗУ или НФ.

Для выявления и локализации ЗУ и НФ применяют следующие группы методов:

Группа 1. Методы мониторинга.

- 1.1. Амплитудный метод.
- 1.2. Метод пространственной корреляции.
- 1.3. Метод разности панорам.
- 1.4. Методы узкополосной фильтрации.
- 1.5. Методы вейвлет-анализа.
- 1.6. Методы слепой обработки.

Группа 2. Методы локации.

- 2.1. Метод параметрической локации.
- 2.2. Метод нелинейной локации.
- 2.3. Методы рефлектометрии.

Группа 3. Методы пеленгации.

- 3.1. Корреляционно-интерферометрический метод.
- 3.2. Квазидоплеровский метод.
- 3.3. Метод триангуляции.

Группа 4. Методы анализа структуры.

- 4.1. Метод визуального осмотра.
 - 4.2. Метод рентгеноструктурного анализа.
 - 4.3. Метод спектральной пирометрии.
 - 4.4. Метод ИК-Фурье микроскопии.
 - 4.5. Метод лоренцевой электронной спектроскопии.
- Группа 5. Методы анализа физических параметров.
- 5.1. Методы анализа электрофизических параметров.
 - 5.2. Методы анализа оптических параметров.

Группа 6. Методы тестирования.

- 6.1. Методы нагрузочного тестирования.
 - 6.2. Методы стресс тестирования.
 - 6.3. Методы тестирования качества работы.
 - 6.4. Методы несанкционированного доступа (взлома).
- Группа 7. Методы анализа информационных потоков.

Группа 1, как правило, применяется для поиска источников радиоизлучения.

Группа 2 широко используется для определения местоположения объектов поиска на основе анализа отклика на зондирующее воздействие.

Группу 3 применяют для определения направления на источник, например, электромагнитного, оптического, звукового полей.

Группа 4 предназначена для восстановления структуры (обратное проектирование) исследуемого объекта.

Группа 5 позволяет на основе измерения параметров электрических и оптических проводных линий опреде-

лить наличие в них несанкционированных объектов или изменений.

Группа 6 предназначена для проверки исследуемого объекта на способность выполнять заложенные функции при различных условиях эксплуатации.

Группа 7 является инструментом анализа информационных потоков СОИ на предмет наличия в них скрытых каналов передачи сигналов управления и потоков данных.

Выбор и реализация каждой контрольной проверки зависит от модели проверяемого (тестируемого) СОИ:

1) объект с известной структурой (может содержать инструменты выявления несанкционированных изменений);

2) объект типа «черный ящик».

Например, при проектировании СОИ могут использоваться технологии, затрудняющие внесение ЗУ и НФ, а также внедряться инструменты проверки целостности конечного объекта. В этом случае перечень контрольных проверок (тестов) задается разработчиком.

Для СОИ, соответствующих объекту типа «черный ящик», перечень проверок будет определяться обобщенной моделью ЗУ или НФ.

Заключение

Предложен комплексный подход к обнаружению и локализации технических и аппаратно-программных недекларированных возможностей СОИ.

По результатам исследований подготовлен проект технического нормативного правового акта, который планируется ввести в качестве государственного стандарта Республики Беларусь СТБ «Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. Классификация по уровню контроля отсутствия закладных устройств».

Литература:

1. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: утв. Приказом председателя Госстанкомиссии России 4.06.1999 года № 114. – М.: ГТК РФ, 1999.

2. Система контроля отсутствия недекларированных возможностей в программном обеспечении : пат. 2434272 Российская Федерация, МПК7: G06F17/00 / В.А. Минаков, В.В. Мирошников, В.В. Котрахов; заявитель ФГУ «ГНИИИ ПТЗИ ФСТЭК России». – заявл. 04.06.2010. – Режим доступа: <http://www.findpatent.ru/patent/243/2434272.html>. – Дата доступа: 08.05.2013.

3. Леошкевич, И.О. Система выявления недекларированных возможностей программного обеспечения, влекущих нарушение конфиденциальности информации автореф. дис. ... канд. техн. наук: 05.13.19 / И.О. Леошкевич; Нац. иссл. ядерн. ун-т «МИФИ» – М., 2011. – 21 с.

4. Технические средства и методы защиты информации / А.П. Зайцев [и др.]; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Машиностроение, 2009. – 508 с.

5. Бузов, Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного доступа к информации.

рованного получения информации / Г.А. Бузов. – М.: Горячая линия – Телеком, 2010. – 240 с.

6. Beaumont, M. Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review) / M. Beaumont, B. Hopkins, T. Newby // Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation [Electronic resource]. – Edinburgh, 2011. – Mode of access: <http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10148/1/DSTO-TN-1012%20PR.pdf>. – Date of access: 12.07.2012.

7. Sebastian, Z. Estimating the Capacity of Temperature-based Covert Channels / S. Zander, P. Branch, G. Armitage // Technical Report 091218A / Centre for Advanced Internet Architectures. – Melbourne, 2009. – 9 p.

Abstract

There are threats for information processed and normal mode of computer system operation if information technology products and systems are used without certification procedures for compliance with the information security requirements. Integrated approach for undeclared features detection and localization in data processing means is proposed. Verification checkouts are divided into three groups according to subject of inquiry: physical fields generated, hardware assets, external wired lines of data processing means. Every verification checkout is carried out by using measurement and analysis methods whereas information technology used in data processing mean.

Поступила в редакцию 18.05.2013 г.

ПОРЯДОК СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ РАЗЛИЧНОГО НАЗНАЧЕНИЯ

УДК 002:004.056

Г.Д. Томина,

Государственное предприятие «НИИ ТЗИ», г. Минск

Аннотация

Статья содержит сведения о правовых основах создания системы защиты информации (СЗИ) информационных систем (ИС) различного назначения, о проблеме классификации ИС как типового объекта информатизации и предоставляет методические рекомендации по порядку создания и проведения аттестации СЗИ ИС владельцем ИС.

Введение

Создание и применение аттестованных систем защиты информации (далее – СЗИ) в государственных информационных системах (далее – ИС), а также ИС, содержащих информацию, распространение и (или) предоставление которой ограничено (за исключением государственных секретов), определяется [1–4]. В Республике Беларусь СЗИ разрабатываются в соответствии с положениями национальной группы стандартов серии «Общие критерии» (далее – ОК): СТБ 34.101.1 – 3-2004 (ИСО/МЭК 15408-1 – 3:1999).

В настоящее время проводятся мероприятия по принятию новой версии ОК, планируемой к введению в 2013 году, которая установит требования к содержанию и оценке требований безопасности только для продуктов информационных технологий (далее – ИТ). Для ИС требования безопасности будут изложены в СТБ ISO/IEC TR 19791-2014, который учитывает создание СЗИ на базе средств защиты продуктов ИТ и дополняет требования новой версии ОК. Однако методические рекомендации по порядку создания СЗИ в [2–4] не изложены.

Классификация ИС различного назначения

Порядок определения класса ИС согласно действующим техническим нормативным правовым актам (далее – ТНПА) устанавливается в зависимости от области применения ИС:

– для государственных ИС, а также ИС, содержащих информацию, распространение и (или) предоставление которой ограничено (далее – регулируемые ИС), – в соот-

ветствии с СТБ 34.101.30-2007 по отнесению ИС к классу типового объекта информатизации (далее – ОИ);

– для критически важных ОИ – в соответствии с СТБ П 34.101.52-2012.

При классификации типовых ОИ по СТБ 34.101.30-2007 у владельца ИС часто возникают сложности при отнесении ИС к классу Б2, А2, поскольку в СТБ 34.101.30-2007 для подкласса 2 вместо информации ограниченного распространения (за исключением государственных секретов) указана служебная информация ограниченного распространения.

Ст. 17 [1] определяет, какая информации относится к информации ограниченного распространения (в том числе, персональные данные, коммерческая тайна и т. д.). Порядок создания и аттестации СЗИ для государственных ИС, а также ИС, содержащих информацию, распространение и (или) предоставление которой ограничено (за исключением государственных секретов), определяется в [2], устанавливающим классификацию по СТБ 34.101.30 2007. Поэтому необходимо при определении подкласса 2 обрабатываемой информации делать поправку для слово «служебная», чтобы соответствовать ст. 17 [1].

В связи с введением в действие в октябре 2013 года Положения [4], выделившего в информации, распространение и (или) предоставление которой ограничено (за исключением государственных секретов), отдельными категориями служебную информацию ограниченного распространения, информацию о частной жизни физического лица и персональные данные, необходимо откорректировать классификацию в СТБ 34.101.30-2007 для разъяснения, к каким подклассам относится остальная информация ограниченного распространения в соответствии со ст. 17 [1].

Описание порядка действий по созданию СЗИ ИС различного назначения

При создании СЗИ ИС в организации должен быть определен комплекс организационных, технических

и криптографических мер, включающий совокупность подразделений по технической защите информации и (или) уполномоченных лиц, используемой ими техники защиты информации и объектов защиты, функционирующих по правилам, которые установлены ТНПА и НПА в области защиты информации.

Для достижения целей создания СЗИ ИС или модернизации существующей СЗИ необходимо выполнить следующие действия в рекомендуемом порядке.

1. Определите перечень хранящихся и обрабатываемых в ИС сведений и разделите их по категории доступа в соответствии с пп. 15 – 17 [1], руководствуясь СТБ 34.101.30-2007 или СТБ П 34.101.52-2012.

Сформируйте и утвердите перечень информации, распространение и (или) предоставление которой ограничено (при необходимости), обрабатываемой в ИС.

2. Проведите анализ создаваемой или модернизируемой ИС в соответствии с п. 10 [5], п. 18 [6]. Убедитесь в наличии и ознакомьтесь с основными характеристиками технических (вспомогательных) средств защиты ИС (помещений, где обрабатывается защищаемая информация и хранятся машинные носители информации).

3. Присвойте ИС класс типового ОИ в соответствии с п. 10 [5] и оформите Акт по отнесению ИС к классу типовых ОИ.

4. Проведите анализ организационно-методического обеспечения ИС: порядка организации технологических процессов обработки защищаемой информации; условий функционирования ИС и обеспечения бесперебойной работы; существующей организационной структуры управления ИС.

5. Примите решение о разработке или корректировке СЗИ ИС и организационно-распорядительных документов (далее – ОРД) системы управления защитой ИС. Определите необходимость в технической и (или) криптографической защите информации.

6. Разработайте или откорректируйте задание по безопасности (далее – ЗБ) на ИС в соответствии с требованиями ТНПА в области защиты информации и проведите оценку ЗБ с учетом следующих аспектов:

а) при определении угроз безопасности активам ИС для выявленных источников угроз опишите модель нарушителя с учетом возможного негативного воздействия атак на активы, уязвимости активов и изложите в ОРД «Модель нарушителя правил разграничения доступа» в соответствии с п. 5 Приложения 2 к [6]. Используйте краткое описание модели нарушителя для изложения в ЗБ;

б) определите риски безопасности по СТБ ISO/IEC 27005-2012, изложите политики безопасности организации по использованию и управлению функциями защиты активов ИС для снижения рисков безопасности;

в) определенные задачи безопасности, функциональные и гарантийные требования безопасности распределите между техническими, криптографическими и организационными мерами безопасности;

г) представьте краткую спецификацию описания функций безопасности, услуг, интерфейсов, организационных и гарантийных мер безопасности;

д) опишите информацию по каждому домену безопасности ИС с учетом перечислений а) – г) и СТБ П 34.101.59-2012;

е) проведите оценку ЗБ в специализированной организации.

7. Для вновь разрабатываемых СЗИ определите, а для модернизируемой СЗИ уточните организационную структуру СЗИ, обоснуйте состав и структуру комплекса технических и программных средств СЗИ с учетом требований ЗБ и изложите их в пояснительной записке к техническому проекту по ГОСТ 34.201-89. Убедитесь, что выбранные вами средства защиты имеют сертификат соответствия согласно [2, 3].

8. Изложите подход организации к управлению информационной безопасностью, руководствуясь п. 5 СТБ ISO/IEC 27002-2012, и укажите организационную структуру в документе «Политика информационной безопасности» в соответствии с п. 10 [5].

9. Опишите организационную структуру, организационные меры при организации процесса обеспечения защиты с учетом инцидентов безопасности и ликвидации их последствий, и изложите их в ОРД «Инструкция по обеспечению защиты информации в информационной системе» в соответствии с п. 17 Приложения 2 к [6].

10. Изложите правила разграничения доступа и методики безопасности для каждого домена безопасности ИС с учетом требований ЗБ в ОРД «Правила разграничения доступа в информационной системе» в соответствии с п. 4 Приложения 2 к [6].

11. Изложите в ОРД организационные меры, определяющие в соответствии с п. 11 [5]: контроль целостности защищаемых сведений; порядок доступа к ресурсам ИС; установление подлинности субъектов; резервирование и уничтожение информации; защиту от вредоносных программ и вторжений; аудит безопасности в ИС с учетом СТБ ISO/IEC 27006-2013.

12. Разработайте комплект рабочей документации на СЗИ согласно ГОСТ 34.201-89 (минимально необходимый состав: спецификация; общее описание СЗИ; руководства пользователей по подсистемам СЗИ; программа и методика испытаний СЗИ).

13. Реализуйте настройки средств защиты СЗИ в соответствии с требованиями ЗБ и комплекта руководств пользователей на СЗИ.

14. Одновременно после принятия решения по пункту 7 определите необходимые изменения в организационной структуре управления ИС в части обеспечения защиты информации и выпустите документ «Описание организационной структуры» в соответствии с ГОСТ 34.201-89.

15. Опишите организационные меры по составу, назначению и функциям подсистем СЗИ, вопросам эксплуатации, технического обслуживания, ремонта и хранения средств защиты в ОРД «Инструкция о порядке применения средств защиты информации в информационной системе» в соответствии с п. 17 Приложения 2 к [6].

16. Утвердите Политику информационной безопасности и комплект ОРД на СЗИ (утверждает руководитель организации-владельца ИС).

17. Определите обязанности персонала, ответственного за эксплуатацию и надежное функционирование ИС и СЗИ, отразите их в должностных инструкциях.

18. Определите в составе ИС набор типовых объектов ИС; для выделенных наборов оформите карточки учета для контроля целостности технических и программных средств. Назначьте приказом владельцев объектов ИС, ответственных за инвентаризацию всех объектов ИС, тиражирование карточек

учета на объекты ИС, формирование и внесение в карточки учета контрольных характеристик.

19. Составьте программу обучения персонала, утвердите список персонала, который должен пройти обучение, и проведите обучение; проконтролируйте знание персоналом ОРД, документации СЗИ и практические навыки по настройке средств защиты. Оформите результат обучения Актом.

20. Проведите настройку средств защиты на типовых объектах в соответствии с задокументированными правилами. Удостоверьтесь, что обученный персонал выполнил настройку средств защиты информации на объектах ИС в соответствии с установленными правилами.

21. Назначьте комиссию и проведите испытания СЗИ в соответствии с Программой и методикой испытаний на СЗИ. Результаты испытаний оформите протоколом и актом приемочных испытаний.

22. Сформируйте комплект документов согласно перечню исходных данных, приведенных в Приложении 2 к [6].

23. С учетом утвержденной организационной структуры организации и в соответствии с п. 14 [6], принимается решение об аттестации СЗИ владельцем ИС либо специализированной организацией. В последнем случае оформляется заявка и предоставляются исходные данные в соответствии с Приложениями 1, 2 к [6].

24. Проведите оценку качества исходных данных и оформите Акт оценки.

25. Разработайте Программу аттестации СЗИ ИС, руководствуясь п. 15 [6].

26. Разработайте Методику проведения испытаний средств защиты информации и оценки СЗИ в реальных условиях эксплуатации (далее – Методика) с учетом требований ЗБ и в соответствии с пп. 8, 18 [6].

27. Проведите проверку уровня подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации в соответствии с перечислением 4 п. 18 [6].

28. Убедитесь, что средства защиты СЗИ настроены в соответствии с правилами безопасности. Проведите испытания СЗИ в соответствии с Методикой, оформите протоколы испытаний и заключения по результатам проверок. Примите решение о готовности (не готовности) СЗИ к вводу в эксплуатацию и оформите его Актом.

29. При положительном решении оформите Аттестат ответственности.

Заключение

Применение владельцем ИС рекомендуемого порядка действий по созданию СЗИ и подготовке к аттестации государственных ИС или ИС, содержащих информацию распространение и (или) предоставление которой ограничено, позволит владельцу ИС контролировать процессы создания СЗИ и аттестации своей ИС при выполнении работ силами подразделения по технической защите информации либо силами подрядчиков, имеющих разрешение (лицензии) на такого рода деятельность.

Литература:

1. Закон Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации» // Нац. реестр правовых актов Респ. Беларусь от 17 ноября 2008 г. №2/1552.

2. Постановление Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2009 г. №5/29837.

3. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 25 мая 2012 № 46 «О некоторых мерах по реализации указа Президента Республики Беларусь от 8 ноября 2011 г. № 515» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2012 г. №7/2045.

4. Положение о технической и криптографической защите информации в Республике Беларусь: утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 // Нац. реестр правовых актов Респ. Беларусь от 17 апреля 2013 г. №1/14225.

5. Положение о порядке защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено: утв. Постановлением Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2009 г. №5/29837.

6. Положение о порядке аттестации систем защиты информации: утв. Постановлением Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2009 г. №5/29837.

Abstract

This article contains information about the legal foundations of creation security information system (ISS) information systems (IS) for different purposes, the problems of classification of IS as a typical object of informatization and guidance on the order of creation and the attestation of ISS IS of its owner.

Поступила в редакцию 18.05.2013 г.

Программаторы для любых микросхем

SEEPROM SEEPROM SEEPROM SEEPROM SEEPROM SEEPROM SEEPROM SEEPROM
EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM
EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM EEPROM
FLASH FLASH FLASH FLASH FLASH FLASH FLASH FLASH FLASH FLASH FLASH FLASH
PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC PIC
MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU MCU
PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL PAL

+375 (17) 266-32-09 www.chipstar.ru

HORNTREDE
ООО "ГорнТрейд"

поставка электронных компонентов

контрактное производство

тел.: +375 17 290 0082

факс: +375 17 290 0084

e-mail: info@horntrade.net

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ

УДК 004.4:004.9

Г.Д. Томина, А.В. Юрьева,

Государственное предприятие «НИИ ТЗИ», г. Минск

Аннотация

Статья содержит анализ технических решений по организации защищенного взаимодействия сторон, рассмотрены требования законодательства в части реализации криптографических средств защиты информации аппаратным и аппаратно-программным способом, предложен комплекс аппаратно-программных средств защищенного канала передачи данных, реализующий требования законодательства.

Введение

Организация защищенного канала передачи данных является актуальной задачей в государственных информационных системах (ИС), а также в ИС, содержащих информацию, распространение и (или) предоставление которой ограничено [1] и отнесенных по СТБ 34.101.30 к классу Б2 типовых объектов информатизации, для которых необходимо обеспечивать между контролируемыми зонами защищенный канал передачи данных. В то же время при оказании государственных электронных услуг юридическим и физическим лицам и обмене электронными документами, содержащими, например, персональные данные или банковскую тайну, для обеспечения безопасности и доверия необходимо обеспечивать конфиденциальность, достоверность и доступность электронных услуг, а также конфиденциальность и достоверность электронных документов.

В настоящее время для организации защищенного взаимодействия используются четыре группы технических решений, связанные со следующими технологиями:

1) идентификации и аутентификации пользователей с использованием сертификатов, цифровых удостоверений (для достоверной идентификации, разграничения доступа субъекта к ресурсам и управления привилегиями субъекта), протоколов Kerberos или домена;

2) доверенного удостоверяющего центра (УЦ) с использованием генерации и выпуска личных и открытых ключей подписи, ключей шифрования, сертификатов и списков отозванных сертификатов;

3) доверенной третьей стороны по проверке достоверности сертификатов, электронных документов и выдаче электронных квитанций по подтверждению их достоверности;

4) доверенного защищенного соединения или канала передачи данных с использованием идентификации и аутентификации по сертификатам, контроля целостности и шифрования передаваемых данных.

Один из наиболее распространенных методов организации защиты информации в процессе ее передачи основан на концепции построения защищенных виртуальных сетей (VPN) поверх открытых сетей передачи.

Защищенный канал можно построить на разных уровнях модели взаимодействия открытых систем:

канальном, сетевом, сеансовом. Чем ниже в стеке реализованы средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов, однако для канальных и сетевых средств возникает зависимость протокола защищенной передачи от используемой технологии связи: Ethernet, 802.X и т.д., что приводит к необходимости адаптации средств при переходе на другую технологию связи.

Формирование защищенных виртуальных каналов на сеансовом уровне позволяет организовать защищенное взаимодействие по сокетам и, в случае разработки указанных средств на кроссплатформенном языке программирования, позволит создать средства защищенного канала передачи данных не зависящие от используемых в ИС операционных систем (ОС).

Наиболее широкое распространение получили протоколы организации защищенных SSL/TLS соединений. Для взаимодействия клиента и сервера при формировании и поддержке защищаемого соединения протокол SSL/TLS предусматривает следующие этапы: идентификации и аутентификации по сертификатам при установлении SSL/TLS-сессии и защищенное взаимодействие.

Для аутентификации взаимодействующих сторон и формирования общих секретных ключей в реализациях протокола SSL, поддерживаемых ОС от ведущих западных компаний, чаще всего используют алгоритм RSA. Однако при построении VPN для государственных ИС или ИС, содержащих информацию, распространение и (или) предоставление которой ограничено, а также при взаимодействии в национальном сегменте инфраструктуры открытых ключей и трансграничном взаимодействии необходимо увязывать технологию VPN с существующими национальными и международными законодательствами.

Недостатком данной технологии является возможность выхода в сеть минуя защищенное соединение.

Большинство из VPN продуктов реализовано программным способом (например, Openssl), одним из базовых элементов которых являются средства, осуществляющие криптографические преобразования (шифрование, подпись) данных. Некоторые из VPN продуктов реализованы аппаратно-программным способом, в которых аппаратную часть составляют носители ключевой информации, представляющие, как правило, хранилище ключевой информации, из которого по предъявлению пароля (PIN-кода) личные ключи подписи и шифрования временно выгружаются в оперативную память ОС, а затем уничтожаются.

Вопросы применения криптографии в РБ и РФ подвержены жесткому законодательному регулированию. Например, в РБ согласно [2] для государственных ИС, а также ИС, содержащих информацию, распространение и (или) предоставление которой ограничено, должны при-

меняться только аппаратные или аппаратно-программные средства, реализующие криптографические операции на «борту». С октября 2013 года в соответствии с [3] аппаратные средства, реализующие криптографические преобразования на «борту», должны будут применяться только в ИС, обрабатывающих служебную информацию ограниченного распространения.

Полностью аппаратная реализация защищенного канала передачи данных приведет к существенному повышению цены изделия за счет необходимости реализации аппаратным способом механизмов организации канала передачи данных, получения и криптопреобразований данных. Предпочтительнее аппаратно-программная реализация защищенного канала передачи данных, поскольку стоимость изделия для каждого пользователя будет зависеть от скоростных характеристик микропроцессора, используемого для криптографических преобразований и объема дополнительной памяти, необходимой для получения и криптообработки электронного документа.

Комплекс аппаратно-программных средств защищенного канала передачи данных

На базе протоколов SSL/TLS можно построить защищенный канал передачи данных, который расширит известные технологии идентификации и аутентификации по сертификату и взаимодействия по защищенному соединению новыми механизмами двусторонней периодической аутентификации и конфигурирования разрешенных путей соединения передачи данных внутри защищенного канала.

При этом, используя протоколы SSL/TLS, можно создавать криптозащищенные каналы-туннели между конечными точками виртуальной сети. В качестве инициаторов каждого защищенного туннеля выступают клиент и сервер, функционирующие на компьютерах в конечных точках туннеля.

Государственное предприятие «НИИ ТЗИ» ведет подготовку к сертификации комплекса аппаратно-программных средств организации защищенного канала передачи данных (далее – комплекс Zchannel), соответствующего требованиям [1], [2], который предназначен для обеспечения криптографической защиты передаваемой информации на базе национальных стандартов, использует двустороннюю периодическую аутентификацию сторон и возможность конфигурирования разрешенных путей соединения передачи данных внутри защищаемого канала.

Программные средства комплекса Zchannel являются кросс-платформенными и функционируют под ОС Windows, Linux, HP. Аппаратные средства комплекса Zchannel представляют собой аппаратные идентификаторы (АИ), обеспечивающие надежное хранение ключевой информации и выполнение криптографических преобразований.

Комплекс Zchannel обеспечивает следующие основные возможности:

- аутентификацию сторон по сертификатам в режиме односторонней аутентификации сервера или взаимной аутентификации сервера и клиента, в т.ч. аутентификацию удаленного сервера по сертификату X.509 сервера

- (обеспечивая защиту от атаки «человек посередине»), аутентификацию клиента на сервере по сертификату X.509 клиента (обеспечивая защиту от несанкционированного доступа к ресурсам сервера);

- защиту путей передачи данных соединения в канале с помощью вызовов функций шифрования, хеширования, выработки электронной цифровой подписи (ЭЦП) из библиотеки криптографических функций АИ, а также проверки ЭЦП путем вызова библиотеки криптографических функций программных средств комплекса Zchannel;

- поддержку стандарта S/MIME для криптографической защиты электронной почты;

- управление контекстами защиты (шифронаборы, длины ключей) при настройке программных средств защищенного канала передачи данных;

- конфигурирование путей (соединений) для защищенного канала, а также применяемых шифронаборов и сертификатов;

- хранение криптографических ключей и других критичных параметров в АИ;

- выполнения криптографических операций шифрования и подписи в АИ;

- защиту канала между клиентом и сервером для обеспечения конфиденциальности и целостности обмена данными;

- защиту канала между клиентом и сервером для обеспечения только целостности обмена данными;

- проверку подлинности сертификата, наличия сертификата в списке сертификатов и отсутствия в списке отозванных сертификатов.

Комплекс Zchannel создает защищенный канал между клиентом и сервером, обеспечивает защиту соединения любого прикладного протокола, работающего через TCP-соединение без динамического открытия портов, в частности, HTTP, SMTP, POP3, IMAP, FTP (passive mode), NFS, SQL и т.д.

Комплекс Zchannel состоит из серверной и клиентской частей. Клиентская часть комплекса Zchannel открывает указанный порт, принимает на него открытые данные от приложения, шифрует и передает их по защищенному каналу в серверную часть комплекса Zchannel. Серверная часть комплекса Zchannel открывает указанный порт, принимает по защищенному каналу данные, расшифровывает и передает их либо на указанный локальный порт приложения, либо на указанный порт на удаленном узле, обеспечивая, таким образом, поддержку защищенного канала для различных серверных приложений.

Для обеспечения совместимости со средствами криптографической защиты информации других производителей комплекс Zchannel соответствует следующим стандартам в области защиты информации:

- международным стандартам и рекомендациям X.509, PKI, PKCS#7, PKCS#11, S/MIME, CMS, а также СТБ 34.101.19, СТБ 34.101.23;

- СТБ 1176.2 и СТБ П 34.101.45 с использованием СТБ 34.101.47, СТБ 34.101.31, а также ГОСТ Р 34.10-2001 для выработки и проверки ЭЦП;

- СТБ 34.101.31, ГОСТ Р 34.11-94 для вычисления значения хеш-функции;

– ГОСТ 28147-89, СТБ 34.101.31 для шифрования данных.

Такой комплекс позволит создать доверенный защищенный канал между двумя и более узлами в сетях для исключения возможности угрозы прослушивания трафика, без необходимости вносить изменения в работу прикладного ПО клиента и сервера.

Заключение

Применение аппаратно-программных средств организации защищенного канала передачи данных позволит решить задачи защищенного взаимодействия для ИС, содержащих информацию, распространение и (или) предоставление которой ограничено (за исключением государственных секретов), а также обеспечит доверенное взаимодействие при оказании государственной ИС электронных услуг юридическим и физическим лицам.

Литература:

1. Постановление Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» // Нац. реестр правовых актов Респ.

Беларусь от 1 июня 2009 г. №5/29837.

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 25 мая 2012 № 46 «О некоторых мерах по реализации указа Президента Республики Беларусь от 8 ноября 2011 г. № 515» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2012 г. №7/2045.

3. Положение о технической и криптографической защите информации в Республике Беларусь: утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 // Нац. реестр правовых актов Респ. Беларусь от 17 апреля 2013 г. №1/14225.

Abstract

The article contains an analysis of technical solutions for organizations secure communication between the parties, the requirements of the legislation in terms of cryptographic information security implementation means by the hardware and hardware-software method, presents the hardware-software complex for organization secure data transmission channel that implements the requirements of the law.

Поступила в редакцию 18.05.2013 г.

ПРАВОВЫЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

УДК 002:004.056

Аннотация

Приведен обзор нормативно-правовой базы Республики Беларусь в области защиты информации критически важных объектов информатизации.

Введение

Построение системы защиты информации критически важных объектов информатизации (далее – КВОИ) определяется постановлением Совета Министров Республики Беларусь от 30 марта 2012 года № 293 «О некоторых вопросах безопасности эксплуатации и надежного функционирования критически важных объектов информатизации», законом Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации», постановлением Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации», а также основывается на других нормативных правовых актах (далее – НПА) Республики Беларусь и технических нормативных правовых актах (далее – ТНПА) в области защиты информации.

Построение защиты критически важных объектов информатизации

Порядок защиты КВОИ включает следующие последовательные процедуры:

1) отнесение объекта информатизации к КВОИ в соответствии с перечнем отраслевых критериев отнесения объектов информатизации к КВОИ;

Д.А. Комликов, Г.Д. Томина, Г.Г. Малюга,
Государственное предприятие «НИИ ТЗИ», г. Минск

2) классификацию КВОИ в соответствии с НПА и ТНПА;

3) организацию защиты КВОИ в соответствии с присвоенным классом КВОИ, НПА и ТНПА;

4) аттестацию системы защиты информации (далее – СЗИ) КВОИ;

5) проведение внешнего контроля КВОИ.

Первая процедура отнесения объекта информатизации к КВОИ выполняется согласно:

Порядку отнесения объекта информатизации к КВОИ, определенному в главе 3 Положения об отнесении объекта информатизации к КВОИ и обеспечения безопасности КВОИ, утвержденного Указом Президента Республики Беларусь от 25 октября 2011 года № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»;

Методики определения соответствия объекта информатизации отраслевым критериям отнесения объектов информатизации к критически важным объектам информатизации по Постановлению Совета Министров Республики Беларусь № 293;

Положения о Государственном реестре критически важных объектах информатизации, утвержденном Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2011 года № 96.

Объект информатизации считается отнесенным к КВОИ со дня его включения в Государственный реестр критически важных объектах информатизации.

Вторая процедура – классификация КВОИ.

Порядок определения классов КВОИ установлен в СТБ П 34.101.52-2012. Согласно классификации КВОИ по требованиям безопасности установлены 18 классов профилей защиты (далее – ПЗ) КВОИ. Стандарты СТБ П 34.101.53-2012 – СТБ П 34.101.58-2012 устанавливают требования безопасности к СЗИ КВОИ для предотвращения умеренного ущерба и содержат требования безопасности к СЗИ, обеспечивающие предотвращение высокого и катастрофического ущерба.

Третья процедура – организация защиты КВОИ в соответствии с присвоенным классом КВОИ включает комплекс мероприятий по созданию его СЗИ согласно следующим документам:

- Положению о порядке защиты информации в государственных информационных системах, а также в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, утвержденному Постановлением Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» (далее – Положение о порядке защиты);

- Положению о порядке организации криптографической защиты информации в государственных информационных системах, в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено (за исключение государственных секретов), а также в критически важных объектах информатизации, утвержденному Приказом Оперативно-аналитического центра Республики Беларусь от 25 мая 2012 года № 46 (далее – Положение о порядке организации КЗИ).

Положение о порядке защиты определяет комплекс мероприятий по созданию СЗИ и совокупность документированных правил, процедур и требований в области защиты информации, действующих в организации владельца информационной системы (ИС). Комплекс мероприятий по созданию СЗИ включает требования пунктов 10–14 Положения о порядке защиты.

Положение о порядке организации КЗИ определяет требования к комплексу средств криптографической защиты информации (далее – СКЗИ), в том числе средств управления криптографическими ключами, средств обеспечения безопасности СКЗИ, а также к комплексу организационных мер, которым необходимо соответствовать для применения в СЗИ ИС, относящихся к объектам информатизации классов А2 или Б2, или к КВОИ классов: А1-у, А1-в, А1-м, Б1-у, Б1-в или Б1-м.

Следует отметить, что комплекс мероприятий по созданию СЗИ включает оценку соответствия СЗИ требованиям НПА и ТНПА в области защиты информации путем проведения комплекса мероприятий по аттестации СЗИ, который, по сути, представляет отдельную процедуру.

Четвертая процедура – аттестация СЗИ КВОИ на соответствие требованиям НПА и ТНПА в области защиты информации включает комплекс мероприятий в соответствии с Положением о порядке аттестации системы защиты информации, утвержденным Постановлением Совета Министров Республики Беларусь от 26 мая 2009 года № 675 «О некоторых вопросах защиты информации» (далее – Положение о порядке аттестации).

Положение о порядке аттестации распространяется на аттестацию СЗИ государственных ИС, а также СЗИ ИС, содержащих информацию, распространение и (или) предостав-

ление которой ограничено (за исключение государственных секретов).

Комплексная оценка СЗИ при аттестации включает проведение мероприятий по пунктам 8 и 18 Положения о порядке аттестации.

Пятая процедура – проведение внешнего контроля включает комплекс мероприятий, проводимых уполномоченным государственным органом по проверке соблюдения установленных требований в области защиты информации для СЗИ государственных ИС, для ИС, содержащих информацию, распространение и (или) предоставление которой ограничено (за исключение государственных секретов), а также КВОИ с учетом следующих документов:

- Положения о порядке защиты (пункт 15);

- Положения о порядке организации КЗИ (пункт 14);

- Инструкции о порядке проведения внешнего контроля критически важных объектов информатизации, утвержденной Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 года № 42. Инструкция определяет перечень проверок (пункт 13), проводимых при внешнем контроле.

Заключение

В соответствии с выше указанным можно утверждать, что в Республике Беларусь создана современная правовая основа для построения СЗИ КВОИ. Представленный в статье обзор позволяет комплексно рассмотреть вопрос построения СЗИ КВОИ.

Литература:

1. Постановление Совета Министров Республики Беларусь от 30.03.2012 № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации» // Нац. реестр правовых актов Респ. Беларусь от 03 апреля 2012 г. № 5/35494.

2. Постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 675 «О некоторых вопросах защиты информации» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2009 г. N 5/29837.

3. Указ Президента Республики Беларусь от 25.10.2011 № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» // Нац. реестр правовых актов Респ. Беларусь от 26 октября 2011 г. № 1/13026.

4. Приказ Оперативно-аналитического центра Республики Беларусь от 25 мая 2012 года № 46 «О некоторых мерах по реализации указа Президента Республики Беларусь от 8 ноября 2011 г. № 515» // Нац. реестр правовых актов Респ. Беларусь от 1 июня 2012 г. № 7/2045.

5. Приказ Оперативно-аналитического центра Республики Беларусь от 30 апреля 2012 года № 42 «Об утверждении Инструкции о порядке проведения внешнего контроля критически важных объектов информатизации» // Нац. реестр правовых актов Респ. Беларусь от 4 мая 2012 г. № 7/2003.

Abstract

Provides an overview of legal and regulatory framework of the Republic of Belarus in the field of information security of critical objects of informatization.

Поступила в редакцию 18.05.2013 г.

ИСКАЖЕНИЕ УЗКОПОЛОСНЫХ ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСНЫХ СИГНАЛОВ ПРИ ПРОХОЖДЕНИИ ЧЕРЕЗ БИИЗОТРОПНЫЙ ЭКРАН

УДК 537.87:621.37

В.Т. Ерофеев, В.Ф. Бондаренко,
НИИ ППМИ БГУ, г. Минск

Аннотация

Разработана методика математического моделирования процессов преобразования импульсных электромагнитных полей, распространяющихся под произвольным углом и несущих узкополосный сигнал, при проникновении через бесконечный плоский композитный экран, выполненный из биизотропного материала с произвольными комплексными параметрами киральности. Для численной реализации модели рассмотрены атомарные функции, которые используются для аппроксимации реальных сигналов. Показано, что ТЕ-поляризованные сигналы при прохождении через экран могут быть преобразованы в ТН-поляризованные узкополосные сигналы и наоборот.

Введение

В последнее время значительное число работ в печати посвящено исследованию электродинамических свойств композитных материалов [1]. Композитные материалы представляют собой однородные матрицы, заполненные большим числом случайно распределенных мелких неоднородностей с различной геометрией и материальным составом [2]. Для электродинамического моделирования композитных материалов используются математические модели биизотропных материалов с эффективными параметрами, полученными с помощью усреднения неоднородностей. Такие усреднения приводят к материальным уравнениям, содержащим линейные комбинации электрических и магнитных полей. В частности к биизотропным средам относятся киральные метаматериалы с необычными электродинамическими свойствами [3].

Расчет электромагнитных экранов выполненных из композитных материалов в настоящее время является актуальной задачей. Экраны используются для решения проблемы электромагнитной совместимости сложных технических устройств радиотехники и электроники, а также для защиты чувствительных приборов от воздействия внешних помехонесущих электромагнитных излучений. В литературе большинство работ посвящено исследованию взаимодействия с экранами полей с гармонической зависимостью от времени. Взаимодействия импульсных полей с биизотропными экранами исследованы недостаточно.

Для приложений важным является разработка и исследование математических моделей, описывающих распространение в среде импульсных сигналов с помощью электромагнитных полей. Для передачи информации используются сигналы с финитным спектром, которые представимы без искажений своими значениями в дискретные моменты времени. Получило развитие математическое моделирование сигналов с применением атомарных функций [4, 5], которые используются для аппроксимации реальных сигналов [6].

Постановка задачи

Рассмотрим пространство R^3 с фиксированной системой декартовых координат $Oxyz$. В пространстве с электрической и магнитной постоянными ϵ_0, μ_0 расположен плоский экран D ($0 < z < \Delta$), заполненный биизотропным материалом с физическими комплексными параметрами $\epsilon = \epsilon_r \epsilon_0$, $\mu = \mu_r \mu_0$, $G = G_r / c$, $Z = Z_r / c$. Из полупространства D_1 ($z < 0$) на слой D воздействует плоское импульсное электромагнитное поле $\vec{E}_0(\vec{r}, t)$, $\vec{H}_0(\vec{r}, t)$, которое в частотной области определяется формулами [7]

$$\begin{aligned}\hat{E}_0(\vec{r}, \omega) &= \hat{A}_0(\omega) \vec{W}_0^{(-1)}(\vec{r}, \omega) + \hat{B}_0(\omega) \vec{W}_0^{(-2)}(\vec{r}, \omega), \\ \hat{H}_0(\vec{r}, \omega) &= h_0 (\hat{A}_0(\omega) \vec{W}_0^{(-2)}(\vec{r}, \omega) + \hat{B}_0(\omega) \vec{W}_0^{(-1)}(\vec{r}, \omega))\end{aligned}\quad (1)$$

где

$$\begin{aligned}\vec{W}_0^{(\mp 1)} &= i \vec{V}_1 \exp(i \omega p_{\pm}(\vec{r}, \theta_0, \varphi_0)), \\ \vec{W}_0^{(\mp 2)} &= \pm \vec{V}_2 \exp(i \omega p_{\pm}(\vec{r}, \theta_0, \varphi_0)), \\ \vec{V}_1 &= \sin \varphi_0 \vec{e}_x - \cos \varphi_0 \vec{e}_y, \\ \vec{V}_2 &= -\cos \theta_0 (\cos \varphi_0 \vec{e}_x + \sin \varphi_0 \vec{e}_y) + \sin \theta_0 \vec{e}_z, \\ p_{\pm} &= \frac{1}{c} (\alpha_1 x + \alpha_2 y \pm z \cos \theta_0), \quad \alpha_1 = \cos \varphi_0 \sin \theta_0, \\ \alpha_2 &= \sin \varphi_0 \sin \theta_0, \quad p = p_{+},\end{aligned}$$

$$h_0 = \frac{1}{i Z_0}, \quad Z_0 = \sqrt{\mu_0 / \epsilon_0}, \quad \hat{A}_0(\omega), \quad \hat{B}_0(\omega) -$$

заданные функции круговой частоты,

$$\omega = 2\pi f; \quad \vec{r} = (x, y, z), \quad \theta_0, \varphi_0 -$$

углы, характеризующие направление распространения первичного поля; c – скорость света в вакууме.

Таким образом,

$$\begin{aligned}\hat{E}_0(\vec{r}, \omega) &= (\hat{A}_0 \vec{V}_1 + \hat{B}_0 \vec{V}_2) e^{i \omega p}, \\ \hat{H}_0(\vec{r}, \omega) &= h_0 (\hat{A}_0 \vec{V}_2 + i \hat{B}_0 \vec{V}_1) e^{i \omega p}.\end{aligned}\quad (2)$$

Поля $\hat{E}_0(\vec{r}, \omega)$, $\hat{H}_0(\vec{r}, \omega)$ являются спектральными плотностями полей $\vec{E}_0(\vec{r}, t)$, $\vec{H}_0(\vec{r}, t)$ во временной области. Электромагнитное поле в частотной области (2) связано с полем во временной области с помощью преобразования Фурье [8]

$$\begin{aligned}\vec{E}_0(\vec{r}, t) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{E}_0(\vec{r}, \omega) e^{-i \omega t} d\omega = \\ &= i A_0(t - p) \vec{V}_1 + B_0(t - p) \vec{V}_2, \\ \vec{H}_0(\vec{r}, t) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{H}_0(\vec{r}, \omega) e^{-i \omega t} d\omega = \\ &= h_0 (A_0(t - p) \vec{V}_2 + i B_0(t - p) \vec{V}_1)\end{aligned}\quad (3)$$

где для временного сигнала $A_0(t)$ имеем соотношения

$$\hat{A}_0(\omega) = \int_{-\infty}^{\infty} A_0(t) e^{i\omega t} dt, \quad A_0(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{A}_0(\omega) e^{-i\omega t} d\omega. \quad (4)$$

Аналогично для $B_0(t)$.

Реальное импульсное электромагнитное поле определим в виде

$$\begin{aligned} \vec{E}_0(\vec{r}, t) &= \text{Re } \vec{E}_0(\vec{r}, t) = -\text{Im } A_0(t-p) \vec{Y}_1 + \text{Re } B_0(t-p) \vec{Y}_2, \\ \vec{H}_0(\vec{r}, t) &= \text{Re } \vec{H}_0(\vec{r}, t) = \\ &= \frac{1}{Z_0} (\text{Im } A_0(t-p) \vec{Y}_2 + \text{Re } B_0(t-p) \vec{Y}_1) \end{aligned} \quad (5)$$

В результате взаимодействия первичного поля (2) с экраном D образуются поля: $\hat{E}'_1, \hat{H}'_1$ – отраженное поле в D_1 ; $\hat{E}_1 = \hat{E}_0 + \hat{E}'_1$, $\hat{H}_1 = \hat{H}_0 + \hat{H}'_1$ – суммарное поле в D_1 ; $\hat{E}, \hat{H}$ – поле в слое D ; $\hat{E}_2, \hat{H}_2$ – поле, проникшее в область D_2 ($z > \Delta$).

Сформулируем краевую задачу в частотной области для спектральных полей.

Краевая задача. Требуется для заданного поля (2) определить поля $\hat{E}'_1, \hat{H}'_1$; $\hat{E}, \hat{H}$; $\hat{E}_2, \hat{H}_2$ соответственно в областях D_1, D, D_2 , которые удовлетворяют уравнениям Максвелла [7]

$$\begin{aligned} \text{rot } \hat{E}'_1 &= i\omega\mu_0 \hat{H}'_1, \quad \text{rot } \hat{H}'_1 = -i\omega\epsilon_0 \hat{E}'_1, \quad z < 0, \\ \text{rot } \hat{E} &= i\omega \left(\mu \hat{H} + Z \hat{E} \right), \\ \text{rot } \hat{H} &= -i\omega \left(\epsilon \hat{E} + G \hat{H} \right), \quad 0 < z < \Delta, \\ \text{rot } \hat{E}_2 &= i\omega\mu_0 \hat{H}_2, \quad \text{rot } \hat{H}_2 = -i\omega\epsilon_0 \hat{E}_2, \quad z > \Delta, \end{aligned} \quad (6)$$

граничным условиям непрерывности тангенциальных составляющих полей на плоскостях $\Gamma_1(z=0)$, $\Gamma_2(z=\Delta)$

$$\begin{aligned} \left(\hat{E}_{1\tau} - \hat{E}'_{1\tau} \right)_{\Gamma_1} &= 0, \quad \left(\hat{H}_{1\tau} - \hat{H}'_{1\tau} \right)_{\Gamma_1} = 0, \\ \left(\hat{E}_{2\tau} - \hat{E}_{\tau} \right)_{\Gamma_2} &= 0, \quad \left(\hat{H}_{2\tau} - \hat{H}_{\tau} \right)_{\Gamma_2} = 0 \end{aligned} \quad (7)$$

и условиям на бесконечности.

Аналитическое решение задачи

В задачах экранирования электромагнитных полей основным является определение отраженных полей и полей, прошедших через экран. Для аналитического решения задачи (6), (7) результирующие поля выразим через базисные поля (1), в виде комбинаций

$$\begin{aligned} \hat{E}'_1 &= \hat{x}_1(\omega) \vec{W}_0^{(+1)} + \hat{x}_2(\omega) \vec{W}_0^{(+2)}, \\ \hat{H}'_1 &= h_0(\hat{x}_1(\omega) \vec{W}_0^{(+2)} + \hat{x}_2(\omega) \vec{W}_0^{(+1)}) \quad z < 0, \\ \hat{E}_2 &= \hat{y}_1(\omega) \vec{W}_0^{(-1)} + \hat{y}_2(\omega) \vec{W}_0^{(-2)}, \\ \hat{H}_2 &= h_0(\hat{y}_1(\omega) \vec{W}_0^{(-2)} + \hat{y}_2(\omega) \vec{W}_0^{(-1)}) \quad z > \Delta. \end{aligned} \quad (8)$$

Поля (8) удовлетворяют уравнениям (6) и решение задачи сводится к определению функций $\hat{x}_j(\omega)$, $\hat{y}_j(\omega)$, $j=1,2$, с учетом условий (7). Для решения задачи (6), (7) эффективным является использование нелокальных граничных условий [9].

Для биизотропного экрана D амплитуды полей (8), зависящие от частоты ω , определяются формулами

$$\begin{aligned} \hat{y}_1 &= \frac{G}{Q} (A_0 Q_{22} + B_0 Q_{12}), \quad \hat{y}_2 = -\frac{G}{Q} (A_0 Q_{21} + B_0 Q_{11}), \\ \hat{x}_1 &= \frac{1}{Q} [A_0 (Q_{21} Q'_{12} - Q_{22} Q'_{11}) + B_0 (Q_{11} Q'_{12} - Q_{12} Q'_{11})], \\ \hat{x}_2 &= \frac{1}{Q} [A_0 (Q_{22} Q'_{21} - Q_{21} Q'_{22}) + B_0 (Q_{12} Q'_{21} - Q_{11} Q'_{22})], \\ G &= 2 \sin^2 \theta_0 \exp(k_0 v_0 \Delta), \quad Q = Q_{11} Q_{22} - Q_{12} Q_{21}. \end{aligned} \quad (9)$$

$$\begin{aligned} Q_{11} &= (\hat{B} \vec{c}, \vec{a}), \quad Q_{12} = (\hat{B} \vec{d}, \vec{a}), \\ Q_{21} &= (\hat{B} \vec{c}, \vec{b}), \quad Q_{22} = (\hat{B} \vec{d}, \vec{b}), \\ Q'_{11} &= (\hat{B} \vec{c}, \vec{a}'), \quad Q'_{12} = (\hat{B} \vec{d}, \vec{a}'), \\ Q'_{21} &= (\hat{B} \vec{c}, \vec{b}'), \quad Q'_{22} = (\hat{B} \vec{d}, \vec{b}'), \\ \vec{a} &= \left(i\alpha_2, -i\alpha_1, Z_0 \frac{\alpha_1}{v_0}, Z_0 \frac{\alpha_2}{v_0} \right), \\ \vec{b} &= \left(i \frac{\alpha_1}{v_0}, i \frac{\alpha_2}{v_0}, Z_0 \alpha_2, -Z_0 \alpha_1 \right), \\ \vec{a}' &= \left(-i\alpha_2, i\alpha_1, Z_0 \frac{\alpha_1}{v_0}, Z_0 \frac{\alpha_2}{v_0} \right), \\ \vec{b}' &= \left(i \frac{\alpha_1}{v_0}, i \frac{\alpha_2}{v_0}, -Z_0 \alpha_2, Z_0 \alpha_1 \right), \\ \vec{c} &= \left(-i\alpha_2, i\alpha_1, \frac{v_0 \alpha_1}{Z_0}, \frac{v_0 \alpha_2}{Z_0} \right), \\ \vec{d} &= \left(iv_0 \alpha_1, iv_0 \alpha_2, -\frac{\alpha_2}{Z_0}, \frac{\alpha_1}{Z_0} \right), \\ \vec{c}' &= \left(i\alpha_2, -i\alpha_1, \frac{v_0 \alpha_1}{Z_0}, \frac{v_0 \alpha_2}{Z_0} \right), \\ \vec{d}' &= \left(iv_0 \alpha_1, iv_0 \alpha_2, \frac{\alpha_2}{Z_0}, -\frac{\alpha_1}{Z_0} \right), \quad v_0 = -i \cos \theta_0. \end{aligned} \quad (10)$$

При $\theta_0 = 0$ коэффициенты (8) вычисляются как пределы $\lim_{\theta_0 \rightarrow 0} \hat{x}_j$, $\lim_{\theta_0 \rightarrow 0} \hat{y}_j$. Матричные элементы матрицы $\hat{B}$, входящей в формулы (10) известны:

$$\hat{B} = \hat{B}(\epsilon, \mu, G, Z, \Delta, \omega) = \{B_{lm}\}, \quad l, m = 1, 2, 3, 4;$$

$$B_{11} = p(p_1(\Phi_2 S_2 + C_2) - p_2(\Phi_1 S_1 + C_1)),$$

$$B_{12} = p(p_2 \theta_1 S_1 - p_1 \theta_2 S_2)$$

$$B_{13} = p(\Phi_1 S_1 - \Phi_2 S_2 + C_1 - C_2), \quad B_{14} = p(\theta_2 S_2 - \theta_1 S_1)$$

$$\begin{aligned}
B_{21} &= p(p_1 \delta_2 S_2 - p_2 \delta_1 S_1) \\
B_{22} &= p(p_1(C_2 - \Phi_2 S_2) + p_2(\Phi_1 S_1 - C_1)) \\
B_{23} &= p(\delta_1 S_1 - \delta_2 S_2) \quad B_{24} = p(\Phi_2 S_2 - \Phi_1 S_1 + C_1 - C_2) \\
B_{31} &= -p_1 p_2 B_{13}, \quad B_{32} = -p_1 p_2 B_{14}, \\
B_{33} &= p(p_1(C_1 + \Phi_1 S_1) - p_2(\Phi_2 S_2 + C_2)) \\
B_{34} &= p(p_2 \theta_2 S_2 - p_1 \theta_1 S_1) \\
B_{41} &= -p_1 p_2 B_{23}, \quad B_{42} = -p_1 p_2 B_{24}, \\
B_{43} &= p(p_1 \delta_1 S_1 - p_2 \delta_2 S_2) \\
B_{44} &= p(p_1(C_1 - \Phi_1 S_1) + p_2(\Phi_2 S_2 - C_2)) \\
S_j &= \text{sh}(k_0 \Delta v_j) \quad C_j = \text{ch}(k_0 \Delta v_j) \quad \Phi_j = \frac{\alpha_1 \alpha_2 g_j}{g v_j},
\end{aligned}$$

$$\theta_j = \frac{g_j(\alpha_1^2 - k_j^2)}{g v_j},$$

$$\delta_j = \frac{g_j(\alpha_2^2 - k_j^2)}{g v_j}, \quad j = 1, 2;$$

$$k_j = \sqrt{g + \frac{1}{2}a^2 + a f_j}, \quad 0 \leq \arg k_j < \pi, \quad f_j = (-1)^j f_0,$$

$$f_0 = \sqrt{\epsilon_r \mu_r - b^2}, \quad 0 \leq \arg f_0 < \pi, \quad a = i(G_r - Z_r)$$

$$b = \frac{1}{2}(G_r + Z_r), \quad g = \epsilon_r \mu_r - G_r Z_r, \quad g_j = f_j - \frac{1}{2}a,$$

$$v_j = \sqrt{\sin^2 \theta_0 - k_j^2}, \quad -\frac{\pi}{2} \leq \arg v_j < \frac{\pi}{2},$$

$$p_j = \frac{1}{Z_0 \mu_r} \left(\frac{i g}{g_j} - Z_r \right), \quad p = \frac{1}{p_1 - p_2}.$$

Для распространения метода решения задачи на N -слойный экран D достаточно в формулах (10) матрицу $\hat{B}$ заменить на матрицу где $\hat{B}_{cl} = \hat{B}_1 \cdot \hat{B}_2 \dots \hat{B}_N$:

$$\hat{B}_k = \hat{B}(\epsilon_k, \mu_k, G_k, Z_k, \Delta_k, \omega), \quad \Delta = \sum_{k=1}^N \Delta_k.$$

Узкополосные сигналы

В дальнейшем рассмотрим случай полей (2), когда $\hat{A}_0 \neq 0$, $\hat{B} = 0$. Из (9) следует

$$\hat{y}_1(\omega) = \hat{h}(\omega) \hat{A}_0(\omega), \quad \hat{y}_2(\omega) = \hat{g}(\omega) \hat{A}_0(\omega) \quad (11)$$

где

$$\hat{h}(\omega) = \frac{G(\omega)}{Q(\omega)} Q_{22}(\omega), \quad \hat{g}(\omega) = -\frac{G(\omega)}{Q(\omega)} Q_{21}(\omega)$$

В качестве сигнала $A_0(t)$ выберем узкополосный сигнал [10], для которого

$$\hat{A}_0(\omega) = \hat{s}_0(\omega - \omega_0), \quad \omega_0 > 0, \quad (12)$$

где $\hat{s}_0(\omega) \neq 0$ при $|\omega| < \alpha$, $\hat{s}_0(\omega) = 0$ при $|\omega| \geq \alpha$, $\frac{\alpha}{\omega_0} \ll 1$; видеоимпульс $s_0(t)$ и спектральная плотность $\hat{s}_0(\omega)$ связаны формулами (4).

Для финитной спектральной плотности $\hat{s}_0(\omega)$ имеют место формулы Котельникова-Шеннона

$$s_0(t) = \sum_{k=-\infty}^{\infty} \delta_k^{(0)} \text{sinc}(\alpha(t - t_k)), \quad -\infty < t < \infty, \quad (13)$$

$$\text{где } \delta_k^{(0)} = s_0(t_k), \quad t_k = \frac{\pi k}{\alpha}, \quad \text{sinc}(x) = \frac{\sin x}{x},$$

$$\hat{s}_0(\omega) = \frac{\pi}{\alpha} \sum_{k=-\infty}^{\infty} \delta_k^{(0)} e^{it_k \omega}, \quad |\omega| < \alpha. \quad (14)$$

Коэффициенты ряда Фурье (14) вычисляются с помощью формулы

$$\delta_m^{(0)} = \frac{1}{2\pi} \int_{-\alpha}^{\alpha} \hat{s}_0(\omega) e^{-it_m \omega} d\omega, \quad m = 0, \pm 1, \pm 2, \dots \quad (15)$$

Из соотношения (12) следует

$$A_0(t) = e^{-i\omega_0 t} s_0(t) \quad (16)$$

Изучим сигнал $y_1(t)$ с финитной спектральной плотностью (11), который проникает в область D_2 . Учитывая условие $\tau \ll 1$, функцию $\hat{h}(\omega)$ на отрезке $\omega_0 - \alpha < \omega < \omega_0 + \alpha$ в окрестности точки ω_0 представим в виде приближения

$$\hat{h}(\omega) \approx c_{1h} + \frac{c_{2h}}{\alpha} (\omega - \omega_0) + \frac{c_{3h}}{\alpha^2} (\omega - \omega_0)^2,$$

$$\text{где } c_{1h} = \hat{h}(\omega_0), \quad c_{2h} = \frac{1}{2} (\hat{h}(\omega_0 + \alpha) - \hat{h}(\omega_0 - \alpha))$$

$$c_{3h} = \frac{1}{2} (\hat{h}(\omega_0 + \alpha) + \hat{h}(\omega_0 - \alpha)) - \hat{h}(\omega_0).$$

$$\text{Тогда } \hat{y}_1(\omega) \approx \hat{h}_1(\omega) = \left(c_{1h} + \frac{c_{2h}}{\alpha} (\omega - \omega_0) + \frac{c_{3h}}{\alpha^2} (\omega - \omega_0)^2 \right) \hat{s}_0(\omega - \omega_0) \quad (17)$$

Для финитной плотности $\hat{s}_j(\omega) = \omega^j \hat{s}_0(\omega)$ в соответствии с формулами Котельникова-Шеннона, имеем

$$\begin{aligned}
s_j(t) &= \sum_{k=-\infty}^{\infty} \delta_k^{(j)} \text{sinc}(\alpha(t - t_k)), \quad -\infty < t < \infty, \\
\hat{s}_j(\omega) &= \frac{\pi}{\alpha} \sum_{k=-\infty}^{\infty} \delta_k^{(j)} e^{it_k \omega}, \quad |\omega| < \alpha, \quad (18)
\end{aligned}$$

где из формул (14), (15) следует

$$\delta_m^{(j)} = \frac{1}{2\pi} \int_{-\alpha}^{\alpha} \omega^j \hat{s}_0(\omega) e^{-it_m \omega} d\omega,$$

$$\delta_m^{(1)} = i \frac{\alpha}{\pi} \beta_m, \quad \beta_m = \sum_{k=-\infty}^{\infty} \delta_k^{(0)} z_{m-k}, \quad z_m = \frac{(-1)^m}{m}, \quad z_0 = 0;$$

$$\delta_m^{(2)} = \frac{2\alpha^2}{\pi^2} \gamma_m, \quad \gamma_m = \sum_{k=-\infty}^{\infty} \delta_k^{(0)} y_{m-k},$$

$$y_m = \frac{(-1)^m}{m^2}, \quad y_0 = \frac{\pi^2}{6}. \quad (19)$$

Учитывая (17), (18), вычислим

$$h_1(t) = e^{-i\omega_0 t} \left(c_{1h} s_0(t) + \frac{c_{2h}}{\alpha} s_1(t) + \frac{c_{3h}}{\alpha^2} s_2(t) \right) =$$

$$= e^{-i\omega_0 t} \sum_{k=-\infty}^{\infty} B_k^h \sin(\alpha(t-t_k)) \quad (20)$$

Преобразуем формулу (20), полагая $\sin(\alpha(t-t_k)) = (-1)^k \sin \alpha t$. Получим

$$h_1(t) = e^{-i\omega_0 t} \sin(\alpha t) B^h(t) \quad (21)$$

$$\text{где } B^h(t) = \sum_{k=-\infty}^{\infty} B_k^h \frac{(-1)^k}{\alpha t - \pi k}.$$

Функция $B^h(t)$ имеет особенности в точках $t = t_k$, $B^h(t_k) = \infty$. При вычислении функции (21) в особых точках t_k необходимо раскрывать неопределенность $0 \cdot \infty$. При раскрытии неопределенности получим

$$h_1(t_k) = \lim_{t \rightarrow t_k} h_1(t) = e^{-i\omega_0 t_k} B_k^h.$$

Таким образом временные сигналы, соответствующие спектральным плотностям, вычислены. Для ТЕ- и ТН-составляющих поля имеем приближения

$$y_1(t) \approx h_1(t) = e^{-i\omega_0 t} \sin(\alpha t) B^h(t),$$

$$y_2(t) \approx g_1(t) = e^{-i\omega_0 t} \sin(\alpha t) B^g(t)$$

Импульсное электромагнитное поле узкополосного сигнала, прошедшего через биизотропный экран D , выражается в виде

$$\begin{aligned} \vec{E}_2 &= i h_1(t-p) \vec{Y}_1 + g_1(t-p) \vec{Y}_2, \\ \vec{H}_2 &= \frac{1}{Z_0} (-h_1(t-p) \vec{Y}_2 + g_1(t-p) \vec{Y}_1). \end{aligned} \quad (22)$$

Атомарные функции

Для представления первичного поля (2) будем использовать атомарную функцию $up(x)$: $up(x) \neq 0$ при $|x| < 1$, $up(x) = 0$ при $|x| \geq 1$, $up(-x) = up(x)$.

С функцией $up(x)$ связана функция

$$Up(y) = \prod_{n=1}^{\infty} \text{sinc}\left(\frac{y}{2^n}\right), \quad -\infty < y < \infty, \quad (23)$$

с помощью преобразования Фурье

$$up(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} Up(y) e^{iyx} dy. \quad (24)$$

В качестве сигнала (12) для первичного поля (2) выберем функцию

$$\hat{A}_0(\omega) = \hat{s}_0(\omega - \omega_0), \quad \hat{s}_0(\omega) = E_0 \frac{2\pi}{\alpha} up\left(\frac{\omega}{\alpha}\right),$$

где E_0 – амплитуда электрического поля, $[E_0] = \frac{B}{M}$.

Используя обратное преобразование для (24), вычислим временной сигнал

$$s_0(t) = \frac{E_0}{\alpha} \int_{-\infty}^{\infty} up\left(\frac{\omega}{\alpha}\right) e^{-i\omega t} d\omega = E_0 Up(\alpha t),$$

тогда в соответствии с формулами (5), (16) при $p = 0$ следует

$$A_0(t) = E_0 e^{-i\omega_0 t} Up(\alpha t), \quad \vec{E}_0(t) = E_0 \sin(\omega_0 t) Up(\alpha t) \vec{Y}_1. \quad (25)$$

При этом огибающая, падающего на экран D осциллирующего сигнала (25), равна

$$T_0(t) = E_0 |Up(\alpha t)|. \quad (26)$$

Учитывая формулы (13), (19), вычислим коэффициенты формул (20)

$$\delta_k^{(0)} = E_0 Up(\pi k), \quad \beta_k = E_0 u_k, \quad \gamma_k = E_0 v_k,$$

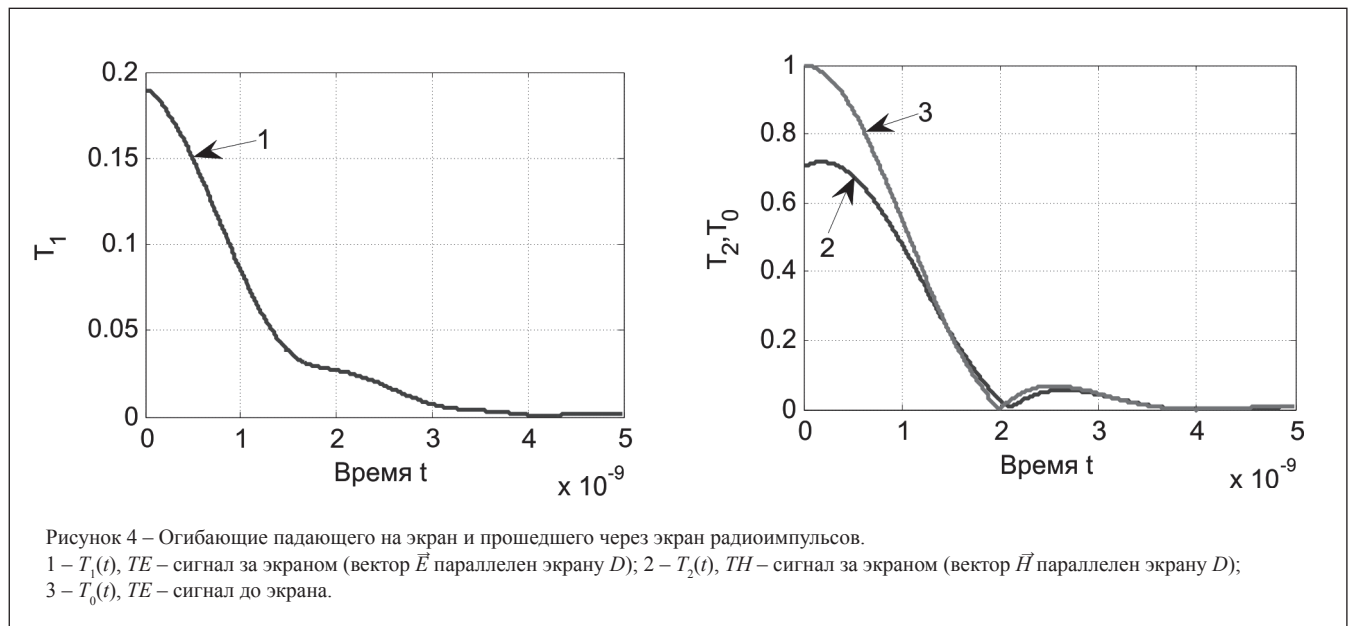
$$u_k = \sum_{m=-\infty}^{\infty} Up(\pi m) z_{k-m}, \quad v_k = \sum_{m=-\infty}^{\infty} Up(\pi m) y_{k-m}.$$

Электрическое поле, прошедшее в область D_2 , равно

$$\vec{E}_2 = i y_1(t-p) \vec{Y}_1 + y_2(t-p) \vec{Y}_2, \quad (27)$$

где

$$y_1(t) = E_0 e^{-i\omega_0 t} \sin(\alpha t) B_0^h(t), \quad y_2(t) = E_0 e^{-i\omega_0 t} \sin(\alpha t) B_0^g(t)$$



$$B_0^h(t) = \sum_{k=-\infty}^{\infty} \left(c_{1h} U p(\pi k) + \frac{i}{\pi} c_{2h} u_k + \frac{2}{\pi^2} c_{3h} v_k \right) \frac{(-1)^k}{\alpha t - \pi k}.$$

Огибающие осциллирующих сигналов, прошедших через экран D , для двух поляризаций определяются формулами

$$T_1(t) = E_0 |\sin(\alpha t) B_0^h(t)|, \quad T_2(t) = E_0 |\sin(\alpha t) B_0^g(t)|. \quad (28)$$

Численный пример

Численно исследована структура поля (27). Расчеты производились для параметров: $\alpha = \pi 10^9$ Гц, $\omega_0 = 6\pi 10^9$ Гц, $\Delta = 5$ см, $\epsilon = 4\epsilon_0$, $\mu = \mu_0$, $G = \frac{1+i}{2c}$, $Z = \frac{1-i}{2c}$.

$$\hat{B}_0 = 0, \quad \theta_0 = \frac{\pi}{4}, \quad \varphi_0 = 0, \quad E_0 = 1.$$

На рисунке 1 изображены графики линий (26), (28). Показано, что импульс (график 3), падающего под углом $\theta_0 = \frac{\pi}{4}$ на экран TE -поля, при прохождении через экран D разлагается на сумму двух импульсов. Носителем первого импульса (график 1) является TE -поле, носителем второго импульса – TH -поле, распространяющееся за экраном под углом $\theta_0 = \frac{\pi}{4}$. Для частоты $\omega_0 = 5,36\pi 10^9$ Гц величина $T_1(0)$ уменьшается и принимает значение 0,093. Заметим, что в работе [9] представлены графики для экрана с аналогичными параметрами в случае монохроматических полей.

Заключение

Построено аналитическое решение краевой задачи проникновения радиоимпульса с финитным спектром через биизотропный плоский слой. В качестве носителя сигнала выбрано электромагнитное поле, распространяющееся в пространстве и подчиняющееся уравнениям Максвелла, для которых сформулирована краевая задача дифракции. Методика решения задачи основана на использовании нелокальных граничных условий, связывающих поля по обе стороны экрана. Для представления узкополосного сигнала использовались атомарные функции и теорема Котельникова-Шеннона, позволяющие представить сигнал через дискретные временные отсчеты. Решение задачи реализовано численно и исследованы искажения и преобразование сигналов

при прохождении через экран.

Литература:

1. Виноградов, А.П. Электродинамика композитных материалов / А.П. Виноградов. – М.: Эдиториал УРСС, 2001. – 208 с.
2. Лагарьков, А.Н. Радиопоглощающие материалы на основе метаматериалов / А.Н. Лагарьков, В.Н. Кисель, В.Н. Семенов. – Радиотехника и электроника, 2012. – Т. 57, № 10. – С. 1119–1127.
3. Гуляев, Ю.В. Метаматериалы: фундаментальные исследования и перспективы применения / Ю.В. Гуляев, А.Н. Лагарьков, С.А. Никитов. – Вестник РАН, 2008. – Т. 78, № 5. – С. 438–457.
4. Кравченко, В.Ф. Лекции по теории атомарных функций и некоторым их приложениям / В.Ф. Кравченко. – М.: Радиотехника, 2003. – 510 с.
5. Кравченко, В.Ф. Алгебра логики, атомарные функции и вейвлеты в физических приложениях / В.Ф. Кравченко, В.Л. Рвачев. – М.: Физматлит, 2006. – 416 с.
6. Басараб, М.А. Аппроксимация финитными функциями и теорема Уиттекера-Котельникова-Шеннона в цифровой обработке сигналов / М.А. Басараб, Е.Г. Зелкин, В.Ф. Кравченко, В.П. Яковлев. – Успехи современной радиоэлектроники. – 2003, – № 9. – С. 3–36.
7. Ерофеев, В.Т. Аналитическое моделирование в электродинамике / В.Т. Ерофеев, И.С. Козловская. – Мн.: БГУ, 2010. – 303 с.
8. Князев, П.Н. Интегральные преобразования / П.Н. Князев. – Мн.: Высшая школа, 1969. – 198 с.
9. Ерофеев, В.Т. Дифракция плоской электромагнитной волны на плоском слое из биизотропного материала / В.Т. Ерофеев, С.В. Малый. – Вестник БГУ. Сер. 1. – 2010, № 2. – С. 11–16.
10. Баскаков, С.И. Радиотехнические цепи и сигналы / С.И. Баскаков. – М.: Высшая школа, 1988. – 448 с.

Abstract

The analytical solution of the boundary-value problem of penetration of a radioimpulse with finite spectrum through a flat biisotropic screen with arbitrary complex parameters of media is obtained. The impulse signal by means of atomic functions is presented. The results of computational experiment for concrete screen are investigated.

Поступила в редакцию 18.05.2013 г.

ОБ ОДНОМ ПОДХОДЕ К СТАТИСТИЧЕСКОМУ РАСПОЗНАВАНИЮ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

УДК 004.421.6: 519.237

В.Ю. Палуха, БГУ, Ю.С. Харин, НИИ ПМИ БГУ, г. Минск

Аннотация

Для решения задачи статистического распознавания криптографических генераторов по их выходным последовательностям разработан общий подход к построению информативных признаков. Описаны признаки на основе

энтропии и рангов матриц, построенные в соответствии с этим подходом. Приводятся результаты компьютерных экспериментов применения построенных информативных признаков для статистического распознавания прореживающего и самосжимающего генераторов.

Введение и постановка задачи

Современная криптография невозможна без случайных и псевдослучайных последовательностей $x_1, x_2, \dots \in V = \{0, 1\}$ [1]. Практическую значимость имеют генераторы последовательностей, близких по своим свойствам к равномерно распределенной случайной последовательности (РПС). Гипотезу о том, что выходная последовательность генератора $\{x_i\}$ является равномерно распределенной, будем обозначать $H_* = \{\{x_i\} \text{ есть РПС}\}$.

При проведении испытаний средств криптографической защиты информации [1] часто возникает задача статистического распознавания генераторов случайных и псевдослучайных последовательностей, т.е. задача отнесения (классификации) наблюдаемой выходной последовательности генератора $x_1, x_2, \dots \in V = \{0, 1\}$ некоторой конечной длительности T к одному из L ($2 \leq L < +\infty$) классов $\Omega_1, \dots, \Omega_L$. Генераторы могут быть разделены на классы $\{\Omega_i\}$ различными способами: физические и программные генераторы; программные генераторы различных типов; программные генераторы одного типа, но с различными параметрами; программные генераторы с одинаковыми параметрами, но с различной инициализирующей информацией. Описание основных типов генераторов можно найти в [1–3]. Данная статья посвящена задаче построения пространства информативных признаков для статистического распознавания криптографических генераторов.

Подход к построению информативных признаков генераторов

Будем предполагать, что выходная последовательность генератора $x_i \in V$ является случайной последовательностью на некотором вероятностном пространстве $(\Omega, \mathcal{C}, P)$. Разобьем последовательность $x_1, x_2, \dots, x_T$ на $l = \lfloor T/n \rfloor$ фрагментов (n -грамм) длины n $X^{(1)}, X^{(2)}, \dots, X^{(l)}, X^{(k)} = (x_{(k-1)n+1}, \dots, x_{kn}) \in V^n$. Пусть наблюдается некоторая статистика $a_k(n) = f(X^{(k)})$, $k = 1, 2, \dots, l$, при различных длинах фрагмента $n \in [n_-, n_+]$, $1 \leq n_- < n_+$; $a_*(n) = E_H \{a_k(n)\}$ – математическое ожидание этой статистики при истинной гипотезе H_* ; $a(n)$ – наблюдаемое выборочное среднее значение статистики: $a(n) = \frac{1}{l} \sum_{k=1}^l a_k(n)$. В качестве признака предлагается использовать уклонение статистики $a(n)$ от математического ожидания в l_p -метрике ($p \in \mathbb{N}$):

$$\rho^{(p)} = \frac{1}{n_+ - n_- + 1} \sqrt[p]{\sum_{n=n_-}^{n_+} |a(n) - a_*(n)|^p}. \quad (1)$$

Нелинейные признаки на основе энтропии

Пусть $p_{i_1, \dots, i_n} = P\{x_{t+1} = i_1, \dots, x_{t+n} = i_n\}$ – распределение вероятностей n -граммы $(x_{t+1}, \dots, x_{t+n}) \in V_n$, которое предполагается не зависящим от $t \in \mathbb{N}$. Многомерная (n -мерная) энтропия Шеннона для фрагмента длины n равна [1]:

$$h(n) = - \sum_{i_1, \dots, i_n} p_{i_1, \dots, i_n} \ln p_{i_1, \dots, i_n}. \quad (2)$$

Теорема 1. Если справедлива гипотеза H_* , то

$$h_*(n) = h(n)|_{H_*} = n \ln 2 = nh_*(1). \quad (3)$$

Используя подстановочный принцип, построим оценку энтропии (2):

$$\hat{h}(n) = - \sum_{i_1, \dots, i_n} \hat{p}_{i_1, \dots, i_n} \ln \hat{p}_{i_1, \dots, i_n}. \quad (4)$$

На основании статистик $\{\hat{h}(n) : n_- \leq n \leq n_+\}$, вычисленных по (4), и математического ожидания (3) построим информативные признаки согласно (1):

$$\rho^{(p)} = \frac{1}{n_+ - n_- + 1} \sqrt[p]{\sum_{n=n_-}^{n_+} |\hat{h}(n) - h_*(n)|^p}. \quad (5)$$

Нелинейные признаки на основе рангов матриц

Разбиваем наблюдаемый ряд $x_1, x_2, \dots$ на фрагменты $X^{(1)}, X^{(2)}, \dots \in V^{n^2}$ длины n^2 : $X^{(k)} = (x_{(k-1)n^2+1}, \dots, x_{kn^2})$. Используя k -й фрагмент $X^{(k)} = (x_1^{(k)}, \dots, x_{n^2}^{(k)}) \in V^{n^2}$ выходной последовательности, построим $(n \times n)$ -матрицу

$$A^{(k)} = (a_{ij}^{(k)}) = \begin{pmatrix} x_1^{(k)} & \dots & x_n^{(k)} \\ \dots & \dots & \dots \\ x_{(n-1)n+1}^{(k)} & \dots & x_{nn}^{(k)} \end{pmatrix} \in V^{n \times n}. \quad (6)$$

Ранг этой матрицы отражает наличие функциональной зависимости в последовательности. Если $\text{rank}(A^{(k)}) = r < n$, то в матрице $A^{(k)}$ имеется $n - r$ линейно зависимых над V_n строк. Поэтому в качестве признака для фрагмента $X^{(k)}$ будем использовать ранг матрицы (6) $r^{(k)} = \text{rank}(A^{(k)}) \in \{0, 1, \dots, \min\{n, N\}\}$. Пусть наблюдается l фрагментов, т.е. $T = l \cdot N^2$. Определим статистику

$$v(n) = \frac{1}{nl} \sum_{k=1}^l r^{(k)}, \quad (7)$$

имеющую смысл среднего относительного ранга.

Теорема 2. При верной гипотезе H_* математическое ожидание статистики (7) имеет вид:

$$E_{H_*} \{v(n)\} = v_*(n) = \frac{1}{n} \sum_{j=0}^n q_{nj} j, \quad (8)$$

где $q_{nj} = P_{H_0} \{r^{(k)} = j\} = 2^{j(2n-j)-n^2} \prod_{i=0}^{j-1} \frac{(1-2^{i-n})^2}{1-2^{i-j}}$,

$$j \in \{0, 1, \dots, n\}.$$

На основании статистик $\{v(n) : n_- \leq n \leq n_+\}$ и математического ожидания (8) построим информативные признаки согласно (1):

$$\rho^{(p)} = \frac{1}{n_+ - n_- + 1} \sqrt[p]{\sum_{n=n_-}^{n_+} |v(n) - v_*(n)|^p}. \quad (9)$$

Решающее правило

Пусть указанными выше методами построено пространство из M информативных признаков $p = (p_1, \dots, p_M) \in \mathbf{R}^M$. Опишем применение метода дискриминантного анализа [4] для решения задачи распознавания в случае двух равновероятных классов. Пусть по входной последовательности построен вектор признаков p и имеется $m_i > M$

обучающих реализаций $\rho_1^{(i)}, \dots, \rho_{m_i}^{(i)} \in \mathbf{R}^M$, принадлежащих классу Ω_i , $i \in \{1, 2\}$. Построим оценки математического ожидания вектора признаков и ковариационной матрицы для каждого из классов. Оценка для математического ожидания в классе Ω_i есть выборочное среднее:

$$\hat{\mu}_i = \frac{1}{m_i} \sum_{m=1}^{m_i} \rho_m^{(i)}, \quad (10)$$

а оценка для ковариационной матрицы – выборочная ковариационная матрица:

$$\hat{\Sigma}_i = \frac{1}{m_i - 1} \sum_{m=1}^{m_i} (\rho_m^{(i)} - \hat{\mu}_i)(\rho_m^{(i)} - \hat{\mu}_i)'. \quad (11)$$

Байесовское решающее правило имеет вид [4]:

$$d = d_0(\rho) = \arg \min_{i \in \{1, 2\}} (\ln |\hat{\Sigma}_i| + (\rho - \hat{\mu}_i)' \hat{\Sigma}_i^{-1} (\rho - \hat{\mu}_i)), \quad \rho \in \square^M, \quad (12)$$

где оценки $\hat{\mu}_i$ и $\hat{\Sigma}_i$ вычисляются по формулам (10) и (11) соответственно.

Результаты компьютерных экспериментов

Проведены две серии компьютерных экспериментов.

Серия 1. Пусть Ω_1 и Ω_2 – самосжимающиеся генераторы с различными характеристическими примитивными многочленами порождающего регистра сдвига. Описание самосжимающегося генератора приведено в [5].

В качестве признака ρ используется значение статистики (5). Заданы параметры:

$n_- = 1$, $n_+ = 20$, $p = 1$. В результате применения решающего правила (12) получена оценка безусловной вероятности ошибки 0,22.

Серия 2. Пусть Ω_1 – прореживающий генератор, Ω_2 – самосжимающийся генератор. Описание прореживающего генератора приведено в [6].

В качестве признака ρ используется значение статистики (9). Заданы параметры

$n_- = 1$, $n_+ = 2236$, $p = 1$. Можно применить метод дискриминантного анализа, описанный выше. Однако можно применить более простое линейное решающее правило. Эксперимент дает оценку безусловной вероятности ошибки, равную 0.

Заключение

Для решения актуальной задачи распознавания криптографических генераторов разработан общий подход к построению информативных признаков. Этот подход учитывает динамику изменения вероятностных характеристик генераторов при изменении длины используемого фрагмента. Построенные согласно этому подходу признаки универсальны, т.к. не используют специфических свойств генераторов, и поэтому их можно применять для распознавания различных типов генераторов. Проиллюстрировано применение одного из признаков для распознавания прореживающего и самосжимающегося генераторов, и другого – для распознавания самосжимающихся генераторов с различными параметрами.

Литература:

1. Харин, Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин [и др.]. – Минск: Новое знание, 2003. – 382 с.

2. Харин, Ю.С. Проблемы математики и информатики в области защиты информации / Ю.С. Харин // Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-матэматычных навук. – 2007. – № 4. – С. 84–95.

3. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – Москва: КУДИЦ-ОБРАЗ, 2003. – 240 с.

4. Харин, Ю.С. Математическая и прикладная статистика / Ю.С. Харин, Е.Е. Жук. – Минск: БГУ, 2004. – 272 с.

5. Meier, W. Analysis of pseudo random sequences generated by cellular automata / W. Meier, O. Staffelbach // D.W. Davies, editor, Advances in Cryptology / Eurocrypt '91, Springer-Verlag, Berlin, 1992. – P. 186 – 199.

6. Coppersmith, D. The shrinking generator / D. Coppersmith, Y. Krawchuk, Y. Mansour // Advanced in Cryptology: Proceedings of Crypto 93, LNCS 773. – 1994. – P. 22 – 39.

Abstract

An approach to construction of informative features is proposed to solve the problem of statistical recognition of cryptographic generators by output sequences. Features based on entropy and ranks of matrices and constructed in accordance to this approach are described. The results of computer experiments on recognition of shrinking and self-pressed generators are presented.

Поступила в редакцию 18.05.2013 г.



тел. +375 17 287 85 66
факс +375 17 287 85 65
тел. моб. +375 29 684 43 09
220068, г. Минск, ул. Некрасова, 114,
оф. 238, 2 этаж, e-mail: info@belplata.by

Разработка и поставка печатных плат:
любой класс точности, широкий спектр покрытий, изготовление образцов от 5 дней.

Поставка фотошаблонов

Поставка трафаретов:
из нержавеющей стали и латуни.

Материалы для печатных плат:
защитные маски, маркировочные краски, фоторезисты, паяльные пасты.

Поставка изделий из феррита:
любые виды сердечников CI, EE, EEM, EP, EER, ETD, EC, EF, ED, EFD, EI, EPO, EPX, EPC и т.д.

Поставка электронных компонентов:
STMicroelectronics, NXP Semiconductors, Vishay, Holtek Semiconductor.

www.belplata.by

О НЕАВТОНОМНЫХ ДВОИЧНЫХ РЕГИСТРАХ СДВИГА, ОБЛАДАЮЩИХ СВОЙСТВОМ СИНХРОНИЗАЦИИ¹

УДК: 519.7

О.А. Логачев, С.В. Смышляев,
МГУ имени М.В. Ломоносова, г. Москва

Аннотация

Работа посвящена свойству локального обращения проходного двоичного регистра сдвига с фильтрующей булевой функцией и связанным свойствам. Известно, что существование эффекта локального обращения для двоичного регистра сдвига с фильтрующей функцией, линейной по последней переменной (т.е. совершенно уравновешенной функцией с правым барьером длины 1) эквивалентно существованию синхронизирующего входного слова для соответствующего неавтономного регистра сдвига с функцией обратной связи, полученной из фильтрующей функции фиксацией нулем ее последней переменной. В настоящей работе исследуются некоторые классы булевых функций, для которых соответствующие неавтономные регистры сдвига обладают синхронизирующими словами (в некоторых работах близкие аналоги синхронизирующего слова называются установочным, корректирующим или возвратным словами). Получены критерии наличия у функции синхронизирующего свойства. Описан ряд классов функций, обладающих синхронизирующим свойством. Показано, что по любому классу функций с синхронизирующим свойством от $n-1$ переменных возможно построить класс совершенно уравновешенных булевых функций с левым барьером без правого барьера от n переменных.

Введение

В работе [1] рассматривался эффект локального обращения проходного двоичного регистра сдвига с фильтрующей булевой функцией. В частности, было показано, что существование эффекта локального обращения для двоичного регистра сдвига с фильтрующей функцией линейной по последней переменной (т.е. совершенно уравновешенной функцией с правым барьером длины, см. [2, 7]) эквивалентно существованию синхронизирующего входного слова для соответствующего неавтономного регистра сдвига с функцией обратной связи, полученной из фильтрующей функции фиксацией нулем ее последней переменной. В настоящей работе исследуются некоторые классы булевых функций, для которых соответствующие неавтономные регистры сдвига обладают синхронизирующими словами. В некоторых работах (см. [3, 4] и др.) близкие аналоги синхронизирующего слова называются установочным, корректирующим или возвратным словами.

Основная часть

Пусть F_2 – поле из двух элементов и N – множество натуральных чисел. Для $n \in N$ будем обозначать через V_n пространство наборов $x = (x_1, x_2, \dots, x_n)$ длины n с компонентами из F_2 , а через $\mathcal{F}_n$ – множество всех булевых функций от n переменных. Для некоторых наборов из V_n будем использовать специальные обозначения: $0^n = (0, 0, \dots, 0)$ и $1^n = (1, 1, \dots, 1)$. Основным объектом исследования в данной

работе будет неавтономный двоичный регистр сдвига с функцией обратной связи f из $\mathcal{F}_n$ (см. рис. 1; « $\oplus$ » – сложение по $\text{mod } 2$), обозначаемый далее $NSR(f)$.

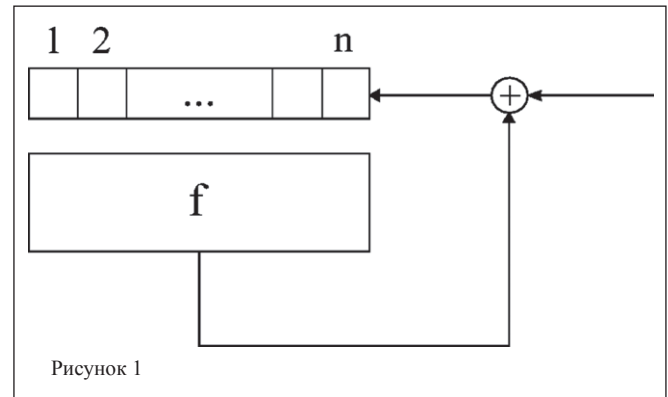


Рисунок 1

Регистр $NSR(f)$ является конечным автоматом без выхода, входной алфавит которого совпадает с F_2 , а внутренний (множество состояний) – с V_n . Функция переходов автомата $\delta^f : V_n \times F_2 \rightarrow V_n$ задается соотношением:

$$\delta^f(x, \epsilon) = \delta_\epsilon^f(x) = (x_2, \dots, x_n, \epsilon \oplus f(x_1, \dots, x_n)), \quad (1)$$

где $x \in V_n$, $\epsilon \in F_2$. Естественным образом это отображение может быть продолжено до отображения, соответствующего произвольному набору $u \in V_n$. Если $u = (u_1, u_2, \dots, u_l)$, то

$$\delta^f(x, u) = \delta_u^f(x) = \delta_{u_l}^f(\dots \delta_{u_2}^f(\delta_{u_1}^f(x)) \dots).$$

Определение 1. Пусть $f \in \mathcal{F}_n$. Будем говорить, что функция f обладает синхронизирующим свойством, а регистр $NSR(f)$ обладает синхронизирующим входным словом, если существует $l \in N$, $y \in V_l$ и $z = z(y) \in V_n$ такие, что

$$\delta_y^f(x) = z = z(y)$$

для любого $x \in V_n$.

Множество функций из $\mathcal{F}_n$, обладающих синхронизирующим свойством и существенно зависящих от крайних переменных, будем обозначать $\mathcal{F}_n^{sync}$. Очевидно, что $\mathcal{F} \setminus \mathcal{F}_n^{sync} \neq \emptyset$. Приведем некоторые примеры функций из этого множества.

Пример 2. Пусть $f \in \mathcal{F}_n$ и $f(x \oplus 1^n) = f(x) \oplus 1$, т.е. функция f – самодвойственная. Тогда для пары векторов $\{x, x \oplus 1^n\}$, $x \in V_n$ и любых $l \in N$, $y \in V_l$ имеем

$$\delta_y^f \neq \delta_y^f(x \oplus 1^n).$$

Следовательно, $f \in \mathcal{F}_n \setminus \mathcal{F}_n^{sync}$.

Пример 3. Пусть $f \in \mathcal{F}_n$ и $f(x \oplus e_1) \oplus f(x) = 1$, т.е. функция f линейна по первой переменной ($e_j = (0, \dots, 0, 1, 0, \dots, 0)$, $j = 1, 2, \dots, n$). Тогда

¹ Работа поддержана Российским фондом фундаментальных исследований (номера проектов 12-01-00680-а, 13-01-00183-а).

отображение $\delta_y^f : V_n \mapsto V_n$ при любом входном наборе $\mathbf{Y}$ является взаимно однозначным. Следовательно, $f \in \mathcal{F}_n \setminus \mathcal{F}_n^{sync}$.

Определение 4. Пусть $f \in \mathcal{F}$. Графом $G^f = (U, E)$ регистра $NSR(f)$ будем называть ориентированный граф с множеством вершин $U = V_n \times V_n$ и множеством ориентированных ребер $E = \{e\}$, $e = ((\mathbf{u}, \mathbf{v}), (\mathbf{u}', \mathbf{v}'))$, где $(\mathbf{u}, \mathbf{v}) \in U$, $(\mathbf{u}', \mathbf{v}') \in U$ и $\delta_e^f(\mathbf{u}) = \mathbf{u}'$, $\delta_e^f(\mathbf{v}) = \mathbf{v}'$ для некоторого $e \in F_2$. При этом $i(e) = (\mathbf{u}, \mathbf{v})$ – начальная вершина ребра e , а $t(e) = (\mathbf{u}', \mathbf{v}')$ – конечная вершина этого ребра.

Для множества вершин U графа G^f через $diag U$ будем обозначать множество вершин этого графа вида $(\mathbf{u}, \mathbf{u})$, $\mathbf{u} \in V_n$.

Определение 5. Пусть $f \in \mathcal{F}_n$. Полугруппой S^f регистра $NSR(f)$ будем называть полугруппу, порожденную частичными функциями переходов δ_0^f, δ_1^f этого автомата, т.е. $S^f = \langle \delta_0^f, \delta_1^f \rangle$.

Тогда справедливы следующие утверждения.

Предложение 6. Функция $f \in \mathcal{F}_n$ обладает синхронизирующим свойством тогда и только тогда, когда для любой вершины $(\mathbf{u}, \mathbf{v}) \in U$, $\mathbf{u} \neq \mathbf{v}$ существуют натуральное m и путь $\pi = (e_1, e_2, \dots, e_m)$, $e_i \in E$, $i = 1, \dots, m$ в графе G^f такой, что $i(e_1) = (\mathbf{u}, \mathbf{v})$ и $t(e_m) \in diag U$.

Предложение 7. Функция $f \in \mathcal{F}_n$ обладает синхронизирующим свойством тогда и только тогда, когда полугруппа S^f содержит отображение-константу из $diag U$.

Для произвольной функции f из $\mathcal{F}_n^{sync}$ определим величину $l(f)$ как минимальную длину синхронизирующей последовательности регистра $NSR(f)$.

Для множества $\mathcal{F}_n^{sync}$ рассмотрим следующую величину:

$$l_{\min}(n) = \min_{f \in \mathcal{F}_n^{sync}} l(f).$$

Лемма 8. Для любого $n \in \mathbb{N}$, $n \geq 2$ выполнено неравенство $l_{\min}(n) \leq n + 1$.

Теорема 9. $l_{\min}(n) = n + 1$.

Рассмотрим некоторые примеры функций — представителей класса монотонных булевых функций.

Лемма 10. Пусть $n \in \mathbb{N}$. Тогда

1°, если n – четное, то функция

$$f(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } \sum_{i=1}^n x_i \leq \frac{n}{2} \\ 1, & \text{если } \sum_{i=1}^n x_i > \frac{n}{2} \end{cases}$$

обладает синхронизирующим свойством;

2°, если n – нечетное, то функция

$$g(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } \sum_{i=1}^n x_i \leq \frac{n-1}{2} \\ 1, & \text{если } \sum_{i=1}^n x_i \geq \frac{n+1}{2} \end{cases}$$

не обладает синхронизирующим свойством.

Обозначим через $\mathcal{E}_n$ множество функций из $\mathcal{F}_n$, существенно зависящих от всех переменных, многочлены Жегалкина которых содержат только мономы степени большей, чем $\lfloor \frac{n}{2} \rfloor$, а также мономы вида $x_1 x_{j_1} x_{j_2} \dots x_{j_k}$, где $1 \leq k \leq n - \lfloor \frac{n}{2} \rfloor$ и $\{j_1, j_2, \dots, j_k\} \subseteq \{\lfloor \frac{n}{2} \rfloor + 1, \dots, n\}$.

Лемма 11. Функции из множества $\mathcal{E}_n$ обладают синхронизирующим свойством.

Пример 12. Обозначим через $\mathcal{L}_n$ – множество бесповторных функций из $\mathcal{F}_n$, т.е. функций существенно зависящих от всех переменных, у которых каждая переменная входит

только в один моном соответствующего многочлена Жегалкина. В это множество входят как функции из $\mathcal{F}_n^{sync}$, так и функции из $\mathcal{F}_n \setminus \mathcal{F}_n^{sync}$.

Функция $f(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ не обладает синхронизирующим свойством (см. Пример).

Функция $f(x_1, \dots, x_n) = x_1 x_2 \oplus x_3 x_4 \oplus \dots \oplus x_{n-1} x_n$, где n – четное, обладает синхронизирующим свойством. Необходимо отметить, что данная функция является представителем еще одного интересного множества бент-функций, связанного с комбинаторикой и криптографией (см. [9]). Для того, чтобы доказать синхронизирующее свойство этой функции, нам потребуется ввести еще одно множество булевых функций (см. Лемму).

Определим подмножество Q_n множества $\mathcal{F}_n$. Функция f из $\mathcal{F}_n$, существенно зависящая от всех своих переменных, принадлежит Q_n тогда и только тогда, когда многочлен Жегалкина этой функции содержит только мономы степени не менее 2, для каждого из которых существует $j \in \{1, \dots, n\}$ такое, что соответствующий моном имеет вид $x^{\mathbf{u}} = x_1^{u_1} \cdot \dots \cdot x_n^{u_n}$, где $u_j = u_{j+1} = 1$ или $u_{j-1} = u_j = 1$.

Лемма 13. Любая функция из множества Q_n обладает синхронизирующим свойством.

Заметим, что все функции, полученные фиксацией первой переменной нулем из функций описанного в работе [5] класса совершенно уравновешенных булевых функций без правого барьера, лежат в объединении множеств Q_n , $n = 1, 2, \dots$. Связь между такими свойствами функций, как совершенная уравновешенность и наличие барьера (см. [2, 6, 7]), и синхронизирующим свойством представляется интересной темой для будущих исследований.

Доказано следующее утверждение, позволяющее по всякому классу функций с синхронизирующим свойством строить класс совершенно уравновешенных булевых функций без правого барьера.

Теорема 14. Пусть $f(x_1, x_2, \dots, x_n) = x_1 \oplus g(x_2, x_3, \dots, x_n)$. Если g отлична от константы и обладает синхронизирующим свойством, то f не имеет правого барьера.

Таким образом, всякому классу функций с синхронизирующим свойством от $n-1$ переменных соответствует класс совершенно уравновешенных булевых функций с левым барьером без правого барьера от n переменных. Как показано в работе [8], по данному классу, в свою очередь, можно построить класс совершенно уравновешенных функций без барьера от $n+2$ переменных той же мощности.

Заключение

Получены критерии наличия у функции синхронизирующего свойства. Описан ряд классов функций, обладающих синхронизирующим свойством. Показано, что по любому классу функций с синхронизирующим свойством от $n-1$ переменных возможно построить класс совершенно уравновешенных булевых функций с левым барьером без правого барьера от n переменных.

Литература:

1. Логачев, О.А. О локальной обратимости одного класса булевых отображений // Материалы IX Международного Семинара «Дискретная математика и ее приложения». – М.: МГУ, 2007. – С. 440–442.
2. Логачев, О.А. Новые методы изучения совершенно уравновешенных булевых функций / О.А. Логачев,

С.В. Смышляев, В.В. Яценко // Дискретная математика. – Т. 21, Вып. 2. – 2009. – С. 51–74.

3. Клосс, Б.Б. Некоторые свойства помехоустойчивых автоматов // Кибернетика. – №1. – 1988. – С. 10–15.

4. Рысцов, И.К. Возвратные слова для разрешимых автоматов // Кибернетика и системный анализ. – №6. – 1994. – С. 21–26.

5. Смышляев, С.В. О некоторых свойствах совершенно уравновешенных булевых функций // Материалы Четвертой Международной Научной Конференции по Проблемам Безопасности и Противодействия Терроризму. МГУ имени М.В. Ломоносова, Москва, 30–31 октября 2008 года. МЦНМО. – М.: 2009. – С. 57–64.

6. Смышляев, С.В. О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. – Вып. 1(7). – 2010. – С. 5–15.

7. Смышляев, С.В. Барьеры совершенно уравновешенных булевых функций // Дискретная математика. – Т. 22. – Вып. 2. – 2010. – С. 66–79.

8. Смышляев, С.В. Построение классов совершенно уравновешенных булевых функций без барьера // Прикладная дискретная математика. – Вып. 3(9). – 2010. – С. 41–50.

9. Rothaus, O.S. On «Bent» Functions // Journal of Combinatorial Theory (A). – V. 20, No.3. – 1976. – P. 300–305.

Abstract

The current paper is dedicated to the property of local invertibility of binary shift registers with filter functions and related properties. It is known that local invertibility for binary shift register with filter function that is linear in the last variable (i.e. is perfectly balanced function with right barrier of length 1) is equivalent to existence of synchronizing tuple for the corresponding non-autonomous shift register with feedback, derived from the filter function by fixation its last variable with 0. In the current paper we study certain classes of Boolean functions for which the corresponding non-autonomous shift registers have synchronizing tuples. New criteria of having synchronization property are obtained and new classes of such functions are described. It is shown that every class of functions with synchronization property of $n-1$ variables can be used to construct a class of perfectly balanced functions of n variables with left barrier and without right barrier.

Поступила в редакцию 18.05.2013 г.

МЕХАНИЗМ СИНХРОНИЗАЦИИ ВЕСОВЫХ КОЭФФИЦИЕНТОВ В ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЯХ КИНЦЕЛЯ И ПРОБЛЕМЫ БЕЗОПАСНОСТИ

УДК 621.391.25

В.Ф. Голиков, Н.В. Брич,
БНТУ, г. Минск

Аннотация

И. Кантер и В. Кинцель предлагают использовать синхронизируемые искусственные нейронные сети в качестве решения задачи по формированию общего секретного ключа, не требующего личной встречи и использования сложных математических алгоритмов. Авторы статьи полагают, что подход нуждается в более глубоких исследованиях, подтверждающих сходимость процесса синхронизации. Моделирование основных типов атак подтверждает предположение об уязвимости модели. В статье проанализировано влияние начальных значений весовых коэффициентов двух сетей на скорость достижения синхронности ИНС. Выявлено положительное свойство – равновероятность направлений движения начальных значений весовых коэффициентов. На основе проведенного исследования авторами предполагается возможность по совершенствованию архитектуры сети и алгоритма коррекции весовых коэффициентов.

Введение

Проблема формирования секретного криптографического ключа с использованием открытого канала связи чаще всего решается в настоящее время применением односторонних функций. Вместе с тем идет поиск альтернативных способов.

Для формирования общего секретного ключа И. Кантер и В. Кинцель предлагают использовать синхронизируемые

искусственные нейронные сети (ИНС) [1, 2]. В результате обучения две нейронные сети становятся точным отражением друг друга, а весовые коэффициенты сетей могут выполнять роль секретного ключа.

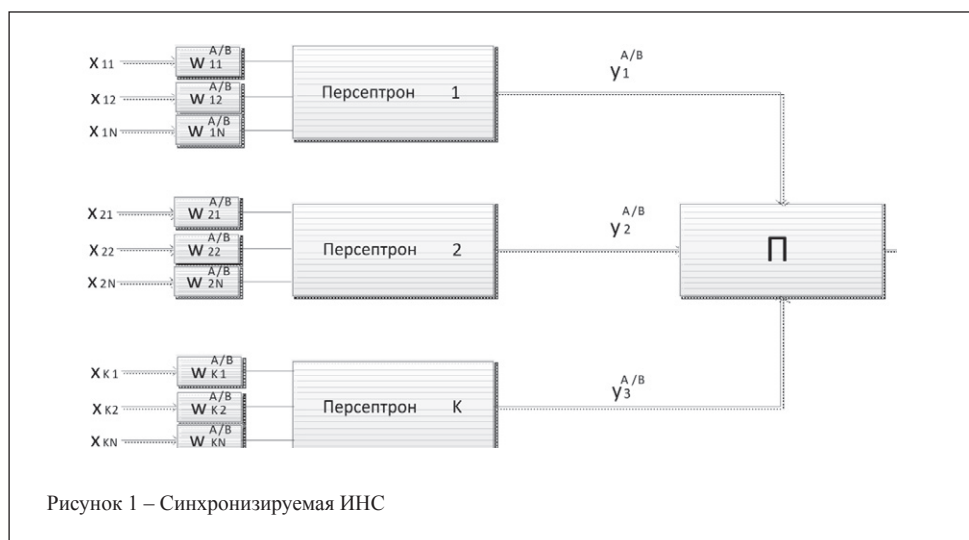
Цель работы – проанализировать механизм синхронизации коэффициентов двух сетей и проблемы безопасности формируемого ключа.

1 Основные сведения об архитектуре ИНС

Архитектура на стороне отправителя и получателя представляет собой двуслойный персептрон (ТРМ-архитектура), состоящий из K внутренних персептронов, каждый из которых имеет N входов (рисунок 1). Значения дискретной входной величины с равномерным распределением обозначено как $x_{kj} = \pm 1$, где $k = 1, 2, \dots, K$, $j = 1, 2, \dots, N$. Значение на выходе k -го внутреннего персептрона отправителя (получателя) обозначено как y_k^A (y_k^B). Индекс $\frac{A}{B}$ означает, что операция касается обеих сетей A и B , а единичный индекс – что операция касается одной сети соответственно. Выходная величина O каждой ИНС:

$$O^{\frac{A}{B}} = \prod_{k=1}^K y_k^{\frac{A}{B}} = \prod_{k=1}^K \sigma(\alpha_k^{\frac{A}{B}}) = \prod_{k=1}^K \sigma\left(\sum_{j=1}^N w_{kj}^{\frac{A}{B}} x_{kj}\right),$$

где $w_{kj}^{\frac{A}{B}}$ – вектор весовых коэффициентов сети; $\sigma(\alpha_k^{\frac{A}{B}})$ – модифицированная функция знака.



Модифицированная функция знака

$$\sigma(\alpha_k^{A/B}) = \begin{cases} 1, & \sigma(\alpha_k^{A/B}) \geq 0, \\ -1, & \sigma(\alpha_k^{A/B}) < 0. \end{cases}$$

Если выходы обеих сетей идентичны, то векторы весов тех персептронов, для которых $(Z^{A/B} \cdot y_k^{A/B}) > 0$, производят шаг в следующем направлении

$$w_{kj}^{A/B}[i+1] = w_{kj}^{A/B}[i] + x_{kj}[i] \cdot o^{A/B}[i].$$

Если $|w_{kj}^{A/B}| > L$, тогда $w_{kj}^{A/B} = L$ с соответствующим знаком.

Таким образом, параметры K, L, N являются несекретными. Секретными являются значения весов $w_{kj}^{A/B}$. В процессе синхронизации по открытому каналу передаются только значения входного вектора и выходных значений $O^{A/B}$.

На первый взгляд, алгоритм эффективен. Во-первых, одному выходному значению $O^{A/B}$ соответствует четыре комбинации выходных значений внутренних персептронов $y_k^{A/B}$. Во-вторых, конкретное $y_k^{A/B}$ может быть сформировано из нескольких комбинаций весов $w_{kj}^{A/B}$. В-третьих, корреляция между значениями весов и выходным значением $O^{A/B}$ уменьшается также благо-

даря наличию ограничения L . Таким образом, злоумышленник не может однозначно определить значения весов персептронов легитимных пользователей. Однако подход обладает некоторыми уязвимостями, на основании которых разработано несколько типов атак – с использованием одной ИНС (методом грубой силы, геометрическая) и с использованием нескольких ИНС.

2 Атака методом грубой силы

В случае простой атаки (атаки методом грубой силы)

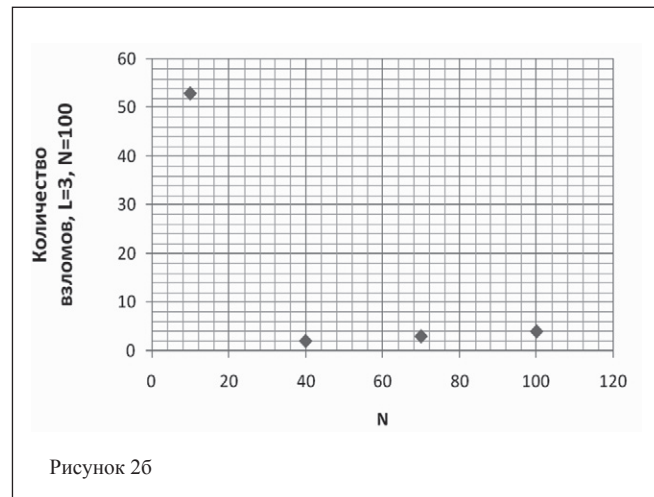
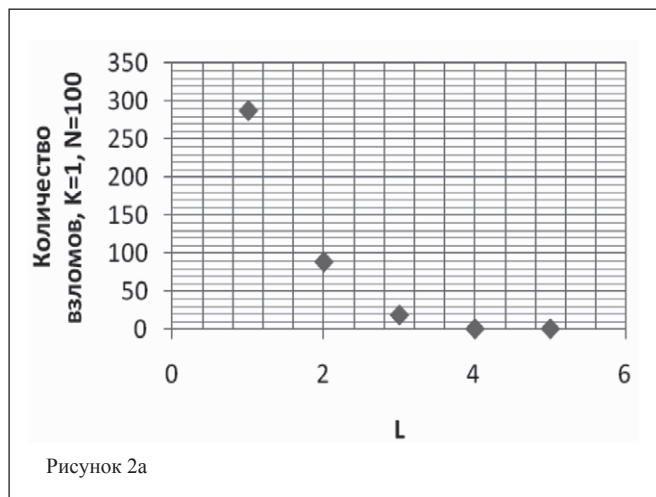
злоумышленник E знает значения входного вектора x_{ij} , выходов $O^{A/B}$ на каждом шаге обучения; использует то же правило обучения, что и легитимный отправитель A (однако вместо значения O^E использует O^A). Подход неэффективен, поскольку достаточным условием $O^A = O^E$ является ситуация, когда совпадает количество четных и нечетных выходных значений каждого персептрона, но необязательно соответственно.

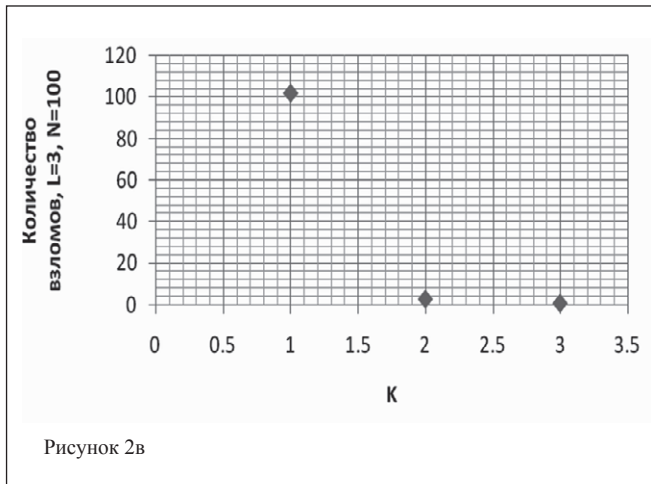
Для изучения особенностей сетей Кинцеля была разработана имитационная модель (консольное приложение) на языке высокого уровня Python 3.2. Приложение позволяет анализировать свойства ИНС и моделировать основные типы атак.

В рамках моделирования проведено 3000 испытаний. Установлено:

1) Действительно, после вхождения двух ИНС в синхронизм, весовые коэффициенты на приемной и передающей сторонах полностью совпадают при всех последующих циклах (проверено для 50 циклов синхронизации после вхождения ИНС в синхронизм).

2) Известно, что среднее время синхронизации зависит от характера входной последовательности x_{kj} , весовых коэффициентов $w_{kj}^{A/B}$, диапазона весов (значения

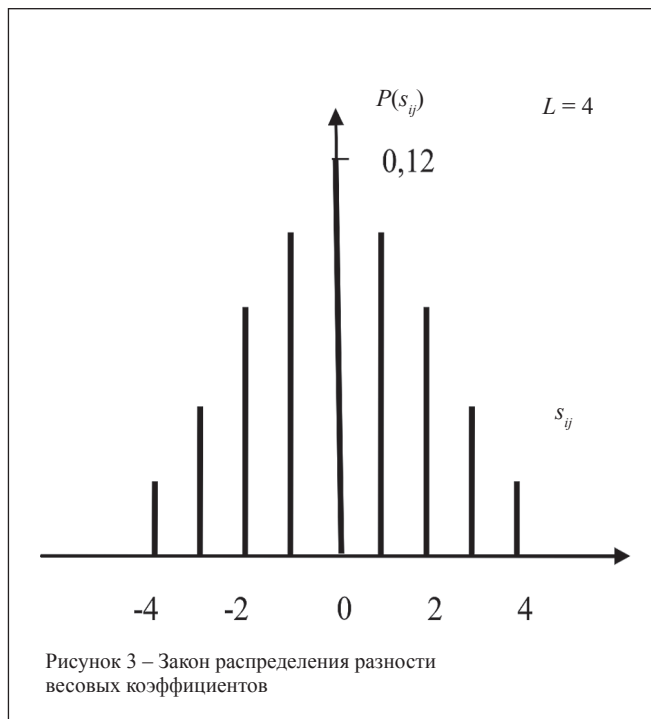




L), количества персептронов K и количества входов для одного персептрона N . В результате моделирования (рисунки 2а, 2б, 2в) установлено, что простая атака является наиболее эффективной при минимальных значениях параметров K, N, L . При увеличении параметров K, N, L атака становится менее эффективной, однако все равно возможна ситуация, при которой обучение ИНС легитимных пользователей длится дольше, чем обучение ИНС злоумышленника $\tau_{learning}^{AE} \leq \tau_{learning}^{AB}$.

3 Исследование вероятностных свойств начальных значений весовых коэффициентов

До начала синхронизации абоненты должны сформировать вектор весовых коэффициентов w , где $w_{ij} \in [-L, L]$, $i = 1, 2, \dots, K; j = 1, 2, \dots, N$. Величину L целесообразно выбирать как 2^q , где q - целое положительное число. Каждый элемент вектора w абонента A - случайное целое число с равномерным законом распределения:



$$P(w_{ij} = sa_{ij}) = \frac{1}{2L+1}, \text{ где } sa_{ij} = -L, -L+1, \dots, 0, 1, \dots, L. \quad (4)$$

Введем в рассмотрение случайную величину начального рассогласования соответствующих весовых коэффициентов сетей $\partial_{ij} = wa_{ij} - wb_{ij}$, закон распределения которой

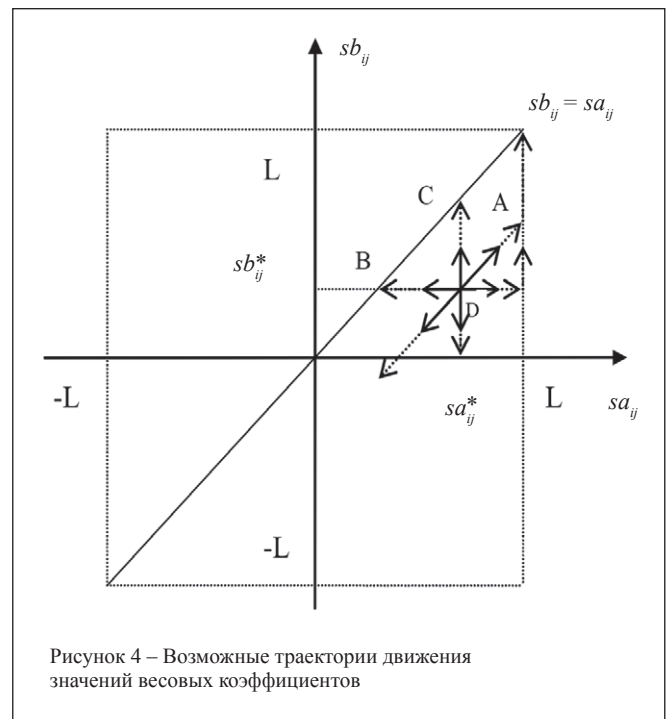
$$P(\partial_{ij} = s_{ij}) = \sum_{sa_{ij}, sb_{ij} \in \{s_{ij} = sa_{ij} - sb_{ij}\}} P(wa_{ij} = sa_{ij}; wb_{ij} = sb_{ij}) \quad (5)$$

Поскольку все значения wa_{ij}, wb_{ij} равновероятны, то для нахождения $P(\partial_{ij} = s_{ij})$ достаточно определить количество значений пар (sa_{ij}, sb_{ij}) , соответствующих каждому возможному значению s_{ij}

$$P(\partial_{ij} = s_{ij}) = \frac{2L+1 + ABS(s_{ij})}{(2L+1)^2} \quad (6)$$

где $ABS(s_{ij})$ - абсолютное значение величины s_{ij} , $s_{ij} \in [-2L, 2L]$. Зависимость (6) изображена на рисунке 3. Из этого рисунка видно, что наибольшей вероятностью обладают совпадающие значения коэффициентов: примерно - 0,12 и значения, отличающиеся на 1, примерно - 0,16. Всего в интервале различий $[-2, 2]$ лежит до 40 % весовых коэффициентов. Следует ожидать, что именно эти коэффициенты в процессе синхронизации будут согласовываться быстрее остальных. Рассмотрим теперь некоторые вероятностные характеристики процесса синхронизации. Нанесем на плоскость (sa_{ij}, sb_{ij}) случайную точку (sa_{ij}^*, sb_{ij}^*) (рисунок 4) и зная правило коррекции весовых коэффициентов, проследим возможные траектории ее движения к полному согласованию (к прямой $sb_{ij} = sa_{ij}$).

События A, B, C, D являются случайными и происходят с определенными вероятностями.



$$\begin{aligned}
 P(A) &= P(Ya_1 = Yb_1, Ya_2 = Ya_3, Yb_2 = Yb_3) = 1/8, \\
 P(B) &= P(Ya_1 \neq Yb_1, Ya_2 = Ya_3, Yb_2 \neq Yb_3) = 1/8, \\
 P(C) &= P(Ya_1 \neq Yb_1, Ya_2 \neq Ya_3, Yb_2 = Yb_3) = 1/8. \\
 P(D) &= 1 - (P(A) + P(B) + P(C)) = 5/8.
 \end{aligned} \quad (7)$$

Заключение

1. Закон распределения разности весовых коэффициентов отличается от равномерного. Наиболее вероятны небольшие разности значений.

2. Направления движения начальных значений весовых коэффициентов равновероятны, что является положительным свойством, т.к. сохраняется максимальная неопределенность у внешнего наблюдателя относительно неизвестных ему значений весовых коэффициентов.

3. Более половины тактов синхронизации являются нерезультативными, что может составить предмет дальнейшего совершенствования архитектуры сети и алгоритма коррекции весовых коэффициентов.

4. Следует помнить, что данные выводы относятся к начальным значениям весовых коэффициентов двух сетей, поскольку они являются независимыми. В процессе синхронизации сетей А и В между соответствующими весовыми коэффициентами появляется корреляционная связь, которая усиливается с увеличением числа тактов синхронизации и приведенные соотношения становятся несправедливыми.

5. Остается открытым вопрос об определении момента полной синхронизации сетей, так как продолжение процесса синхронизации может позволить успешно завершиться одной из описанных атак.

Литература:

1. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W.Kinzel.–2005. – Vol. 5, n.1. – P. 130–140.

2. Kinzel, W. Neural Cryptography / W.Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

Abstract

IdoKanter andWolfgang Kinzel offer synchronizedneural networksusing for key derivation. Authors suppose that this approach should be investigated into the matter, algorithm convergence should be confirmed.Algorithm vulnerability is confirmed by attacks simulation. The initial weight vectors values influence on speed of synchronization wasanalyzed. Equal probability of initial weight vectors motion directions was found. On this base authors propose new line of research concerned with improvement of network architecture and correction algorithm.

Поступила в редакцию 18.05.2013 г.

ПРИНЦИПЫ ПОСТРОЕНИЯ АДАПТИВНОЙ СИСТЕМЫ КИБЕРЗАЩИТЫ

УДК 004.056.57:032.26

С.В. Безобразов, В.А. Головки,
БрГТУ, г. Брест

Аннотация

Методы искусственного интеллекта в целом, а также искусственные иммунные системы и искусственные нейронные сети в частности, являются мощным инструментом в области анализа данных. Они хорошо себя зарекомендовали в решении сложных инженерных задач в различных отраслях. Зачастую, интеграция методов искусственного интеллекта приводит к достижению лучших результатов, нежели использование их по отдельности. В данной статье мы описываем основные принципы построения интеллектуальной системы защиты информации от вредоносных программ и сетевых вторжений. Такая система базируется на интеграции методов искусственных иммунных систем и искусственных нейронных сетей. Основной упор будет сделан на исследование адаптивной способности предлагаемого подхода.

Введение

Современный мир переживает резкий рост числа и уровня сложности киберугроз, направленных как на отдельных пользователей сети Интернет, так и на информационные ресурсы национальных государств. В арсенале киберпреступников сегодня находятся разнообразные средства организации кибератак. Наиболее опасными атаками считаются сетевые атаки, осуществляемые посредством глобальной сети Интернет и разработка и распространение

вредоносных программ. Так в 2010 году промышленные объекты Ирана были атакованы вредоносной программой Stuxnet с целью несанкционированного сбора данных и диверсий в автоматизированных системах управления промышленных объектов посредством физического разрушения инфраструктуры. Компьютерный червь оказался настолько сложным, что на его «расшифровку» понадобилось несколько месяцев упорных трудов. Многие специалисты по информационной безопасности заговорили о том, что за созданием Stuxnet стоят спецслужбы отдельного государства. В 2012 году антивирусной компанией «Лаборатория Касперского» были обнаружены другие системы кибершпионажа «Duqu», «Flame» и «Gauss», разработанные по всей вероятности спецслужбами отдельных государств. Примечательным в этих событиях является то, что перечисленные вредоносные программы оставались неизвестными и не детектируемыми на протяжении месяцев и даже лет.

Сетевые атаки также представляют большую угрозу информационным ресурсам. Так в 2013 году атакам подверглись некоторые правительственные и коммерческие сайты ряда государств. Так известная хакерская группа Anonymous организовала DDoS атаки на сайты министерства обороны и министерства образования Израиля, а также взломать web-сайт Министерства иностранных дел Палестины и похитить конфиденциальную инфор-



является бинарная структура иммунных детекторов [1, 5], которая налагает ряд серьезных ограничений. В отличие от существующих подходов мы предложили в основу иммунного детектора положить нейронную сеть встречного распространения. Это позволило нам избавиться от ряда недостатков и повысить адаптивную способность иммунной системы для защиты информации.

Нейросетевая иммунная система киберзащиты

Для повышения уровня обнаружения вредоносных программ и сетевых атак нами была предложена система, базирующаяся на интеграции искусственных нейронных сетей и искусственных иммунных систем [6–9]. Структура предложенной системы представлена на рисунке 1.

Предложенная система основана на принципах и механизмах искусственной иммунной системы [8], где главную роль по обнаружению

мацию. А неизвестные киберпреступники организовали успешную атаку на крупнейшую биржу Bitcoin, что стало причиной нарушения корректного осуществления транзакций, а также взлому электронных хранилищ.

Все это свидетельствует о том, что применяемые сегодня методы обнаружения вредоносных программ и сетевых атак не позволяют быть уверенными в надежности предоставляемой защиты компьютерных систем и сетей. Все они характеризуются рядом существенных недостатков, и позволяют киберпреступникам обходить существующие системы защиты. В связи с этим, актуальным является разработка и применение принципиально новых методов и алгоритмов защиты компьютерных систем от киберугроз. Современные системы защиты информации должны характеризоваться высокой степенью защиты, способностью к адаптации и эволюции с целью поддержания высокого уровня защиты.

В данной статье мы представляем систему защиты информации, которая базируется на методах искусственного интеллекта – искусственных иммунных систем и искусственных нейронных сетях.

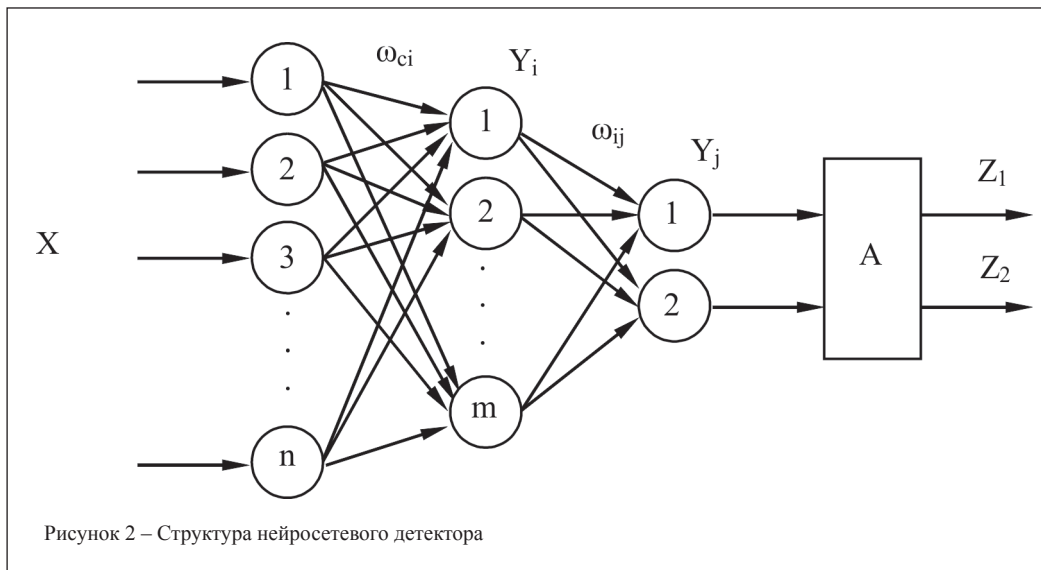
На сегодняшний день существует несколько основных алгоритмов искусственных иммунных систем. Это такие общеизвестные алгоритмы как алгоритм негативного отбора (the negative selection algorithm) [1], алгоритм клонального отбора (the clonal selection algorithm) [2], алгоритм идиотипической сети (the idiotypic network) [3], алгоритм дендритных клеток (the dendritic cell algorithm) [4]. Перечисленные алгоритмы имеют свои сильные и слабые стороны. На наш взгляд существенным недостатком существующих разработок на основе алгоритмов искусственных иммунных систем

вредоносных программ и сетевых атак играют нейросетевые детекторы. Структура нейросетевого детектора представлена на рисунке 2.

Детектор состоит из нейронной сети встречного распространения [10] и арбитра. Нейронная сеть состоит из трех слоев. Первый слой является распределительным. Данные, поступающие на сеть, он распределяет на нейроны второго слоя. Второй слой – скрытый, и состоит из нейронов Кохонена, которые осуществляют кластеризацию входных образов, и использует правило конкурентного обучения [10]. Третий слой нейронной сети состоит из линейных нейронов и служит для отображения результатов классификации. Арбитр принимает окончательное решение о принадлежности того или иного образа к определенному классу. После процесса обучения нейросетевой детектор способен корректно классифицировать программные исполняемые модули и обнаруживать вредоносное ПО.

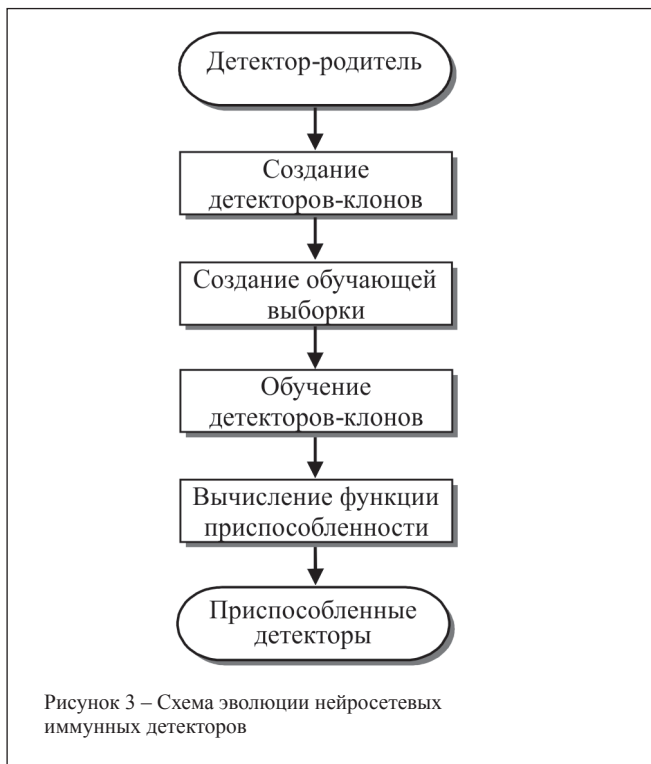
Искусственная иммунная система эмулирует основные принципы и механизмы биологической иммунной системы с целью построения распределенной самоорганизующейся системы для эффективного решения широкого круга инженерных задач, например – классификация образов, анализ и обработка больших массивов данных, оптимизация и т.д. Благодаря принципам и механизмам искусственной иммунной системы нейросетевые детекторы непрерывно эволюционируют и «подстраиваются» под особенности развития вредоносных программ и сетевых атак, позволяя системе киберзащиты адаптироваться к новым реалиям и поддерживать высокий уровень детектируемости вредоносных объектов.

Рассмотрим отдельный случай эволюции и адаптации нейросетевого иммунного детектора. Предположим, что i -й



детектор обнаружил вредоносный объект и инициировал соответствующий сигнал. После этого он подвергается процедурам клонирования и мутации. В результате, в системе образуется некоторое количество новых однотипных детекторов, обучение которых проводилось на обнаруженном вредоносном объекте. Т.е. обнаруженный вредоносный объект инициировал механизмы эволюции. В общем случае алгоритм эволюции в нейросетевой искусственной иммунной системе может выглядеть следующим образом (рисунок 3):

1. Создание популяции D детекторов-клонов. Родителем является детектор, обнаруживший вредоносный объект.
2. Создается обучающая выборка L на основе обнаруженного вредоносного объекта.



3. Обучение детекторов-клонов на созданной обучающей выборке.

4. Вычисление функции приспособленности F обученных клонов. Если функция приспособленности детектора-клона ниже чем детектора-родителя, то детектор-клон уничтожается.

Функция приспособленности (фитнесс-функция) используется для определения «качества», или точности, обнаружения. В качестве функции приспособленности

может использоваться среднеквадратичная ошибка между входным и выходным вектором нейросетевого иммунного детектора:

$$E_i = \frac{1}{2} \sum_{k=1}^L \sum_{j=1}^2 (Z_{ij}^k - l_{ij}^k)^2, \quad (1)$$

где Z_{ij}^k – значение j -го выхода i -го детектора при подаче на вход его k -го образа; l_{ij}^k – эталонное выходное значение i -го детектора-клона.

Каждый иммунный детектор в системе имеет определенное время жизни в течении которого он сканирует программные объекты. Если на протяжении этого времени детектор не обнаруживает вредоносное ПО он уничтожается как заведомо «слабый» детектор, а на его место приходит новый. Однако не все детекторы заменяются на новые. Из списка детекторов-клонов, полученных в результате процесса эволюции, отбираются детекторы с наивысшим показателем функции приспособленности и трансформируются в так называемые детекторы иммунной памяти. Такие детекторы существуют в системе на протяжении всего периода ее функционирования и являются некоторым аналогом антивирусной базы сигнатур. Такие детекторы быстро реагируют на повторное проникновение в компьютерную систему вредоносного ПО, блокируют его и уничтожают.

Заключение

Сложившаяся ситуация требует совершенствования методов защиты компьютерных систем от новых киберугроз. Мы разработали и предложили принципиально новые алгоритмы организации системы киберзащиты, основанные на применении методов искусственного интеллекта. Разработанная система способна не только обнаруживать ранее известные вредоносные программы, но повысить уровень детектирования новых, ранее неизвестных вредоносных объектов. Предложенная система киберзащиты имеет способности к адаптации и эволюции. Разработанный подход можно применять не только для обнаружения вредоносных файловых объектов, но и для обнаружения сетевых вторжений [11]. Проведенные эксперименты [7, 11] подтверждают эффективность системы в обнаружении кибератак.

На сегодняшний день разработан действующий прототип, который выставлялся на многочисленных национальных и международных выставках и завоевал высокие награды. Разработанные методики и алгоритмы защищены патентом. Исследовательская работа поддерживалась рядом государственных грантов.

Литература:

1. Forrest, S. Self-nonself discrimination in a computer / S. Forrest, A. Perelson, L. Allen, R. Cherukuri // In Proceedings of the IEEE Symposium on Security and Privacy, 1994. – P. 202–212.
2. Burnet, F. The Clonal Selection Theory of Acquired Immunity / F. Burnet. – Cambridge University Press, 1959.
3. Jerne, N. Towards a network theory of the immune system. Ann. Immunology (Inst. Pasteur), 125C / N. Jerne. – 1974. – P. 373–389.
4. Greensmith, J. The deterministic dendritic cell algorithm / J. Greensmith, U. Aickelin // In Proc. of the 7th International Conference on Artificial Immune Systems (ICARIS). – Springer, 2008. – P. 291–302.
5. Harmer, P. An artificial immune system architecture for computer security applications / P. Harmer, P. Williams, G. Gunsch, G. Lamont // IEEE Transaction on Evolutionary Computation, 2002. – 6(3). – P. 252–280.
6. Безобразов, С.В. Нейросетевая искусственная иммунная система для обнаружения вредоносных программ: принципы построения / С.В. Безобразов, В.А. Головкин // Вестник БрГТУ. Физика, математика, информатика. – 2009.
7. Безобразов, С.В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головкин // Научная сессия НИЯУ МИФИ «Нейроинформатика»: материалы Всеросс. науч. конф., МИФИ, Москва, 25–29 янв. 2010. – Москва, 2010. – С. 273–287.
8. Головкин, В.А. Проектирование интеллектуальных систем обнаружения аномалий / В.А. Головкин, С.В. Безобразов // Материалы международной научно-технической конференции «Открытые семантические технологии

проектирования интеллектуальных систем OSTIS-2011». – Минск: БГУИР, 2011. – С. 185–196.

9. Golovko, V. Evolution of Immune Detectors in Intelligent Security System for Malware Detection / V. Golovko, S. Bezobrazov, V. Melianchuk, M. Komar // Proceedings of the 6th IEEE international conference on intelligent data acquisition and advanced computing system IDAACS-2011. – Prague: Technical university, 2011. – P. 722–726.

10. Головкин, В.А. Нейронные сети: обучение, организация, применение / В.А. Головкин // Нейрокомпьютеры и их применение: учеб. пособие. – М.: 2001. – 256 с.

11. Komar, M. Intelligent System for Detection of Networking Intrusion. / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov – In Proc. 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing System (IDAACS-2011). – Prague, Czech Republic, 2011. – P. 374–377.

Abstract

Artificial immune systems (AIS) and artificial neural networks (ANN) are very powerful technique for data mining and pattern recognition. Over the past few decades, application of these approaches has been growing rapidly in different domain. However, to date a consistent performance of AIS and ANN has not achieved. We sincerely believe that integration of these both techniques can allow constructing an intelligent system for information security. In this research we report a novel method for malicious code detection. It is based on main principles of AIS, which consist of different immune detectors and each immune detector represents counterpropagation neural network. The main goal of proposed approach is to detect unknown, previous unseen threat (malicious code, intrusion detection, etc.). It is achieved by the adaptation of the neural network immune detectors to the continually changeable computer environment. As a result the immune detectors have capability to evolve during a life. The evolution ability of neural immune detectors in artificial immune system is presented. The results of the experiments are shown the performance of the algorithm in increasing the quality of new, unknown threat detection.

Поступила в редакцию 18.05.2013 г.

ПОДХОД К ПОСТРОЕНИЮ СРЕДСТВ ЗАЩИТЫ «ОБЛАЧНЫХ» СИСТЕМ

УДК 004.3'2

В.И. Хведчук, В.В. Буслюк, С.С. Дереченник,
БрГТУ, г. Брест

Аннотация

В работе предлагается подход к хранению личных данных в корпоративной системе, базирующейся на «облачной» технологии. Проводится обзор известных решений в данной области. Рассмотрены базовые решения на базе протокола NFC. Выделены, в качестве основных, решения фирм Inside Secure и Texas Instruments. Предложена структура устройства на базе протокола, используемого в стационарных линиях связи с использованием отечественной элементной базы. В результате получается защищенная среда, позволяющая обеспечить доступ к «облачным» ресурсам и обеспечивающая мобильность корпоративных систем, построенных на

современной основе. При этом необходимо решение дополнительно проблем с обслуживанием такого рода структур, связанных, прежде всего, с человеческим фактором. Здесь, конечно же, важную роль должно сыграть обучение кадров. Предполагается к использованию в корпоративной среде университета.

Введение

В настоящее время информационные технологии проникают в различные сферы деятельности человека, общества, государства. Происходит изменение обычных для нас процессов и объектов. Меняются способы оплаты услуг и

товаров, идентификации, обмена информацией. Не редкость сейчас идентификационная или банковская карта. Со временем этот процесс продолжится. Примером может служить введение мобильных технологий. Пока еще привычным является платеж в банке, но звонок по стационарному телефону уже не является единственным средством online-коммуникации. Массовая информатизация охватывает все новые сферы деятельности, появляется все больше «облачных» услуг. Но этот количественный рост требует качественно иного подхода к обеспечению надежности и безопасности базовых механизмов подобных сервисов и услуг. И не последнюю роль здесь может сыграть задача обучения современным технологиям защиты информации. Причем как сотрудников компаний, представляющих данные сервисы и услуги, так и их клиентов. При этом важной остается задача обеспечения защиты при доступе к «облачным» технологиям с помощью стационарных коммуникаций ввиду их надежности.

Обзор решений по защите «облачных» систем. Современные облачные технологии предполагают переход к новой парадигме вычислений, хранения данных, управления доступом, вводят такие понятия, как шина служб, кэширование. Присутствуют возможности доступа к удаленному рабочему столу, безопасная доставка по защищенному SSL-соединению. Появляется и проблема хранения личных данных [1].

Имеются сведения и об аппаратной защите данных у Google. Предлагается использовать миниатюрные крип-

тографические карты Yubico. Установленные в USB-порт позволят зарегистрироваться на новом сайте или войти в аккаунт Google, не набирая паролей (причем достаточно сложных, состоящих из случайных букв или цифр). Такой способ аутентификации аналогичен открытию двери ключом. Возможен переход на беспроводные протоколы и усиление защиты введением одноразового кода [2].

Отмечается, что современные средства обеспечения безопасности по своей функциональности вышли за рамки защиты ПЭВМ от вирусов. Речь идет об интернет-сервисах, онлайн-платежах, социальных сетях, мобильных устройствах, облачных хранилищах. Появились новые функции – резервное копирование, хранение и синхронизация паролей, безопасные онлайн-платежи, родительский контроль. Имеются также функции генерации паролей достаточной сложности. Такого рода функции включены в новую версию пакета CRYSTAL от Kaspersky Lab, NORTON 360 [3]. Пока неизвестно о наличии защиты в «облаках» в белорусском антивирусе ВирусБлокАда.

Развиваются также средства защиты и на десктопах, в том числе и на базе операционной системы [4, 5].

Аппаратная платформа. В качестве аппаратных платформ для реализации средств обеспечения безопасности с учетом облачной природы объекта защиты используются чаще всего решения на базе протокола NFC.

Реализации в данной области предлагают многие фирмы, но наиболее широким спектром в области защищенных решений обладает компания Atmel [6]. Известна

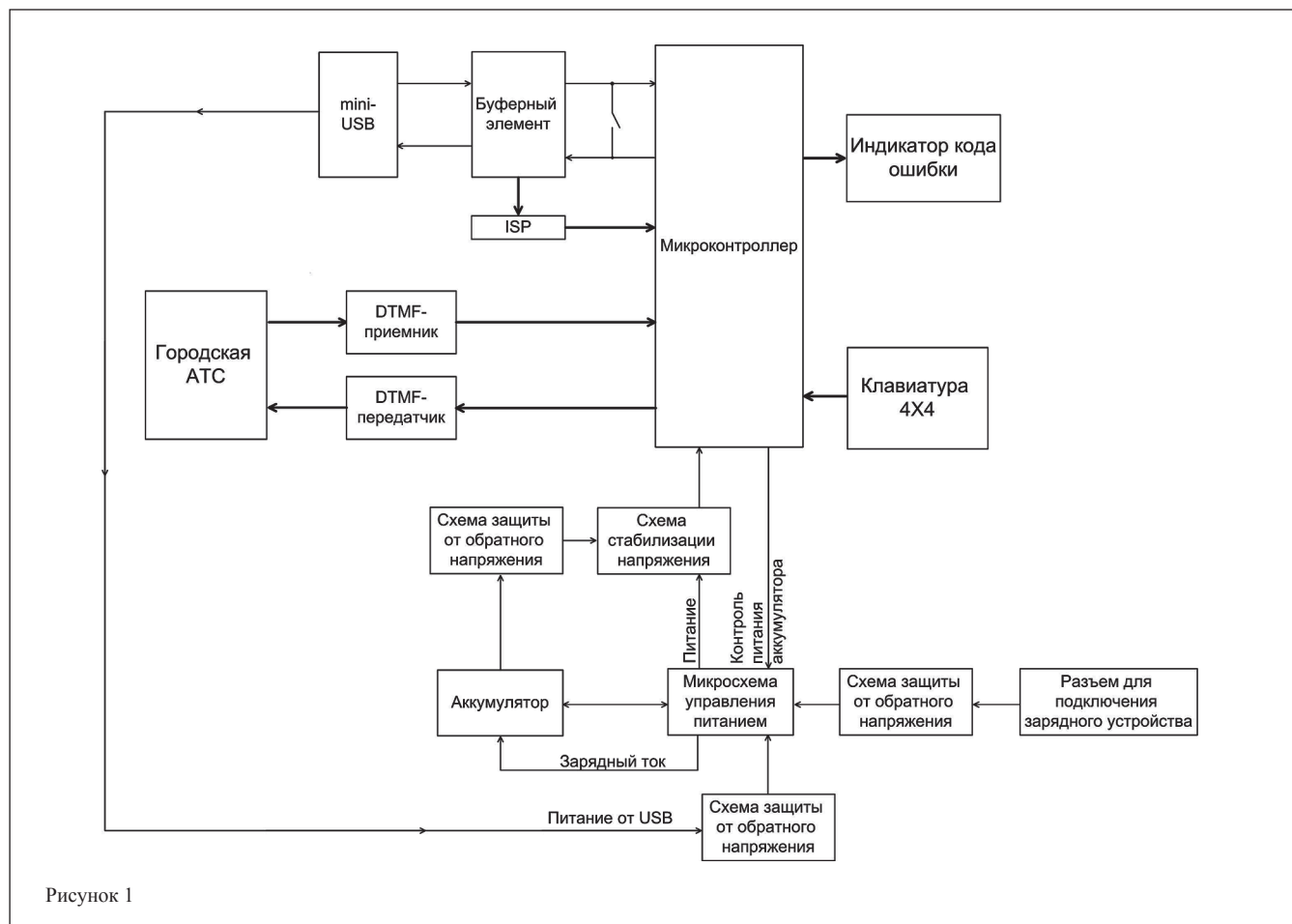


Рисунок 1

также своей проработкой вопросов построения закрытых приложений компания Inside Secure, которая приобрела в 2010 году подразделение Atmel, занимавшееся разработкой защищенных микроконтроллеров [7, 8]. Функции обеспечения информационной безопасности, реализуемые с помощью решений компании Inside Secure:

- аутентификация субъектов и объектов информационного взаимодействия (предоставление взаимодействующим сторонам возможности убедиться в том, что противоположная сторона действительно является тем, за кого себя выдает);

- шифрование информации (защита информации в случае перехвата ее третьими лицами);

- контроль целостности (гарантия того, что информация не была искажена или подменена);

- управление доступом (разграничение доступа к информации различных пользователей);

- управление ключами (организация создания, распространения и использования ключей субъектов и объектов информационной системы с целью создания необходимого базиса для процедур аутентификации, шифрования, контроля подлинности и управления доступом).

Хорошая схемотехническая проработка реализации NFC от фирмы Texas Instruments имеется в [9–11], причем со ссылкой на соответствующие стандарты. Описана также необходимая программная поддержка.

Структура коммуникационного процессора. В структуре устройства (рисунок 1) выделяются следующие основные блоки: микроконтроллер; ISP; mini-USB; ключ «Режим отладки»; буферный элемент; DTMF-приемник; DTMF-передатчик; аккумулятор; схема защиты от обратного напряжения; схема стабилизации напряжения; разъем для подключения зарядного устройства (ЗУ); микросхема управления питанием; клавиатура 4×4; индикатор кода ошибки. Назначение блоков устройства:

- ISP (In-System Programming – системное программирование) для программирования микроконтроллера;

- mini-USB – для связи с и прошивки микроконтроллера;

- ключ «режим отладки» – для отладки устройства при отсутствии компьютера и телефонной линии;

- буферный элемент – это приемопередатчик от разъема USB – устройство, которое обеспечивает обмен данными между несколькими устройствами по одной двухпроводной линии связи. Микроконтроллер осуществляет связь с компьютером для передачи и приема данных от устройства, отладки;

- DTMF-приемник (от англ. Dual Tone Multi Frequency – двухтональная мультичастотная посылка) – для приема зашифрованных данных от телефонной сети;

- DTMF-передатчик – для передачи зашифрованных данных в телефонную сеть;

- схема защиты от обратного напряжения – для электронной защиты при ошибочном подключении аккумулятора, ЗУ, mini-USB;

- схема стабилизации напряжения – экономичный преобразователь напряжения, необходимый для нормальной работы микросхем;

- микросхема управления питанием – осуществляет «умное» управление питанием, выбор необходимых источников питания, обеспечение безопасной зарядки аккумулятора и индикацию текущего состояния питания;

- клавиатура 4×4 – для ввода информации в устройство при отсутствии компьютера;

- индикатор кода ошибки – индикация текущего состояния устройства.

Заключение

Таким образом, возможно получить защищенную среду, позволяющую обеспечить доступ к «облачным» ресурсам и обеспечивающую мобильность корпоративных систем, построенных на современной основе. При этом решаются дополнительно проблемы с обслуживанием такого рода структур, связанных, прежде всего, с человеческим фактором. Здесь, конечно же, важную роль должно сыграть обучение кадров. Предполагается к использованию в корпоративной среде университета.

Литература:

1. Редкар, Т. Платформа Windows Azure / Т. Редкар, Т. Гвидичи. М.: ДМК Пресс, 2012. – 656 с.
2. Пароли – это прошлый век // Хакер. – № 3. – 2013. – С. 8.
3. Защита и сохранение самого ценного // CHIP, № 4. – 2013. – С. 66–67.
4. Карп, Д. Хитрости Windows 7. Для профессионалов / Д. Карп. – СПб.: Питер, 2011. – 512 с.
5. Станек, У. Windows 7 для продвинутых / У. Станек. – СПб.: Питер, 2010. – 576 с.
6. AVR XMEGA microcontroller. – http://www.atmel.com/products/microcontrollers/avr/AVR_XMEGA.aspx, 09.02.2013.
7. Secure microcontroller. – http://www.insidesecure.com/eng/content/download/871/8385/version/3/file/FLYER-SecureMicrocontroller_BD.pdf, 09.02.2013
8. New NFC-based chip from Inside Secure protects luxury goods from counterfeiters and cloners. – <http://www.insidesecure.com/eng/Media/Press-releases/NEW-NFC-BASED-CHIP-FROM-INSIDE-SECURE-PROTECTS-LUXURY-GOODS-FROM-COUNTERFEITERS-AND-CLONERS>, 09.02.2013
9. Alexander Kozitsky, Josh Wyatt, Johannes Sturz, Juergen Mayer-Zintel. NFC and RFID Reader Ultra-Low-Power Card Presence Detection Using MSP430 and TRF79xxA. – <http://www.ti.com/lit/an/sloa184/sloa184.pdf>, 06.04.2013
10. Multi-protocol fully integrated 13.56-mhz rfid/near field communication (NFC) transceiver IC – <http://www.ti.com/lit/an/sloa184/slos743f.pdf>, 06.04.2013
11. Mixed signal microcontroller. – <http://www.ti.com/lit/an/sloa184/slas518.pdf>, 06.04.2013

Abstract

The paper proposes an approach to the storage of personal data in the corporate system based on the "cloud" technology. Provides an overview the prior art in this field. Describes the basic solutions based on NFC protocol. Solutions companies Inside Secure and Texas Instruments are selected key. Proposed the structure of a device based on the protocol fixed lines. Use national element base. The result is a secure environment, allowing secure access to the "cloud" resources and providing enterprise mobility systems based on a modern basis. Thus it is necessary to additionally maintenance problems such structures associated primarily with human factor. Here, of course, has an important role the training of service personnel. It is assumed to be used in the corporate environment of the university.

Поступила в редакцию 18.05.2013 г.

О ДИНАМИКЕ ПАМЯТИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ МАКЛАРЕНА-МАРСАЛЬИ

УДК 004.421.5-519.217.2

И.Б. Бережной, Ю.С. Харин,
НИИ ПМИ БГУ, г. Минск

Аннотация

Рассматривается класс криптографических генераторов псевдослучайных последовательностей Макларена-Марсальи. Исследуется вероятностная модель динамики памяти генераторов Макларена-Марсальи. Получены отдельные вероятностные свойства памяти.

Введение

В системах криптографической защиты информации важную роль играют последовательности случайных чисел [1, 2]. На практике для их генерации в основном используют программные генераторы, когда детерминированным алгоритмом создается псевдослучайная последовательность, как можно больше похожая на случайную. В последнее время особое внимание уделяется генераторам с памятью. Так, в конкурсе eSTREAM, целью которого было создание европейских стандартов для поточных систем шифрования, два из четырех финалистов в профиле «поточные шифры для программного применения с большой пропускной способностью» являются такими генераторами [3]. Современные генераторы в подавляющем большинстве представляют собой комплексы комбинированных определенным образом модулей, представляющих собой различные криптографические примитивы [1, 2]. Данные примитивы для эффективной работы всего генератора должны иметь достаточно простую структуру и при этом обладать хорошими криптографическими свойствами. Одним из таких широко известных примитивов является класс генераторов Макларена-Марсальи [4], которые сочетают свойство простоты реализации с достаточно высоким качеством выходной последовательности [5]. Об этом свидетельствует и тот факт, что один из участников конкурса eSTREAM, получивший хорошую оценку, поточный шифр «Ямб» [6] содержит модуль аналогичной структуры.

Ранее класс генераторов Макларена-Марсальи изучался авторами в статье [7], в которой представлена формула для периода выходной последовательности, уточняющая приведенную в [2] формулу, доказаны некоторые вероятностные свойства, на основании которых построены формулы и оценки, характеризующие влияние генератора на некоторые статистические характеристики выходной последовательности. В данной статье продолжено исследование класса генераторов Макларена-Марсальи: исследуется вероятностная модель динамики памяти генераторов Макларена-Марсальи при различных условиях, доказан критерий равномерности предельного распределения вероятностей памяти, получена формула для предельного распределения в общем случае, на основании которой найдены некоторые вероятностные характеристики динамики памяти.

1 Математическая модель генераторов Макларена-Марсальи

Генераторы Макларена-Марсальи, исследуемые в данной статье, имеют структуру, представленную на рисунке 1. Любой генератор данного семейства состоит из модифици-

руемой памяти размера L и двух простейших генераторов псевдослучайных последовательностей: G_1 и G_2 . Генератор G_1 порождает «заполняющую» («исходную») последовательность $\{\zeta_t\}$ над некоторым конечным множеством V , генератор G_2 – «управляющую» последовательность над множеством $A = \{0, 1, \dots, L-1\}$. Результирующей (выходной) последовательностью является последовательность над V . Имеется некоторое начальное заполнение памяти – вектор-столбец $X_0 = (x_{0,1}, x_{0,2}, \dots, x_{0,L})^T \in V^L$ (T – знак транспонирования).

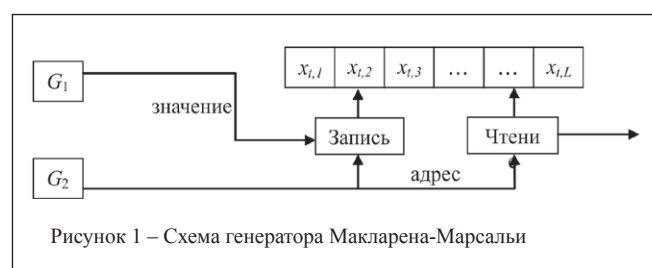


Рисунок 1 – Схема генератора Макларена-Марсальи

Определим функцию $Y = \chi(X, v, a)$, где $X, Y \in V^L$, $v \in V$, $a \in A$, следующим образом:

$$Y = (y_1, y_2, \dots, y_L), \quad y_i = \begin{cases} x_p & \text{если } i \neq a; \\ v, & \text{если } i = a. \end{cases} \quad (1)$$

Другими словами, функция $\chi(X, v, a)$ заменяет в векторе X значение элемента с номером a на значение v .

Пусть $\{X_t; t = 1, 2, \dots\}$ – последовательность состояний памяти X , X_0 – некоторое начальное заполнение памяти. Тогда динамика генератора на тактах $t = 1, 2, \dots$ опишется формулами:

$$\begin{aligned} Y_t &= X_{t-1, \zeta_t}, \\ X_t &= \chi(X_{t-1}, \zeta_t, \eta_t). \end{aligned} \quad (2)$$

Таким образом, на каждом такте в выходную последовательность считывается элемент из памяти X по адресу, определяемому генератором G_2 , затем по этому адресу в память заносится новый элемент из последовательности, порождаемой генератором G_1 .

2 Вероятностная модель динамики памяти

Пусть $\{\zeta_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности независимых в совокупности случайных величин с распределениями вероятностей:

$$\begin{aligned} P\{\zeta_t = i\} &= \lambda_i \neq 0, \quad i \in V, \quad \sum_{i \in V} \lambda_i = 1; \\ P\{\eta_t = j\} &= \gamma_j \neq 0, \quad j \in A, \quad \sum_{j \in A} \gamma_j = 1. \end{aligned} \quad (3)$$

Теорема 1. Пусть $\{\zeta_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности независимых в совокупности случайных величин с распределениями вероятностей (3). Тогда последователь-

ность $\{X_t\}$ состояний памяти представляет собой регулярную цепь Маркова первого порядка с пространством состояний V^L и матрицей переходных вероятностей $P = (p_{j,k})$:

$$p_{J,K} = P\{X_{t+1} = K | X_t = J\} = \sum_{i \in V} \sum_{j \in A} \lambda_j \gamma_j \delta_{K, \chi(J, i, j)}, \quad (4)$$

$$J, K \in V^L,$$

где $\delta_{J,K} = \begin{cases} 1, J = K; \\ 0, J \neq K. \end{cases}$ – символ Кронекера.

Обозначим: $H(U, W) = \sum_{i=1}^L (1 - \delta_{A_i, B_i})$ – количество несовпадающих элементов векторов $U, W \in V^L$.

Следствие 1. При выполнении условий (3) элементы матрицы P переходных вероятностей имеют следующий вид:

$$p_{J,K} = \begin{cases} \sum_{i=1}^L \gamma_i \lambda_{j_i}, & \text{если } H(J, K) = 0, \text{ т.е. } K = J = (j_1, j_2, \dots, j_L); \\ \gamma_i \lambda_{j_s}, & \text{если } H(J, K) = 1, \text{ т.е. } K = \chi(J, s, i), s \neq j_s; \\ 0, & \text{если } H(J, K) \geq 2. \end{cases} \quad (5)$$

Теорема 2. Пусть $\{\zeta_i\}$ и $\{\eta_i\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности независимых в совокупности случайных величин с распределениями вероятностей (3). Тогда стационарное распределение вероятностей α цепи Маркова $\{X_t\}$ существует и имеет мультипликативный вид:

$$\alpha_K = \lambda_{k_1} \cdot \lambda_{k_2} \cdot \dots \cdot \lambda_{k_L}, K = (k_1, k_2, \dots, k_L) \in V^L. \quad (6)$$

Следствие 2. Стационарное распределение вероятностей (6) состояний памяти $\{X_t\}$ не зависит от распределения вероятностей $\{\gamma_i\}$ управляющей последовательности $\{\eta_i\}$.

Следствие 3. Пусть выполняются условия теоремы 2. Стационарное распределение вероятностей α состояний памяти $\{X_t\}$ является равномерным (т.е. $\forall K \in V^L \alpha_K = 1/|V^L|$) тогда и только тогда, когда распределение вероятностей $\{\lambda_i\}$ элементов заполняющей последовательности $\{\zeta_i\}$ – равномерное ($\lambda_i \equiv 1/|V|$).

Данные следствия определяют, что равномерность стационарного распределения вероятностей состояний памяти $\{X_t\}$ эквивалентна равномерности распределения вероятностей элементов заполняющей последовательности $\{\zeta_i\}$, если $\{\zeta_i\}$ и $\{\eta_i\}$ – последовательности независимых в совокупности случайных величин. Другими словами, вероятностные свойства $\{X_t\}$ не ухудшаются в сравнении с $\{\zeta_i\}$.

Введем следующие обозначения:

$u_K^{(n)}$ – частота вектора K в последовательности состояний памяти $\{X_t\}$, $t \in \{1, 2, \dots, n\}$, т.е.

$$u_K^{(n)} = \frac{1}{n} \sum_{i=1}^n \delta_{X_i, K};$$

f_K – время первого возврата в состояние K , т.е.

$f_K = n \in N: X_n = X_0 = K, \forall i = 1, n-1 X_i \neq K$.

Следствие 4. Пусть выполняются теоремы 2. Тогда верны следующие утверждения:

1. Вне зависимости от начального распределения

математическое ожидание $u_K^{(n)}$ при $n \rightarrow \infty$ удовлетворяет предельному соотношению:

$$E\{u_K^{(n)}\} \rightarrow \lambda_{k_1} \cdot \lambda_{k_2} \cdot \dots \cdot \lambda_{k_L}, K = (k_1, k_2, \dots, k_L) \in V^L. \quad (7)$$

2. Математическое ожидание времени возврата в исходное состояние памяти K определяется формулой:

$$E\{f_K\} = \frac{1}{\lambda_{k_1} \cdot \lambda_{k_2} \cdot \dots \cdot \lambda_{k_L}}. \quad (8)$$

Данное следствие описывает частотные характеристики динамики памяти генератора. С их помощью можно оценить, как часто элемент выходной последовательности выбирался из заданного состояния памяти и имел соответствующее условное распределение вероятностей.

Теорема 3. Пусть $\{\zeta_i\}$ и $\{\eta_i\}$ – определенные на некотором вероятностном пространстве (Ω, F, P) последовательности случайных величин с распределениями вероятностей (3), причем элементы $\{\eta_i\}$ независимы в совокупности, а $\{\zeta_i\}$ представляет собой цепь Маркова первого порядка с матрицей переходных вероятностей $Q = (q_{u,v})$, $u, v \in V$. Тогда случайная последовательность состояний памяти $\{X_t\}$ представляет собой однородную цепь Маркова второго порядка с матрицей переходных вероятностей $P = (p_{I,J,K})$:

$$p_{I,J,K} = P\{X_{t+1} = K | X_t = J, X_{t-1} = I\} = \frac{\sum_{i \in V} \sum_{j \in A} (\lambda_i \gamma_j \delta_{J, \chi(I, i, j)} \sum_{l \in V} \sum_{s \in A} q_{j,l} \lambda_s \delta_{K, \chi(J, l, s)})}{\sum_{i \in V} \sum_{j \in A} \lambda_i \gamma_j \delta_{J, \chi(I, i, j)}}. \quad (9)$$

$$I, J, K \in V^L.$$

Следствие 5. При выполнении условий теоремы 3 элементы матрицы переходных вероятностей $P = (p_{I,J,K})$ имеют следующий вид:

$$p_{I,J,K} = \begin{cases} \frac{\sum_{s \in A} (\gamma_s \lambda_{k_s} \sum_{r \in A} (\gamma_r q_{k_s, k_r}))}{\sum_{s \in A} \gamma_s \lambda_{k_s}}, & \text{если } K = J = I; \\ \frac{\sum_{s \in A} (\gamma_s \lambda_{j_s} \cdot \gamma_r q_{j_s, k_r})}{\sum_{s \in A} \gamma_s \lambda_{j_s}}, & \text{если } K = \chi(J, k_r, r), k_r \neq j_r, J = I; \\ \sum_{r \in A} (\gamma_r q_{j_s, k_r}) & \text{если } K = J = \chi(I, j_s, s), j_s \neq i_s; \\ \gamma_r \cdot q_{j_s, k_r}, & \text{если } K = \chi(J, k_r, r), k_r \neq j_r, J = \chi(I, j_s, s), j_s \neq i_s; \\ 0, & \text{если } H(I, J) \geq 2 \text{ или } H(J, K) \geq 2, \end{cases} \quad (10)$$

где $K = (k_1, k_2, \dots, k_L)$, $J = (j_1, j_2, \dots, j_L)$, $I = (i_1, i_2, \dots, i_L)$.

Следствие 6. Если в условиях теоремы 3 одномерные распределения вероятностей λ и γ элементов последовательностей $\{\zeta_i\}$ и $\{\eta_i\}$ – равномерные, то элементы матрицы переходных вероятностей $P = (p_{I,J,K})$ имеют следующий вид:

$$p_{I,J,K} = \begin{cases} \frac{1}{L^2} \sum_{s \in A} \sum_{r \in A} q_{k_s, k_r}, & \text{если } K = J = I; \\ \frac{1}{L^2} \sum_{s \in A} (q_{j_s, k_r}) & \text{если } K = \chi(J, k_r, r), k_r \neq j_r, J = I; \\ \frac{1}{L} \sum_{r \in A} (q_{j_s, k_r}) & \text{если } K = J = \chi(I, j_s, s), j_s \neq i_s; \\ \frac{1}{L} q_{j_s, k_r}, & \text{если } K = \chi(J, k_r, r), k_r \neq j_r, J = \chi(I, j_s, s), j_s \neq i_s; \\ 0, & \text{если } H(I, J) \geq 2 \text{ или } H(J, K) \geq 2. \end{cases} \quad (11)$$

Следствие 6 наглядно иллюстрирует связь между матрицей переходных вероятностей $P = (p_{I,J,K})$ последовательности состояний памяти $\{X_t\}$ и матрицей переходных вероятностей $Q = (q_{u,v})$ заполняющей последовательности $\{\zeta_t\}$. Формула (11) также позволяет проводить оценку параметров заполняющей последовательности $\{\zeta_t\}$ по выборке из последовательности $\{X_t\}$.

Полученные результаты компьютерных экспериментов иллюстрируют согласие результатов компьютерного моделирования с теоретическими результатами анализа динамики памяти генератора Макларена-Марсальи.

Заключение

В данной статье продолжено исследование класса генераторов Макларена-Марсальи. Построена вероятностная модель динамики памяти генераторов Макларена-Марсальи. Формулы, описывающие данную модель, позволяют рассматривать выходные последовательности как скрытые цепи Маркова и применять в дальнейшем известные методы их анализа (например, алгоритм Витерби). Доказан критерий равномерности стационарного распределения вероятностей памяти. Получена формула для предельного распределения в общем случае, на основании которой найдены некоторые вероятностные характеристики динамики памяти, позволяющие повысить точность общих алгоритмов анализа скрытых цепей Маркова.

Результаты компьютерных экспериментов иллюстрируют согласие с теоретическими результатами.

Литература:

1. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Минск: Новое знание, 2003.
2. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005. – 480 с.
3. eSTREAM: the ECRYPT Stream Cipher Project. – Mode of access: <http://www.ecrypt.eu.org/stream/project.html>. – Date of access: 10.04.2013.
4. MacLaren, M. Uniform Random Number Generators / M. MacLaren, G. Marsaglia // Journal of the Association for Computing Machinery. – 1965. – V. 12(1). – P. 83–89.
5. Кнут, Д. Искусство программирования, том 2. Получисленные алгоритмы = The Art of Computer Programming, vol.2. Seminumerical Algorithms. – 3-е изд. / Д. Кнут. – М.: Вильямс, 2007.
6. «Yamb», LAN Crypto Submission to the ECRYPT Stream Cipher Project / Starodubtzev Sergey A., Lebedev Anatoly N., Volchkov Alexey A. – Mode of access: <http://www.ecrypt.eu.org/stream/yamb.html>. – Date of access: 10.04.2013.
7. Бережной, И.Б. О периодичности и вероятностных свойствах генератора Макларена-Марсальи / И.Б. Бережной, Ю.С. Харин // Материалы XI международной научно-практической конференции «Информационная безопасность-2010», 22–25 июня 2010 г. – Таганрог. – Ч. 3. – С. 83–85.
8. Кемени, Дж. Конечные цепи Маркова / Джон Дж. Кемени, Дж. Лори Снелл. – М.: Наука, 1970. – 272 с.

Abstract

A family of the Maclaren-Marsaglia cryptographic generators for pseudorandom sequences is considered. A probabilistic model of the memory dynamics for the Maclaren-Marsaglia generators is proposed and analysed. Some probabilistic properties of the memory are presented.

Поступила в редакцию 18.05.2013 г.

ИЕРАРХИЧЕСКАЯ НЕЙРОСЕТЕВАЯ СИСТЕМА ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

УДК 004.8.032.26

Л.Ю. Войцехович, В.А. Головки
БрГТУ, г. Брест

Аннотация

В работе представлена иерархическая многоагентная система обнаружения атак в компьютерных сетях, описана ее структура и изложены основные результаты экспериментов. Отдельный агент представляет собой комбинацию нелинейной рециркуляционной нейронной сети и персептрона. Данная модель основана на многослойной архитектуре взаимодействия агентов, которая задается набором правил, представленных в виде графа. Модель может выполнять классификацию сетевых атак

по классам и типам сетевой активности. Эксперименты свидетельствуют о том, что такое архитектурное решение позволяет сократить число ложных срабатываний, повысить точность распознавания и обнаруживать новые и модифицированные образы сетевых атак.

Введение

Безопасность компьютерных систем – одна из наиболее актуальных проблем современной индустрии информационных технологий. Ее актуальность постоянно возрастает, так как

с развитием информационного пространства увеличивается количество компьютерных атак и различных злоупотреблений в сфере высоких технологий, что увеличивает уязвимость компьютерных систем.

В настоящее время разрабатывается большое количество различных технологий защиты компьютерных сетей, которые базируются на применении нейронных сетей (neural networks), на технологиях извлечения данных (data mining), статистическом анализе и т.п. К недостаткам существующих технологий защиты, в первую очередь, можно отнести уязвимость к новым или неизвестным атакам, записи о которых отсутствуют в системе, низкая точность и скорость работы.

Существует две основные технологии обнаружения вторжений: обнаружение злоупотреблений и обнаружение аномалий. Обнаружение злоупотреблений (например, IDIOT [1] и STAT [2]) основано на использовании сигнатур о заранее известных атаках. Основным недостатком таких систем является их неспособность обнаруживать новые или неизвестные атаки, т.е. записи о которых в системе отсутствуют. Системы обнаружения аномалий [3] (например, система IDES [4]) идентифицируют атаку в случае значительного отклонения наблюдаемой сетевой активности от заданного профиля нормального поведения. Главным преимуществом таких систем является возможность определения ранее не встречавшихся атак, однако они характеризуются низкой точностью и скоростью работы.

Целью данной работы является разработка нейросетевой модели классификации для построения системы обнаружения сетевых атак (COA) реального времени, способной обнаруживать модифицированные и неизвестные атаки, записи о которых изначально отсутствуют в базе данных системы. Предлагаемый подход базируется на нейросетевой иерархической многоагентной модели, где в качестве агента выступает детектор, состоящий из рециркуляционной нейронной сети и многослойного персептрона [5, 6, 7].

1 Архитектурное решение COA

В работе в качестве основного агента (детектора) системы обнаружения атак предложена модель (рисунок 1), представляющая собой объединение нелинейной рециркуляционной нейронной сети (NPCA) и многослойного персептрона (MLP) [8]. В результате применения NPCA формируется сжатый набор исходных данных, который используются MLP непосредственно для выполнения классификации.

В результате специального объединения нейросетевых детекторов предложена иерархическая многоагентная система (рисунок 2) для обнаружения и классификации компьютерных атак. Такая система базируется на организации совместной работы заданного числа «интеллектуальных» агентов при помощи набора правил, которые задаются в виде направленного графа.

Рассматриваемая модель классификации включает три уровня, при чем каждый последующий уровень

подтверждает или опровергает результаты, полученные детекторами на предыдущем этапе. Такая модель способна определить является ли входной образ нормальным соединением или это атака определенного класса. Кроме того, позволяет также установить тип атаки.

Результаты экспериментов демонстрируют возможности системы по обнаружению модифицированных образов сетевых атак. Кроме того, система способна обнаруживать новые атаки, если данные коррелируют с уже накопленными в ходе работы системы знаниями о злонамеренном трафике.

2 Результаты экспериментов

Для обучения и тестирования предложенной системы использовались данные, представленные в таблице 1. Сетевые вторжения, можно отнести к одному из четырех классов: DoS, Probe, U2R и R2L [9]: DoS – это атаки отказа в обслуживании, Probe – сканирование сети с целью обнаружения уязвимых хостов или служб, U2R-предполагает, что злоумышленник пытается получить привилегии root-а или администратора и, наконец, R2L – неавторизованный доступ со стороны удаленной машины. Каждая категория включает атаки различного типа.

В ходе экспериментов с базой сетевых атак [9], содержащей почти 500 тысяч записей о сетевой активности реальной компьютерной сети, подсчитывалась статистика обнаружения сетевых вторжений и распознавания записей. Распознавание выполняется на основании имеющейся у системы информации об атаках, образы которых были использованы на этапе обучения. Таким образом, часть данных применялась для настройки системы (обучения нейронных сетей) (см. таблицу 1), далее все данные (в том числе участвовавшие в обучении) подавались на многоагентный классификатор для тестирования системы.

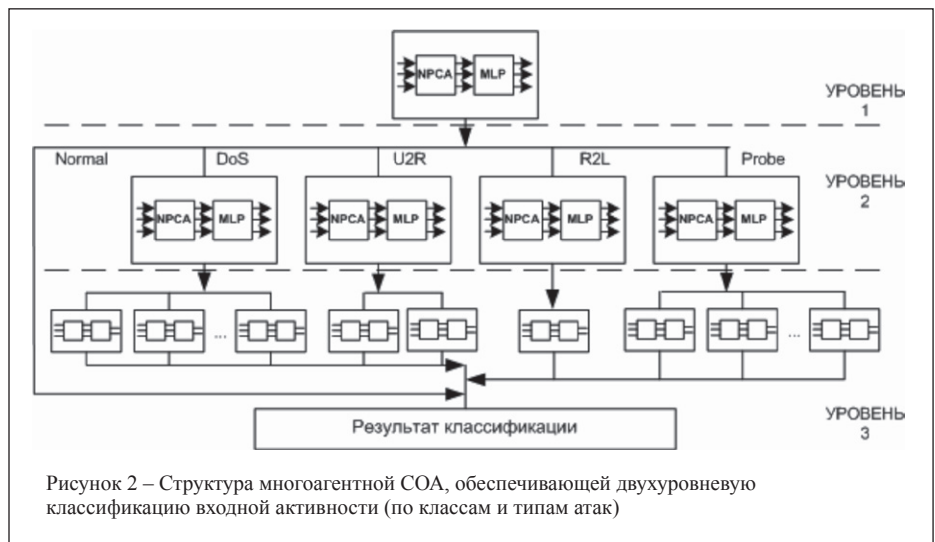
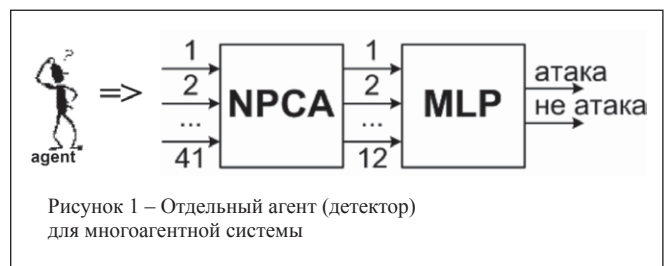


Таблица 1 – Обучающая и тестовая выборки

	DoS	U2R	R2L	Probe	Normal	Итого
обучение	3571	37	278	800	1500	6186
тестирование	391 458	52	1126	4107	97 277	494 020

В таблице 2 отражены результаты распознавания детекторами второго уровня различных классов сетевой активности. Детекторы третьего уровня позволяют выявлять тип атаки.

Таблица 2 – Результаты обнаружения класса атаки

класс	кол-во	обнаружено	распознано
DoS	391 458	384 125 (98,13%)	370 658 (94,68%)
U2R	52	47 (90,39%)	45 (86,54%)
R2L	1126	1068 (94,85%)	1066 (94,67%)
Probe	4107	4056 (98,75)	4056 (98,75)

По сравнению с моделями, предложенными в [5, 6], предложенная система позволила повысить точность распознавания и снизить количество ошибок первого рода. Основные характеристики предложенной модели по обнаружению сетевых атак приведены на в таблице 3.

Таблица 3 – Результаты ROC анализа предложенной модели

чувствительность	специфичность	точность
0,98	0,96	0,98

Заключение

В данной работе была рассмотрена иерархическая многоагентная система обнаружения сетевых атак, которая базируется на объединении нейросетевых детекторов. Система может применяться для расширения возможностей современных коммерческих приложений защиты информационных систем, а также функционировать как отдельный модуль. Предложенный подход позволяет: выполнить двухуровневую классификацию как по классам, так и по типам сетевой активности; снизить количество ложных срабатываний благодаря формированию коллективного решения совокупностью детекторов; обнаруживать новые и модифицированные сетевые атаки.

Литература:

1. Kumar, S. A software architecture to support misuse intrusion detection / E.H. Spafford // In Proceedings of the 18th National Conference on Information Security. – 1995. – P. 194–204.
2. Ilgun, K. USTAT: A real-time intrusion detection system for Unix. Master's Thesis. University of California at Santa Barbara, Santa Barbara, CA – 1992.
3. Animesh Patcha, Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends // Computer Networks – 2007. – 51. – P. 3448–3470.
4. Lunt, T. Detecting intruders in computer systems // In Proceedings of the 1993 Conference on Auditing and Computer Technology. – 1993.
5. Golovko, V. Dimensionality Reduction and Attack Recognition using Neural Network Approaches / V. Golovko, L. Vaitsekhovich, P. Kochurko, U. Rubanau // In Joint Conference on Neural Networks (IJCNN-2007). – Orlando, FL, USA, 2007. – P. 2734–2739.
6. Vaitsekhovich, L. Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System / L. Vaitsekhovich, V. Golovko, U. Rubanau // In 10th International Conference on Pattern Recognition and Information Processing (PRIP-2009). – Minsk, Belarus, 2009. – P. 285–289.
7. Golovko, V. Neural Network and Artificial Immune System for Malware and Network Intrusion Detection / V. Golovko, S. Bezobrazov, P. Kachurka and L. Vaitsekhovich // Advanced in Machine Learning II. Springer Berlin Heidelberg. – 2010. – V. 263. – P. 485–513.
8. Головкин, В.А. Нейронные сети: обучение, организация и применение: Кн. 4: учеб. пособие для вузов / В.А. Головкин, общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.
9. 1999 KDD Cup Competition – Information on: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.

Abstract

In this article a hierarchical multi-agent model of intrusion detection system have been addressed. Its structure and operation algorithms are described. A single agent is represented by a combination of Nonlinear Principal Component Analysis Neural Network and Multi-layer Perceptron. The algorithm of agent interaction can be described with a directed graph. The model is able to perform a classification of network intrusions by classes as well as by types. Experiments indicate that the proposed model reduces the number of false positives, increases accuracy and can detect modified and even new attack instances.

Поступила в редакцию 18.05.2013 г.

ОБНАРУЖЕНИЕ И РАСПОЗНАВАНИЕ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ РЕЦИРКУЛЯЦИОННЫХ НЕЙРОННЫХ СЕТЕЙ

УДК 004.8.032.26

П.А. Кочурко,
БрГТУ, г. Брест

Аннотация

Представлены подходы к обнаружению и распознаванию сетевых атак с использованием рециркуляционных нейронных сетей. Реализованы технологии обнаружения аномалий и обнаружения злоупотреблений, объединение которых в рамках единого подхода позволяет получить высокую степень защи-

щенности компьютерных систем. Приводятся экспериментальные результаты, подтверждающие эффективность технологии.

Введение

Технологии обнаружения атак – важное звено в цепи средств обеспечения информационной безопасности,

противостоящих угрозам реализации уязвимостей. Каждая вторая организация в течение 2009–2010 годов зафиксировала различные атаки на свои информационные ресурсы, а 45,6 % из них подверглись целенаправленному нападению [1]. В 2011 году глобальный ущерб от атак на компьютерные информационные технологии превысил 250 млрд долл. США в год [2].

Основными недостатками существующих подходов к обнаружению атак (в первую очередь – на основе правил) являются: слабая способность обнаружения новых, неизвестных ранее или модифицированных атак; недостаточно высокая степень адаптивности; необходимость постоянного обновления баз правил, а значит – зависимость качества функционирования системы от компании-разработчика и качества сигнатур, полученных от поставщика.

Исследователи обращаются к большому количеству технологий (статистический анализ, деревья решений, искусственные иммунные системы, нечеткая логика и др.), среди которых стоит выделить подходы на основе искусственных нейронных сетей (ИНС), поскольку они сочетают высокое качество распознавания и классификации со способностью к адаптации и обобщению данных. В данной работе предлагается новое решение задачи обнаружения и распознавания сетевых атак на основе нелинейных рециркуляционных нейронных сетей (РНС). Оно объединяет в едином подходе парадигмы обнаружения аномалий и обнаружения некорректного поведения для лучшего распознавания известных атак и обнаружения новых и модифицированных сетевых атак.

РНС как детектор далеко отстоящих векторов

Рециркуляционные нейронные сети отличаются от других ИНС тем, что информация, подающаяся на вход, в том же виде восстанавливается на выходе. В процессе обучения весовые коэффициенты РНС настраиваются таким образом, чтобы минимизировать среднеквадратичную ошибку для всех тренировочных входных векторов. Итогом такого обучения станет то, что в процессе функционирования РНС подаваемые на вход векторы будут восстанавливаться на выходе тем более точно, чем больше они схожи с векторами из тренировочного набора. Далеко отстоящие векторы, в свою очередь, будут восстанавливаться недостаточно корректно.

Численная характеристика, которая позволяет судить о том, насколько данный входной вектор «похож» или «не похож» на вектор из тренировочного набора – ошибка реконструкции вектора:

$$E^k = \sum_{j=1}^{N(X)} (\bar{X}_j^k - X_j^k)^2, \quad (1)$$

где $N(X)$ – количество параметров во входном векторе X (ранг первого и последнего слоев РНС). При этом, чем меньше ошибка реконструкции (1), тем больше входной вектор похож на векторы тренировочного набора.

РНС-детекторы атак

и их совместное функционирование

В рамках СОА детекторы на базе нелинейных РНС могут использоваться в разных ролях в зависимости от того, на каком наборе данных они обучены.

Детектор аномалий. При обучении на нормальном трафике в автоматическом режиме РНС-детектор получает

и сохраняет для дальнейшего использования информацию о явных и неявных закономерностях поведения. В процессе функционирования такой детектор определяет соединения, не принадлежащие к классу нормальных, то есть атаки (рисунок 1).

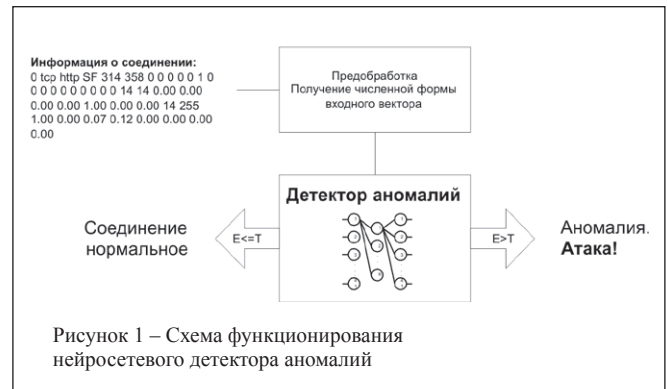


Рисунок 1 – Схема функционирования нейросетевого детектора аномалий

Детектор злоупотреблений. РНС может обучаться на соединениях-атаках, тем самым инкапсулируя информацию не о нормальном поведении, а шаблоны некорректного поведения. В этом случае в процессе функционирования сигналом об атаке будет ошибка реконструкции ниже установленного порога (2), в противном случае входной вектор не относится к атакам и является нормальным соединением (рисунок 2).

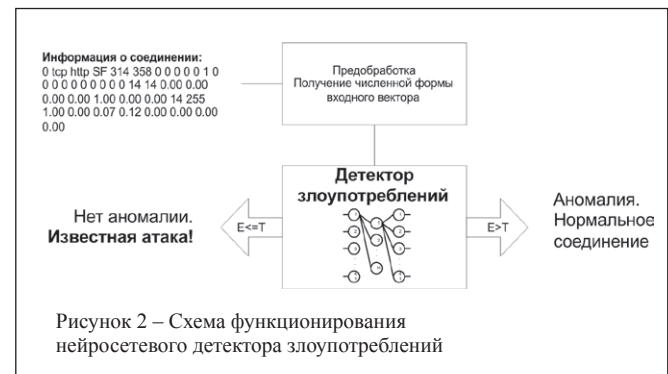
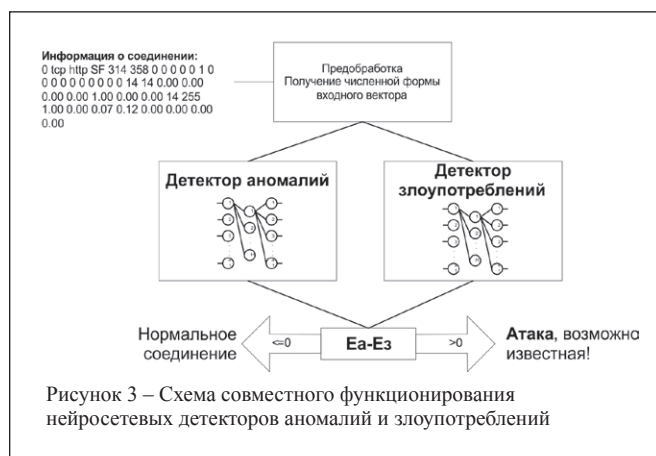


Рисунок 2 – Схема функционирования нейросетевого детектора злоупотреблений

Ансамбль детекторов аномалий и злоупотреблений. При совместном использовании детектора аномалий и детектора злоупотреблений на базе РНС решение принимается не по двоичным векторам результатов работы каждого детектора, а непосредственно по их выходным данным. Использование нейродетекторов аномалий и злоупотреблений на базе РНС одинаковой архитектуры, обученных до одинакового уровня ошибки, позволяет произвести принятие решения исходя из ошибок реконструкции (1) на обоих детекторах:

$$\begin{cases} X \in A_N, & \text{если } E_A \leq E_3, \\ X \in A_P, & \text{если } E_A > E_3, \end{cases} \quad (2)$$

где E_A – ошибка реконструкции детектора аномалий, E_3 – ошибка реконструкции детектора злоупотреблений, A_N – нормальные соединения, A_P – соединения-атаки (рисунок 3).



Детекторы отдельных классов атак являются производным от детекторов злоупотреблений на базе РНС. Нейросетевой детектор определяет сходство входного вектора с векторами из тренировочного набора. При обучении РНС не на всем наборе вредоносного трафика, а только на выборке из атак конкретного класса, детектор сможет определить принадлежность входного образа именно к данному классу атак. Далеко отстоящие вектора (ошибка реконструкции) (1) превышает пороговое значение) в этом случае не будут являться нормальными соединениями, а могут быть охарактеризованы как соединения, не принадлежащие данному классу атак.

Классификатор на базе РНС-детекторов. Описанные выше детекторы отдельных классов способны оценивать принадлежность входного вектора к классам по отдельности. Для определения класса сетевой атаки детекторы отдельных классов объединяются в общий классификатор. Предложенный классификатор состоит из N детекторов отдельных классов на базе рециркуляционных нейронных сетей, каждый из которых имеет порог T_i , и при реконструкции входного образа выдает ошибку реконструкции E_i . Для приведения оценок детекторов, обученных в разных условиях, к сравнимым значениям, ошибка реконструкции масштабируется по порогу: $\delta_i = E_i / T_i$ – относительная ошибка реконструкции. Чем меньше δ_i , тем более вероятна принадлежность входного образа X к классу A_i .

Система, использующая метод совокупного классификатора, может гибко изменяться и подстраиваться под новые входные данные: соединения, определенные как аномальные по отношению ко всем детекторам, формируют новый класс, для которого обучается новый детектор. Таким образом, изначально в системе может быть только детектор аномалий, обученный на нормальном трафике. В дальнейшем, при обнаружении им аномальных соединений – атак – для их последующего распознавания могут быть обучены соответствующие детекторы (рисунок 4).

Результаты тестирования

В качестве критериев для сравнения эффективности предложенного подхода с существующими методами использовались следующие показатели: FPR – уровень ложных срабатываний, FNR – уровень пропуска цели,



ACC – точность классификации, CR и CR_i – уровень распознавания в рамках всего набора данных или i -го класса атак. Для обучения и тестирования детекторов использовалась база данных DARPA/KDD [3], содержащая атаки 22 типов, принадлежащие четырем классам – DOS, U2R, R2L, Probe, а также нормальные соединения.

Лучшие методы, не использующие нейронные сети, имеют ошибки FPR и FNR до 10 %, а при высоком качестве распознавания атак класса DOS ($CR_{dos}=97-99\%$), качество распознавания атак классов R2L и U2R значительно ниже – $CR_{r2l}=1-46\%$, $CR_{u2r}=2-50\%$ [4–5]. В свою очередь, нейросетевые подходы показывают значительно более высокие результаты. Наименьший показатель вероятности ошибок первого и второго рода – 0,3–1,2 %, и распознавание всех классов атак на уровне 98–99 % [6–7]. Однако, при таких высоких показателях качества обнаружения и распознавания известных атак не обеспечивается обнаружение новых, неизвестных атак.

В таблицах 1 и 2 представлены результаты обнаружения и распознавания атак предложенными методами.

Таблица 1 – Результаты тестирования методик обнаружения атак

Технология	FPR, %	FNR, %	ACC, %
Детектор аномалий	12,93	0,36	97,18
Детектор злоупотреблений	0,04	2,73	97,96
Совместное функционирование	0,02	1,79	98,36
Совокупный классификатор 4-х классов атак	3,74	0,01	99,23
Совокупный классификатор 22-х типов атак	1,94	0,14	99,51

Таблица 2 – Результаты тестирования методики распознавания атак

	CR_{dos}^* , %	CR_{probe}^* , %	CR_{r2l}^* , %	CR_{u2l}^* , %	CR , %
Классификатор 4-х классов атак	99,31	99,12	97,86	100,0	98,78
Классификатор 22-х типов атак	99,78	95,18	97,60	100,00	99,40

Полученные результаты превосходят результаты пространственных подходов (см. таблицы 3–4), в том числе нейросетевых (см. таблицы 5–6).

Таблица 3 – Средние результаты обнаружения при помощи различных технологий [8, 9, 5, 10]

Технология	FPR, %	FNR, %
Победитель KDD-99, Bagged Boosting	0,5	25,4
Правила	2	10
Кластеризация	10	7
K-NN	8	9
SVM	10	2

Таблица 4 – Результаты распознавания классов атак в некоторых исследованиях [11, 10, 13]

	CR_{dos}^* , %	CR_{probe}^* , %	CR_{r2l}^* , %	CR_{u2l}^* , %
Гауссовский классификатор	82,4	90,2	9,6	22,8
K-NN	97,3	87,6	6,4	29,8
Алгоритм ближайшего кластера	97,1	88,8	3,4	2,2
Лидер-алгоритм	97,2	83,8	1,0	6,6
Алгоритм гиперсферы	97,2	84,8	1,0	8,3
Fuzzy Art Map	97,0	77,2	3,7	6,1
Дерево решений C4.5	97,0	80,8	4,6	1,8
Bagged Boosting	97,1	83,3	13,2	8,4
Деревья решений	99,8	50,0	33,3	50,0
Байесовы сети	99,7	52,6	46,2	25,0

Как видим, при достаточно высоком уровне распознавания атак классов probe и dos большинство подходов очень плохо распознают атаки наиболее опасных типов – u2l и r2l.

Таблица 5 – Результаты обнаружения при помощи известных нейросетевых методов

Технология	FPR, %	FNR, %
Модульная структура из MLP [11] на известных атаках	9	7
Модульная структура из MLP [11] на неизвестных атаках	18	14
MLP [14]	0,8	5,8
MLP [15]	3	23
MLP [16]	неизвестно	0,4
Сети Элмана [15]	0	23
Иерархия SOM [17]	1,4	9,3
Flexible Neural Tree [18]	0,3	1,2
Fuzzy NN [19] на неизвестных атаках	–	31,2

Таблица 6 – Результаты распознавания классов атак при помощи нейросетевых методов

	CR_{dos}^* , %	CR_{probe}^* , %	CR_{r2l}^* , %	CR_{u2l}^* , %
Flexible Neural Tree [18]	98,8	99,3	98,8	99,9
Fuzzy NN [19]	100,0	100,0	99,8	40,0
Иерархия PCA-сетей [20]	100,0	100,0	97,2	–
PCA-сети и SOM [20]	99,0	75,2	77,0	–
Иерархия SOM [17]	96,9	81,3	0,0	1,1
MLP и нечеткая кластеризация [11]	99,9	48,1	93,2	83,3
RBF [20]	98,8	98,0	97,2	–

Заключение

Экспериментальное тестирование показало, что точность обнаружения и распознавания известных атак совокупным классификатором на базе РНС-детекторов отдельных классов находится на уровне 99 %, а качество обнаружения неизвестных атак – на уровне 98 %. В зависимости от количества

входящих в классификатор детекторов от 80 % до 98 % обнаруженных неизвестных атак распознаются как атаки класса «неизвестная атака». Совместное использование обнаружения аномалий и обнаружения злоупотреблений в рамках одного подхода позволяет увеличить точность обнаружения и распознавания, и обеспечить требуемую адаптивность и масштабируемость системы.

Литература:

1. CSI Computer Crime and Security Survey 2010 [Electronic resource] Mode of access: <http://gocsi.com/survey>. – Date of access: 11.01.2011.
2. Proposal for a Regulation Of The European Parliament And Council concerning the European Network and Information Security Agency (ENISA) [Electronic resource] Mode of access: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2010/sec_2010_1126_en.pdf. – Date of access: 11.01.2011.
3. KDD Cup'99 Competition. [Electronic resource] Mode of access: <http://kdd.ics.uci.edu/databases/kddcup99/>

kddcup99.html. – Date of access: 20.04.2009.

4. Srilatha, C. et al. Feature deduction and ensemble design of intrusion detection systems / C. Srilatha, A. Ajith, Th. Johnson. – Computers & Security. – 2005. – №24. – P. 295–307.

5. Eskin, E. A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data / E. Eskin // Data Mining for Security Applications; Eds.: D. Barbar, S. Jajodia. – Boston, Kluwer Academic Publishers, 2002.

6. Jahanbani, A. and Karimi, H. A new Approach for Detecting Intrusions Based on the PCA Neural Networks / A. Jahanbani, H. Karimi. – Journal of Basic and Applied Scientific Research. – 2012. – V. 2 (1). – P. 672–679.

7. Anyanwu, L.O. Scalable Intrusion Detection with Recurrent Neural Networks / L.O. Anyanwu, L. Keengwe, G.A. Arome. – International Journal of Multimedia and Ubiquitous Engineering. – 2011. – V. 6, №1.

8. Lee, W. A framework for constructing features and models for intrusion detection systems / W. Lee, S.J. Stolfo // ACM Trans. on Inform. and System Security. – 2000. – №3(4). – P. 227–261.

9. Frank, J. Artificial intelligence and intrusion detection: Current and future directions / J. Frank // The 17th National Computer Security Conference: proceedings, Baltimore, MD, 1999 / National Institute of Standards and Technology [Electronic resource] – 1999. – Mode of access: <http://svn.assembla.com/svn/odinIDS/Egio/temp/frank94artificialCiteSeer.pdf>. – Date of access: 02.02.2010.

10. Pfahringer, B. Winning the KDD99 Classification Cup: Bagged Boosting / B. Pfahringer // SIGKDD Explorations. – 2000. – V. 1, №2. – P. 65–66.

11. Wang, G. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering / G. Wang, J. Hao, J. Ma, L. Huang // Expert Systems with Applications. – 2010. – №2. – P. 6225–6232.

12. Жульков, Е.В. Построение модульных нейронных сетей для обнаружения классов сетевых атак: дис. ... канд. техн. наук: 05.13.19 / Е.В. Жульков. – СПб., 2007. – 155 л.

13. Sabhnani, M. Application of Machine Learning Algorithms to KDD Intrusion detection dataset within Misuse detection context / M. Sabhnani, G. Serpen // The

international conference on Machine Learning: Models, technologies and Applications: proceedings, 2003. – 2003. – P. 209–215.

14. Saravanakumar, S. Development and Implementation of Artificial Neural Networks for Intrusion Detection in Computer Network / S. Saravanakumar, Umamahchhari, D. Jayalakshmi, R. Sugumar // International Journal of Computer Science and Network Security. – 2010. – V. 10, №7. – P. 271–275.

15. Ghosh, A.K. Learning program behavior profiles for intrusion detection / A.K. Ghosh, A. Schwartzbard, M. Schatz // 1st USENIX Workshop on Intrusion Detection and Network Monitoring: proceedings, Santa Clara, CA, 1999, 9–12 April / USENIX. – USENIX, 1999. – P. 51–62.

16. Ali, A. Intelligent Adaptive Intrusion Detection Systems Using Neural Networks (Comparative study) / A. Ali, A. Saleh, T. Badawy // International Journal of Video & Image Processing and Network Security. – 2010. – V. 10, №1. – P. 1–12.

17. Kayacik, H.G. A Hierarchical SOM-Based Intrusion Detection System / H.G. Kayacik, A.N. Zincir-Heywood, M. Heywood // Engineering Applications of Artificial Intelligence. – 2006. – №9. – P. 439–451.

18. Novosad, T. Fast Intrusion Detection System based on Flexible Neural Tree / T. Novosad, J. Platos, V. Snasel, A. Ajith // Sixth International Conference on Information Assurance and Security (IAS): proceedings, USA. – 2010. – P. 142–147.

19. Muna, M.J. Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network / M.J. Muna, M. Mehrotra // International Journal of Computer Science and Security. – 2010. – V. 4 (3). – P. 258–294.

20. Liu, G. A hierarchical intrusion detection model based on the PCA neural networks / G. Liu, Z. Yi, S. Yang // Neurocomputing. – 2007. – P. 1561–1568.

Abstract

The approach to network intrusion detection and recognition with use of recirculation neural networks is presented. The technologies of anomaly detection and misuse detection are utilized and combined into one technology. Such technology shows high degree of computer system protection. Experimental results prove efficiency of technology.

Поступила в редакцию 18.05.2013 г.

О ВЫЯВЛЕНИИ ЗАВИСИМОСТИ БОЛЬШОЙ ГЛУБИНЫ В ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ НА ОСНОВЕ ЦЕПИ МАРКОВА УСЛОВНОГО ПОРЯДКА

УДК 519.2: 003.26

Аннотация

В статье рассматривается цепь Маркова условного порядка, которая относится к классу так называемых «мало-параметрических» моделей дискретных временных рядов. Данная модель использовалась для статистического анализа выходных последовательностей криптографических

генераторов. Представлены результаты компьютерных экспериментов.

Введение

Методы теории вероятностей и математической статистики широко применяются в задачах защиты информации

**М.В. Мальцев,
НИИ ПМИ БГУ, г. Минск**

для тестирования криптографических генераторов [1]. Генератор, используемый в реальных приложениях, должен порождать выходную последовательность, неотличимую от равномерно распределенной случайной последовательности (РПСР) [1], часто называемой также «чисто случайной» последовательностью, элементы которой независимы в совокупности и имеют равномерное распределение вероятностей. Известным примером отклонения от РПСР является используемый в протоколах SSL и WEP генератор RC4 [2], в котором несколько «смещено» распределение вероятностей второго байта: вероятность получить нуль в этом байте равна $1/128$, а не $1/256$. Для обнаружения отклонения от модели «чистой случайности» применяется статистическое тестирование, задача которого – установить, обладает ли выходная последовательность исследуемого генератора определенными свойствами РПСР. Статистические тесты объединяются в так называемые батареи тестов, примерами которых являются батарея NIST [3], разработанная Лабораторией Информационных технологий Национального Института стандартов и технологий США, батарея DIEHARD [4] разработанная Джорджем Марсальей, батарея Дональда Кнута [5].

Как уже отмечалось, элементы РПСР должны быть независимыми, однако вышеприведенные батареи тестов не позволяют определять зависимости большой глубины, поэтому для их выявления требуются дополнительные исследования. Математической моделью, в которой будущее состояние зависит от s прошлых, является цепь Маркова s -го порядка. Но число независимых параметров D полностью связано с увеличением порядка: $D = (N-1)N^s$, поэтому использовать ее напрямую для определения зависимостей большой глубины в выходных последовательностях криптографических генераторов практически невозможно. Для решения этой проблемы разрабатываются так называемые «малопараметрические» модели цепи Маркова s -го порядка, которые представляют собой частные случаи полностью связанной цепи Маркова, матрица вероятностей одношаговых переходов которых может быть описана значительно меньшим числом параметров, чем D . Примерами таких моделей являются цепь Маркова с частичными связями [6], модель Рафтери [7]. В настоящей статье рассматривается «малопараметрическая» модель, предложенная в [8, 9], – цепь Маркова условного порядка.

Цепь Маркова условного порядка

Приведем математическое описание цепи Маркова условного порядка. Примем обозначения: N – множество натуральных чисел; $A = \{0, 1, \dots, N-1\}$ – пространство состояний мощности $N \in \mathbb{N}$, $2 \leq N < \infty$; $J_n^m = (j_n, j_{n+1}, \dots, j_m) \in A^{m-n+1}$, $m, n \in \mathbb{N}$, $m \geq n$, – мультииндекс; $\langle J_n^m \rangle = \sum_{k=n}^m N^{k-n} j_k \in \{0, 1, \dots, N^{m-n+1}-1\}$ – числовое представление мультииндекса J_n^m ; $F_k^l G_n^m$ – конкатенация мультииндексов F_k^l и G_n^m ; $\{x_t \in A : t \in \mathbb{N}\}$ – однородная цепь Маркова s -го порядка ($2 \leq s < \infty$) с $(s+1)$ -мерной матрицей вероятностей одно-

шаговых переходов $P = (P_{J_1^{s+1}})$, $P_{J_1^{s+1}} = P\{x_{t+s} = j_{s+1} | x_{t+s-1} = j_s, \dots, x_t = j_1\}$, $J_1^{s+1} \in A^{s+1}$, $t \in \mathbb{N}$; $L \in \{1, \dots, s-1\}$, $K = N^L - 1$ – натуральные числа; $Q^{(1)}, \dots, Q^{(M)}$ – семейство M ($1 \leq M \leq K+1$) различных квадратных стохастических матриц порядка N : $Q^{(m)} = (q_{i,j}^{(m)})$, $0 \leq q_{i,j}^{(m)} \leq 1$, $\sum_{j \in A} q_{i,j}^{(m)} = 1$, $i, j \in A$, $1 \leq m \leq M$; $v_{l,y}(J_1^l) = \sum_{t=1}^{n-s} I\{x_{t+s-l-y+1} = j_1, x_{t+s-l+2} = j_2^l\}$, $l \geq 2$, $y \geq 0$, $l+y \leq s+1$, – частота состояния $J_1^l \in A^l$ с пропуском в y символов между j_1 и J_2^l .

Цепь Маркова s -го порядка ($2 \leq s < \infty$) $\{x_t \in A : t \in \mathbb{N}\}$ называется цепью Маркова условного порядка [8, 9], если ее вероятности одношаговых переходов имеют вид:

$$P_{J_1^{s+1}} = \sum_{k=0}^K I\{\langle J_{s-L+1}^s \rangle = k\} q_{j_{b_k}, j_{s+1}}^{(m_k)}, J_1^{s+1} \in A^{s+1} \quad (1)$$

где $1 \leq m_k \leq M \leq K+1$, $1 \leq b_k \leq s-L$, $0 \leq k \leq K$, $\min_{0 \leq k \leq K} b_k = 1$, при этом в последовательности $m_0, \dots, m_K$ встречаются все элементы множества $\{1, 2, \dots, M\}$. Последовательность L элементов J_{s-L+1}^s определяющая условие в формуле (1), называется базовым фрагментом памяти (БФП), L – длина БФП; величина $s_k = s - b_k + 1$ называется условным порядком. Таким образом, состояние x_t процесса в момент времени t зависит не от всех s предыдущих состояний, как это было бы для полностью связанной цепи Маркова порядка s , а от $L+1$ состояний (j_{b_k}, J_{s-L+1}^s). Отметим, что при $L = s-1$, $s_0 = \dots = s_K = s$, получаем полностью связанную цепь Маркова порядка s .

Если последовательность, порождаемая криптографическим генератором, представляет собой эргодическую цепь Маркова, то с течением времени текущее распределение вероятностей стремится к стационарному распределению вероятностей. Поэтому для исследования надежности таких генераторов важно определить условия, при которых стационарное распределение вероятностей является равномерным. Следующая теорема устанавливает такие условия для цепи Маркова условного порядка.

Теорема. Если цепь Маркова условного порядка (1) – эргодическая, то ее стационарное распределение вероятностей является равномерным тогда и только тогда, когда:

$$\begin{cases} Q^{(m_k)} = N^{-1} \cdot \mathbf{1}_{N \times N}, \text{ если } s_k \in \{L+1, \dots, s-1\}, \\ Q^{(m_k)} - \text{бистохастическая матрица, т.е.} \\ \left\{ \begin{aligned} & \text{т.е. } \sum_{i \in A} Q_{ij}^{(m_k)} = 1, \forall j \in A, \text{ если } s_k = s, \end{aligned} \right. \end{cases}$$

где $\mathbf{1}_{N \times N}$ – $(N \times N)$ -матрица, все элементы которой равны 1, $k = 0, 1, \dots, K$.

В дальнейшем будем рассматривать случай, когда каждому значению БФП соответствует своя матрица вероятностей переходов, т.е. $m_k = k+1$, $k = 0, 1, \dots, K$.

В [8] построены оценки максимального правдоподобия вероятностей переходов, условных порядков:

$$q_{j_0, J_{L+1}}^{(k+1)} = \begin{cases} \sum_{J_1^L \in A^L} I\{\langle J_1^L \rangle = k\} \frac{v_{L+2, s_k-L-1}(J_0^{L+1})}{v_{L+1, s_k-L-1}(J_0^L)}, & \text{если } v_{L+1, s_k-L-1}(J_0^L) > 0, \\ 1/N, & \text{если } v_{L+1, s_k-L-1}(J_0^L) = 0, \end{cases} \quad (2)$$

$$s_k = \arg \max_{L+1 \leq y \leq s} \sum_{J_1^L \in A^L} I\{< J_1^L > = k\} \sum_{J_0, J_{L+1} \in A} v_{L+2, y-L-1}(J_0^{L+1}) \ln \hat{q}_{j_0, j_{L+1}}^{(k+1)}$$

$$k = 0, \dots, K.$$

В [9] на основе асимптотических свойств оценок (2) построен статистический тест для проверки гипотез о значении матриц вероятностей одношаговых переходов $Q^{(k)}$, $k = 1, \dots, K+1$: $H_0 = \{Q^{(1)} = Q_0^{(1)}, \dots, Q^{(K+1)} = Q_0^{(K+1)}\}$, $H_1 = \bar{H}_0$, где $Q_0^{(1)}, \dots, Q_0^{(K+1)}$ – некоторые фиксированные матрицы вероятностей переходов. Если $N = 2$, $A = \{0, 1\}$, все элементы матриц $Q_0^{(1)}, \dots, Q_0^{(K+1)}$ равны $1/2$, то тест позволяет обнаруживать отклонения от PPCП и имеет вид (порядок цепи Маркова, длина БФП и условные порядки фиксированы):

$$\text{принимается } \begin{cases} H_0(\text{PPCП}): \rho \leq \Delta, \\ H_1: \rho > \Delta, \end{cases} \quad (3)$$

$$\text{где } \rho = \sum_{J_0^{L+1} \in A^{L+1}} \sum_{k=0}^K I\{< J_1^L > = k\} 2v_{L+1, s_k-L-1}(J_0^L) (\hat{q}_{j_0, j_{L+1}}^{(k+1)} - 1/2),$$

$\Delta = G_u^{-1}(1-\alpha)$ – квантиль уровня $1-\alpha$ ($\alpha \in (0, 1)$) стандартного χ^2 -распределения с $u = 2^{L+1}$ степенями свободы.

3 Результаты компьютерных экспериментов

Проведена серия компьютерных экспериментов на модельных и реальных данных. Во всех экспериментах уровень значимости $\alpha = 0.05$.

3.1 Модельные данные

При верной гипотезе H_0 генерировалось $U = 1000$ реализаций цепи Маркова условного порядка длительности $n = 100000$ с параметрами: $N = 2$, $A = \{0, 1\}$, $s = 16$, $L = 4$, $(b_0, \dots, b_K) = (11, 1, 9, 3, 2, 7, 12, 5, 6, 10, 1, 4, 10, 1, 8, 9)$, все элементы матриц вероятностей одношаговых переходов равны $1/N = 1/2$. В ходе эксперимента вычислялась величина $\hat{\alpha} = \frac{1}{U} \sum_{u=1}^U I\{\rho_u > \Delta\}$, где ρ_u – значение статистики

ρ , вычисленной по u -ой реализации, которая характеризует долю решений в пользу H_1 . При вычислении ρ_u все значения параметров модели за исключением матриц вероятностей одношаговых переходов полагались известными. На рисунке 1 по горизонтальной оси откладывался номер реализации, по вертикальной – значение тестовой статистики ρ , точками отмечались величины ρ_u , сплошной линией



Рисунок 1 – Результаты экспериментов для модельных данных

изображен порог теста $\Delta = G_{32}^{-1}(0.95) \approx 46.2$. Значение $\hat{\alpha} = 0.045$, вычисленное в ходе эксперимента, согласуется с теоретическими результатами.

Аналогичный результат был получен в экспериментах, в которых параметры $(b_0, \dots, b_K)$ полагались неизвестными и для вычисления тестовой статистики выбирались случайным образом из множества допустимых значений ($1 \leq b_k \leq s-L = 12$).

3.2 Реальные данные

Исследовались выходные последовательности самосжимающегося генератора [10] и регистра сдвига с переменной обратной связью [11]. Генерировалось по 100 реализаций каждого генератора длительности $n = 100\,000$ со случайно выбранным начальным заполнением регистров. При фиксированной длине БФП L изменялся порядок цепи Маркова от $L+1$ до 100. При этом первая половина последовательности длины $n_{0.5} = 50\,000$ использовалась для построения оценок условных порядков по формуле (2), вторая половина – для вычисления тестовой статистики ρ . Для каждой пары (s, L) вычислялась величина $\hat{\alpha}$, которая отмечалась на рисунках точкой (по горизонтальной оси откладывался порядок s). Сплошная линия на рисунках – уровень значимости α . Характеристический многочлен самосжимающегося генератора $f(x) = x^{36} + x^{11} + 1$ (период выходной последовательности $T_1 = 2^{18}$), характеристические многочлены регистра сдвига с переменной обратной связью $f_1(x) = x^{23} + x^5 + 1$, $f_2(x) = x^{23} + x^9 + 1$, управляющий многочлен $g(x) = x^{18} + x^{16} + x^{11} + x^4 + 1$ (период выходной последовательности $T_2 \geq 2^{18} - 1$). Все вышеперечисленные многочлены являются примитивными. Результаты представлены на рисунке 2 и рисунке 3.

Заключение

Таким образом, в статье представлены результаты обнаружения отклонения от модели «чисто случайной» последовательности выходных последовательностей самосжимающегося генератора и регистра сдвига с переменной обратной связью. Для обнаружения отклонений использовалась цепь Маркова условного порядка – математическая модель, учитывающая зависимости высоких порядков при относительно небольшом числе независимых параметров. Результаты компьютерных экспериментов демонстрируют применимость теста (3) при определенных значениях s и L . Отметим нелинейный характер зависимости $\hat{\alpha}$ как от порядка s , так и от длины БФП L . К примеру, для самосжимающегося генератора при $s = 3$ число решений в пользу H_1 больше, чем при $s = 4$, а при $L = 6$ число решений в пользу H_1 наибольшее при $L < 50$.

Литература:

1. Математические и компьютерные основы криптологии / Ю.С. Харин [и др.]. – Минск: Новое знание, 2003.
2. Sepehrdad, P. Discovery and Exploitation of New Biases in RC4 / P. Sepehrdad, S. Vaudenay, M. Vuagnoux // Lecture Notes in Computer Science. 2011. – V. 6544. – P. 74–91.
3. A statistical test suite for random and pseudorandom number generators for cryptographic applications: NIST Special Publication 800-22 Rev. 1a. National Institute of Standards and Technology, 2010. – 131 p.

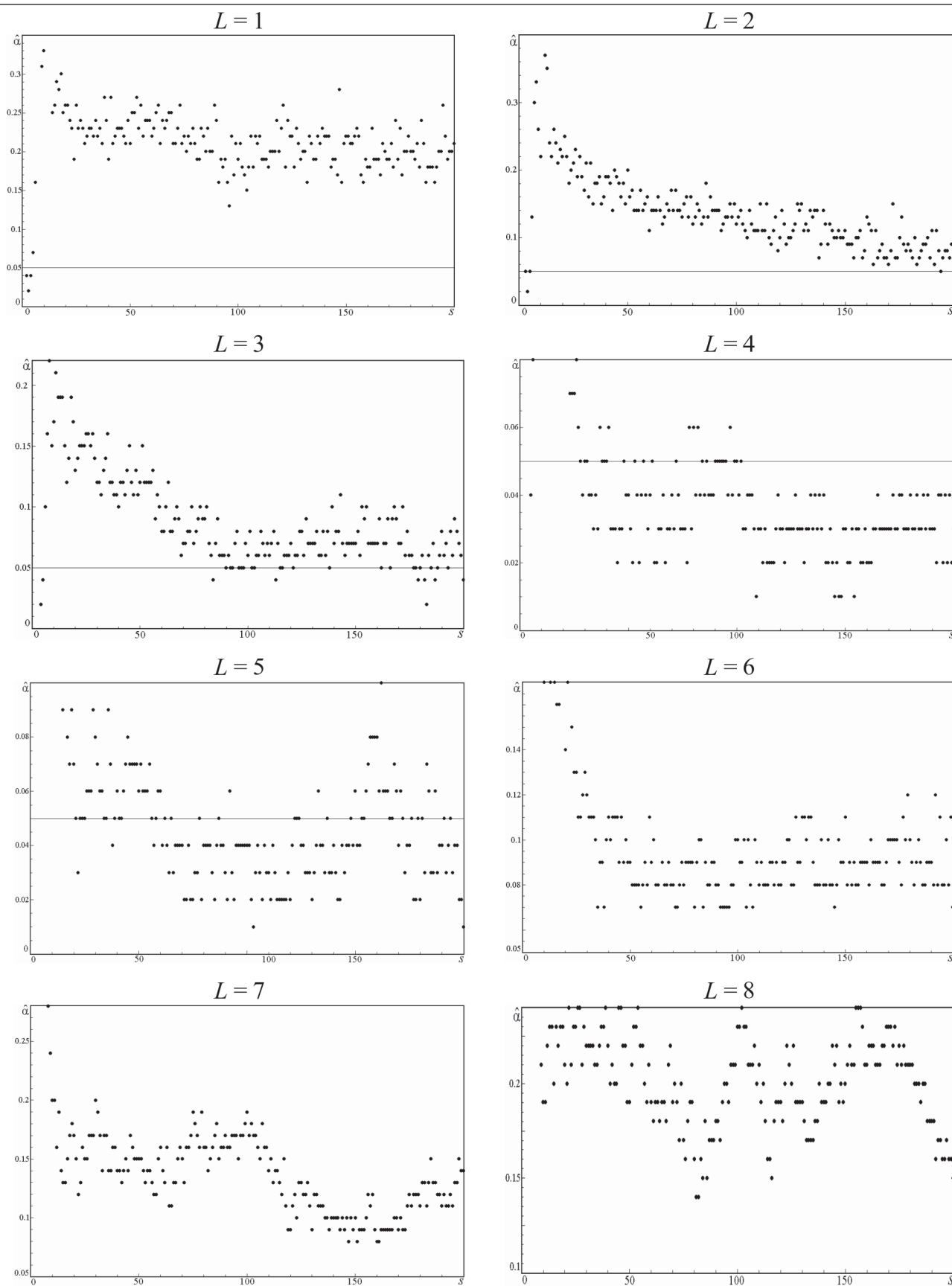


Рисунок 2 – Результаты экспериментов для самосжимающего генератора

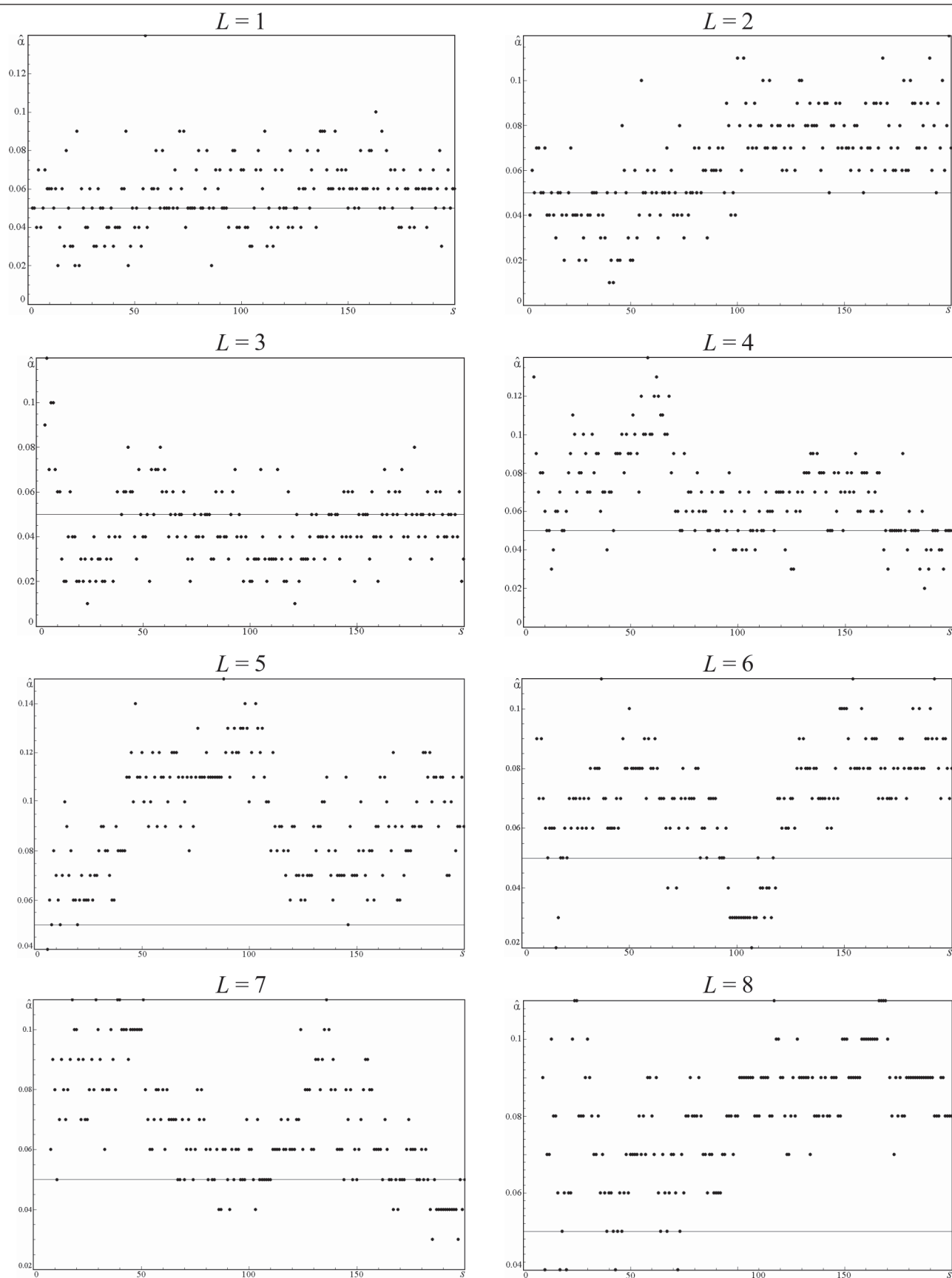


Рисунок 3 – Результаты экспериментов для регистра сдвига с переменной обратной связью

4. Marsaglia, G. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness / G. Marsaglia [Electronic resource]. – Florida State University, 1995.

5. Искусство программирования: в 3 т. Т. 1: Полужисленные методы / Д.Э. Кнут. – М.: Вильямс, 2007.

6. Харин, Ю.С. Цепь Маркова с частичными связями ЦМ(s, r) и статистические выводы о ее параметрах / Ю.С. Харин, А.И. Петлицкий // Дискретная математика. – 2007. – Т. 19, № 2. – С. 109–130.

7. Raftery, A.E. A model for high-order Markov chains / A.E. Raftery // J. Royal Statistical Society. – 1985. – V. B-47, № 3. – P. 528–539.

8. Харин, Ю.С. Алгоритмы статистического анализа цепей Маркова с условной глубиной памяти / Ю.С. Харин, М.В. Мальцев // Информатика. – 2011. – №1. – С. 34–43.

9. Харин, Ю.С. Статистическая проверка гипотез о параметрах цепи Маркова условного порядка / Ю.С. Харин, М.В. Мальцев // Вестн. НАН Беларуси, Серия. физ.-мат. наук. – 2012. – №3. – С. 5–12.

10. Meier, W. The self-shrinking generator / W. Meier, O. Staffelbach // Advances in Cryptology – EUROCRYPT 94. 1995. Springer-Verlag LNCS 950. – P. 205–214.

11. Основы криптографии / А.П. Алферов [и др.]. М.: Гелиос АРБ, 2001.

Abstract

The paper deals with Markov chain of conditional order, which is a parsimonious model of discrete time series. The model was used for statistical analysis of cryptographic generators output sequences.

The results of computer experiments are presented.

Поступила в редакцию 18.05.2013 г.

ПОВТОРЯЕМОСТЬ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СОСТОЯНИЙ ПОЛНОЦИКЛОВЫХ АВТОНОМНЫХ АВТОМАТОВ

УДК 519.711.2, 519.713.2.

А.Н. Гайдук,
НИИ ППМИ БГУ, г. Минск

Аннотация

В настоящей работе рассматривается полноцикловой генератор псевдослучайной последовательности. Попадание генератора псевдослучайной последовательности в ранее использованное состояние означает повторную выработку выходной последовательности, что является крайне нежелательным явлением. Анализ этого события для случая когда длины вырабатываемой псевдослучайной последовательности полноциклового генератора являются случайными величинами приведен в работе [1], случай когда длины вырабатываемой псевдослучайной последовательности являются произвольными фиксированными величинами рассмотрен в работе [2]. В настоящей работе для случая отрезков равной длины вырабатываемой псевдослучайной последовательности получена более простая модель, которая согласуется с результатами работы [1]–[2].

Введение

Будем рассматривать в качестве генератора псевдослучайной последовательности автономный автомат $U = (S, Z, \varphi, \psi)$, где $S = \{s_1, s_2, \dots, s_N\}$ – конечное множество состояний, $Z = \{0, 1\}$ – конечное множество выходных символов, $\varphi: S \rightarrow S$ – функция переходов, $\psi: S \rightarrow Z$ – функция выходов. Канонические уравнения функционирования автономного автомата U имеют вид:

$$\begin{aligned} s(t+1) &= \varphi(s(t)) \\ z(t) &= \psi(s(t)), \quad t \geq 0, \end{aligned}$$

$s(0)$ – начальное состояние.

Под состоянием генератора понимаем состояние описывающего его автономного автомата.

Постановка задачи

Пусть в процессе вычислений используется n отрезков последовательности псевдослучайных чисел, полученных с помощью полноциклового генератора. Будем отождествлять

начальное состояние $s_i = (s_{i,1}, \dots, s_{i,m})$ i -го отрезка последовательности псевдослучайных чисел с числом

$X_i = \sum_{k=1}^m s_{i,k} 2^{m-k}$. Через L_i обозначим длину i -го отрезка.

Будем считать, что случайные величины $X_1, \dots, X_n$ независимы в совокупности и при всех i :

$$P(X_i = k) = \frac{1}{2^m}, \quad k = 0, \dots, 2^m - 1.$$

Требуется оценить вероятность перекрытия n отрезков длин $L_1, \dots, L_n$.

Повторяемость последовательностей состояний случайной длины (модель М1)

В работе [1] исследовался случай, когда длины отрезков $L_1, \dots, L_n$ являются случайными величинами:

$$P(L_i = k) = p_k, \quad k = 1, \dots, N,$$

причем

$$P(1 \leq L_i \leq \frac{N}{2}) = 1.$$

В [1] доказана теорема, которая позволяет построить оценки снизу и сверху для вероятности неперекрывания отрезков $L_1, \dots, L_n$.

Повторяемость последовательностей состояний произвольной длины (модель М2)

В работе [2] получены результаты для отрезков произвольных длин. Пусть отрезки имеют следующие длины: $L_1, \dots, L_n$, где, вообще говоря, $L_i \neq L_j$ при $i \neq j$. Перекрывание отсутствует, если все пары отрезков не имеют перекрытий.

Теорема 1. Вероятность не перекрывания n отрезков длин $L_1, \dots, L_n$, $\sum_{j=1}^n L_j = L$, при цикле длины N автомата равна

$$\frac{(n-1)! C_{N-L+n-1}^{n-1}}{N^{n-1}}. \quad (1)$$

Повторяемость последовательностей состояний равной длины (модель М3)

Для случая отрезков равной длины в настоящей работе предлагается более простая формула. Предположим, что длины отрезков удовлетворяют следующему соотношению: $L_1 = L_2 = \dots = L_n = L_0$. Перекрытие отсутствует, если все пары отрезков не имеют перекрытий.

Теорема 2. Если мы можем пренебречь величиной $\frac{nL_0}{N}$, тогда вероятность не перекрытия n отрезков длин $L_1 = L_2 = \dots = L_n = L_0$, при цикле длины N автомата равна

$$\frac{(M-1) \dots (M-n+1)}{M^{n-1}}, \quad M = \frac{N}{2L_0}. \quad (2)$$

Доказательство

Действительно, поскольку мы пренебрегаем величиной $\frac{nL_0}{N}$, то мы можем свести задачу к следующей. Т.к. у нас отрезки равной длины, то мы их заменим точками, а общее число состояний автомата уменьшим в $2L_0$ раз. Обозначим $M = \frac{N}{2L_0}$. Тогда количество способов, которыми мы можем выбрать произвольную точку, равно M . А для того, чтобы не происходило перекрытий, мы будем выбирать следующую точку так, чтобы она не совпадала ни с какой предыдущей. Тогда искомая вероятность равна (2).

Заключение

Нами было рассмотрено 3 модели:

- повторяемость последовательностей состояний равной длины;
- повторяемость последовательностей состояний произвольной длины;
- повторяемость последовательностей состояний случайной длины.

Приведем некоторые численные результаты. Пусть $N = 10^{10}$, а длины отрезков неслучайны и одинаковы: $L_1 = L_2 = \dots = 10^4$. В таблице 1 представлены вероятности, вычисленные по моделям М2 и М3, а также вытекающих из теоремы 2 работы [1] оценок снизу и сверху для вероятностей не перекрытия отрезков модели М1.

Таблица 1 – Связь между моделями М1, М2 и М3

n	Модель М3	Модель М2	Модель М1	
			Оценка снизу	Оценка сверху
200	0.961	0.961	0.961	0.961
400	0.852	0.852	0.852	0.853
600	0.698	0.698	0.697	0.700
800	0.527	0.527	0.525	0.531
1000	0.368	0.368	0.365	0.372
1200	0.236	0.237	0.234	0.242
1400	0.140	0.140	0.138	0.145
1600	0.077	0.077	0.074	0.081
1800	0.039	0.039	0.037	0.042
2000	0.018	0.018	0.017	0.020

Литература:

1. Михайлов, В.Г. О повторяемости датчика псевдослучайных чисел при его многократном использовании / В.Г. Михайлов // Теория вероятн. и ее примен. – 1995. – Т. 40. – в. 4. – С. 786–797.
2. Бабаш, А.В. Криптография / А.В. Бабаш, Г.П. Шанкин. – М.: Солон-Р. – 2002. – 512 с.

Abstract

The full-cyclic generator of pseudorandom sequence is considered. Hit of the generator in earlier used state means that output sequence will be used twice that is the extremely undesirable phenomenon. The analysis of this event for a case when lengths of output sequences of the full-cyclic generator are random variables is provided in [1], a case when lengths of output sequences are any fixed values is considered in [2]. In this article for a case of equal length output sequences simpler model that is consistent with the results of [1]-[2] is presented.

Поступила в редакцию 18.05.2013 г.

ОЦЕНКА ЗАЩИЩЕННОСТИ ЦИФРОВЫХ СИГНАЛОВ АМ, ЧМ, ФМ, КАМ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

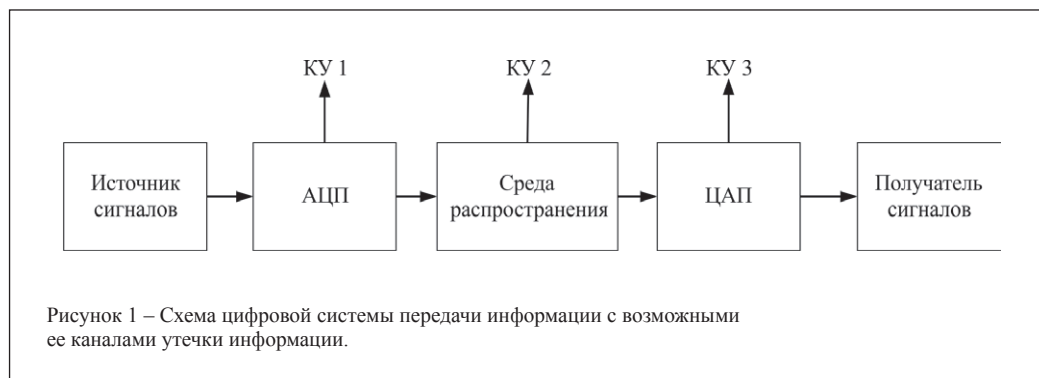
УДК 621.397.7:004.056.57

Д.С. Рябенко, В.К. Железняк
ПГУ, г. Полоцк

Аннотация

Исследуется оптимальный сигнал для оценки защищенности цифровых каналов утечки информации. Технология технической защиты информации формирует обобщенные требования к теории и технике передачи систем сигналов. Рассматривается система сигналов, используемая для передачи информации как совокупность сигналов, объединяемых единым правилом построения. Известно, что помехоустойчивость

– одно из основных требований к системе передачи. Предложены оптимальная система сигналов, обеспечивающая максимальную помехоустойчивость при минимальных отношениях энергии бита к спектральной плотности мощности шума в каналах утечки информации, методы оценки защищенности дискретных систем сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума, а также выбор и обоснование оптимального



сигнала, который позволит оценить защищенность цифровых каналов утечки информации.

Введение

Защищенность цифровых сигналов в канале утечки информации основана на формировании исходных требований, учитывающих свойства канала передачи сигнала, характеристики и параметры формируемых сигналов для передачи каналом передачи и их структура. Сигнал канала передачи оценивают средней мощностью передачи сигнала, его искажением, оцениваемым отношением энергии бита к спектральной плотности мощности шума, определяющим вероятность ошибки. Важнейшей задачей является обеспечение при их приеме помехоустойчивости, достаточной для малой вероятности ошибки. Помехоустойчивость при воздействии шумов обеспечивают когерентным либо некогерентным приемом сигналов, их видами. Виды сигналов различают по их цифровой модуляции. Нами рассматриваются фазоманипулированные сигналы ФМн, частотно-манипулированные ЧМн, амплитудно-манипулированные АМн и сигналы с квадратурно-амплитудной модуляцией КАМ.

Важным являются методы оценки защищенности дискретных систем сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума.

Основная часть

При выявлении технических каналов утечки цифровой системы передачи информации необходимо рассматривать систему, включающую основное (стационарное) оборудование, оконечные устройства, среду распространения, распределительные и коммутационные устройства, системы электропитания, системы заземления.

Схема цифровой системы передачи информации с возможными ее каналами утечки информации представлена на рисунке 1.

На рисунке 1 представлены возможные каналы утечки информации, организуемые полями рассеивания цифрового сигнала: КУ1 – на выходе АЦП, КУ2 – при передаче цифрового сигнала, представленного последовательностью импульсов, по среде распространения, КУ3 – в ЦАП при формировании из цифровой последовательности исходного аналогового сигнала.

В зависимости от природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные и электрические каналы утечки информации [1].

Токи и напряжения информационных электрических

цепей являются источниками магнитных и электрических полей, ослаблены, как правило, неоднородной средой распространения (в том числе, неоднородными экранами). Магнитные и электрические поля наводят токи (напряжения) на неинформационные электрические цепи. Наведенные токи и напряжения распространяются

в неинформационных электрических цепях и создают вторичные магнитные и электрические поля, которые могут распространяться на значительные расстояния.

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений системы передачи информации – электромагнитные излучения элементов системы передачи информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в электрических и магнитных цепях системы, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания:

- излучений элементов системы передачи информации;
- излучений на частотах работы высокочастотных генераторов;
- излучений на частотах самовозбуждения усилителей низкой частоты.

Для цифровых систем передачи информации характерно наличие побочных электромагнитных излучений элементов системы передачи информации. При аналогово-цифровом преобразовании сигнала, несущего информационную составляющую, его передаче через среду распространения и обратном цифро-аналоговом преобразовании, данный электрический сигнал, при прохождении через элементы системы передачи информации возбуждает электрические и магнитные поля в окружающем пространстве. Эти поля модулированы по закону изменения информационного сигнала. Перехват таких полей может быть осуществлен даже на значительном расстоянии.

Критерием оценки цифровых систем передачи информации может служить помехоустойчивость.

Помехоустойчивость зависит от расстояния между сигналами $d(S_i, S_j)$, образующих систему [2]. Под оптимальной системой следует понимать систему сигналов, обеспечивающую максимальную помехоустойчивость при заданных априорных условиях передачи информации.

$$d(S_i, S_j) = \left\{ \int_0^{T_c} [S_i(t) - S_j(t)]^2 dt \right\}^{1/2}, \quad (1)$$

где T_c – длительность сигнала.

Помехоустойчивость системы сигналов увеличивается при увеличении расстояния d .

Для достижения большего расстояния коэффициент взаимной корреляции должен быть минимальным:

$$d(S_i, S_j) = [2E(1 - R_{ij})]^{1/2}, \quad (2)$$

где $R_{ij} = \frac{1}{E} \int_0^T S_i(t) S_j(t) dt$ – коэффициент взаимной корреляции между сигналами $S_i(t)$ и $S_j(t)$, принимающие значения в пределах от -1 до +1, E – одинаковые энергии сигналов.

Для оптимальной системы сигналов $R = -1/M - 1$ [3]. Это достигается равенством всех коэффициентов корреляции, т.е. $R_{ij} = R$ для всех i и j .

Для детального анализа сигналов необходимо учесть, что отношение сигнал/шум в канале утечки информации гораздо меньше единицы, а их наводки являются несимметричными.

На рисунке 2 представлена зависимость вероятности ошибки P от отношения мощности сигнала к мощности шума h для когерентного (1) приема двоичных ФМн сигналов, некогерентного (3) и когерентного (2) приема двоичных ЧМн сигналов [4].

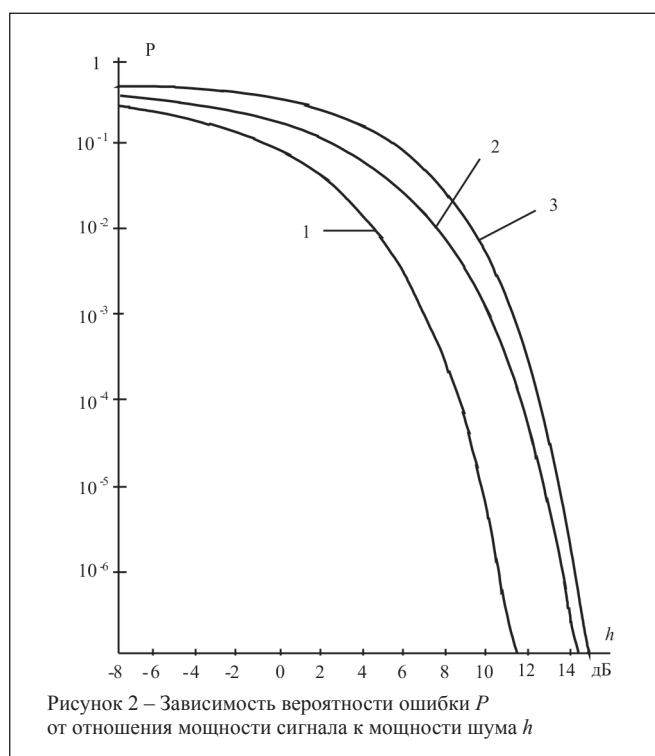
Из рисунка следует, что при малом значении отношения сигнал/шум разброс вероятности ошибок весьма незначителен.

Зависимость вероятности двоичного ФМ-сигнала от отношения энергии сигнала E_s к спектральной плотности мощности помехи N_0 для когерентного приема [3]

$$P_e = 1 - F \left[\sqrt{\frac{2E_s}{N_0}} \right]. \quad (3)$$

Зависимость вероятности ортогональных ЧМн сигналов на промежутке времени $[0, T]$ для когерентного приема при условии равенства энергии сигналов [3]

$$P_e = 1 - F \left[\sqrt{\frac{E_s}{N_0}} \right]. \quad (4)$$



Различия между системами передачи информации определяются объемом алфавита источника n и сигнала m .

В зависимости от m системы передачи информации разделяют на двоичные $m = 2$ и m -ичные $m > 2$.

Сравнение двоичных и m -арных систем связи производят с учетом приемника информации [1]. Двоичные системы связи без декодирования и многократные системы связи с двоичным декодированием эквивалентны, так как в обоих случаях на входе получателя информация представлена в виде двоичных символов. В данном случае при сравнении таких систем связи сравнивают вероятности ошибки, приходящиеся на один двоичный символ.

Рассмотрим случай определения вероятности ошибки m -арных ортогональных сигналов. При когерентном детектировании вероятности ошибки m -арных ортогональных сигналов вычисляется по формуле [5]

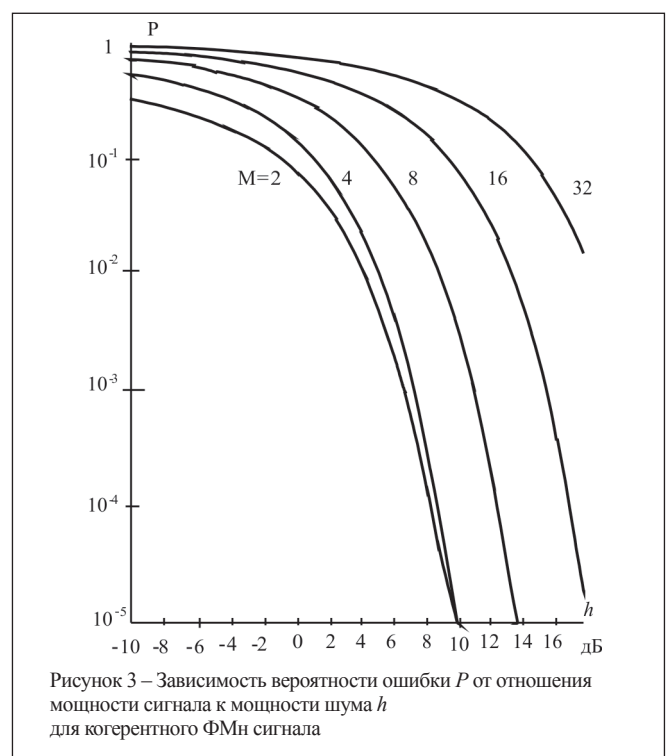
$$P_{ошM} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \left[1 - \left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^y e^{-x^2/2} dx \right)^{M-1} \right] \exp \left[-\frac{1}{2} \left(y - \sqrt{\frac{2E_s}{N_0}} \right)^2 \right] dy \quad (5)$$

Если символьная средняя вероятность ошибки E_b , то для перевода в битовую $E_s = kE_b$, где k – коэффициент, выражаемый из формулы

$$P_b = \frac{2^{k-1}}{2^k - 1} P_M \approx \frac{P_M}{2}, k \gg 1 \quad (6)$$

Формирование ортогональных ЧМн и противоположных ФМн сигналов основано на определенных закономерностях.

Для ЧМн сигналов условие ортогональности соблюдается при равенстве нулю взаимной энергии двух гармонических колебаний $S_k(t)$ и $S_m(t)$ в промежутке времени $[0, T]$ [3]



$$E(S_k, S_m) = \int_0^T A_k A_m \cos(w_k t + \varphi_k) \cos(w_m t + \varphi_m) dt = 0. \quad (7)$$

Двоичные системы передают одну двоичную единицу (или один бит) информации. Алфавит, содержащий M символов, передает $\log_2 M$ двоичной единицы информации на каждый символ. M -ичные сигналы формируют посредством многопозиционной манипуляции несущего колебания по амплитуде, частоте и фазе. Используя $M=2^k$, где k – количество двоичных единиц в символе. Применение сигналов с многопозиционной АМн возможно в каналах с низким уровнем аддитивного шума.

На рисунке 3 [4] показана зависимость вероятности ошибочного приема символа от нормированного отношения сигнал/шум, определяемого как отношение сигнал/шум, приходящее на двоичную единицу информации [4]

$$h_2 = \frac{h_k}{k} = h_m \log_2 M. \quad (8)$$

Из рисунка 3 следует, что при малом отношении сигнал/шум $h_2(\text{дБ}) < 0$ для $M=2$ вероятность ошибочного приема символа меньше, чем для $M > 2$. В этой связи сигнал с двухпозиционной ФМн имеет предпочтение перед сигналами с $M > 2$, так как не обнаружив сигнал двоичной ФМн сигнала в шумах при отношении сигнал/шум < 0 (дБ), можно гарантировать защищенность сигналов многопозиционного сигнала.

При некогерентном приеме начальная фаза неизвестна и является случайной величиной [2]. Наибольшая помехоустойчивость соответствует при передаче двоичной информации ортогональными сигналами. Вероятность ошибки при некогерентном приеме двух ортогональных сигналов выражается [2, 6]:

$$P_{\text{ош}} = 0,5 \exp(-0,5 h_2^2), \quad (9)$$

Помехоустойчивость когерентного и некогерентного приема двух ортогональных сигналов отличается незначительно.

Из ряда работ следует, что наилучшей помехоустойчивостью обладает двоичная система сигналов с фазовой манипуляцией ФМн при когерентном приеме, отношение сигнал/шум которой [6]

$$h = \sqrt{2E_s / N_0}, \quad (10)$$

где N_0 – спектральная плотность мощности шума, E_s – энергия сигнала.

При $M > 2$ ФМн снижается помехоустойчивость из-за взаимного влияния между сигналами, обусловленного взаимной корреляцией.

В многопозиционной системе ЧМн символы передаются с различными значениями частоты. Некогерентный прием ортогональных сигналов ЧМн (рисунок 4) в области нормированного отношения сигнал/шум на двоичную единицу h_2 (дБ) меньше 0 дБ имеют ту же зависимость от вероятности ошибочного приема P , т.е. двоичная система ($m=2$) имеет преимущество по сравнению с системами $m > 2$.

Отношение сигнал/шум для m -го символа связана с отношением сигнал/шум на двоичную единицу [4]

$$h_2 = \frac{h}{k}. \quad (11)$$

Вероятность ошибки [4]

$$P_l \langle Me^{-k \frac{h_2}{2}} = \exp \left[-k \left(\frac{h_2}{2} - \ln 2 \right) \right]$$

Вероятность ошибочного приема экспоненциально стремится к нулю при условии, что отношение сигнал/шум на двоичную единицу удовлетворяет неравенству [4]

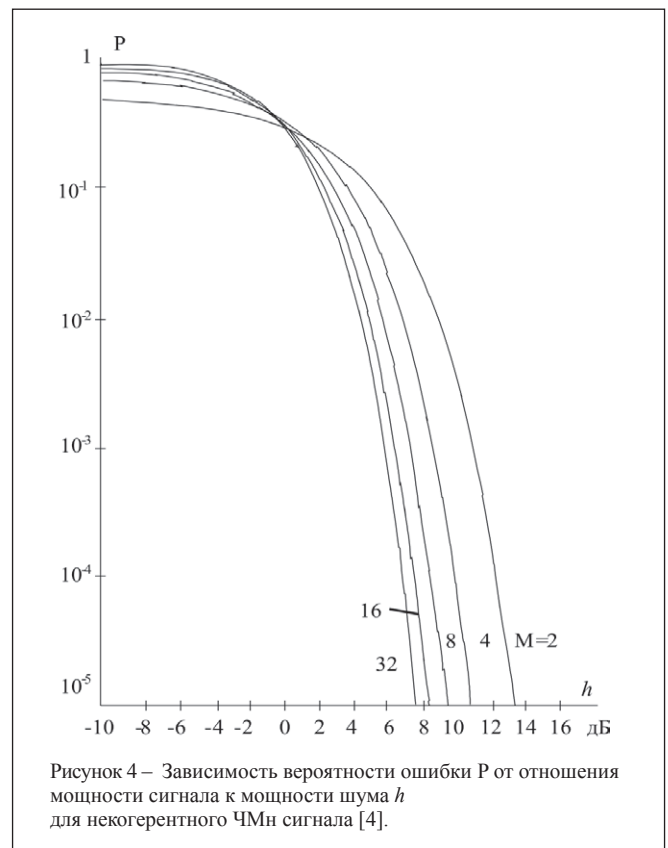
$$h_2 > \ln 2.$$

При пороговых значениях, если энергия сигнала на двоичный символ превышает спектральную плотность мощности шума в 1,39 раза, можно говорить об использовании двоичного ортогонального сигнала в качестве измерительного в канале утечки информации, учитывая его преимущества в большей чувствительности и несинхронности системы.

Сигналы КАМ обладают большими значениями минимального межточечного расстояния d , чем АМ и ФМ, а следовательно и большим значением помехоустойчивости [7].

Средняя вероятность ошибки для КАМ-М, $M=2^k$, k – четно, на m -арный символ равна [7]

$$P_{\text{ош}} = 4 \left(1 - \frac{1}{\sqrt{M}} \right) Q \left(\frac{d}{\sqrt{2N_0}} \right) \left[1 - \left(1 - \frac{1}{\sqrt{M}} \right) Q \left(\frac{d}{\sqrt{2N_0}} \right) \right], \quad (12)$$



где
$$\frac{d}{\sqrt{2N_0}} = \sqrt{\frac{h_m^2}{(\sqrt{M}-1)^2}} = \sqrt{\frac{3h_c^2}{M-1}}, h_m^2 = \frac{E_m}{N_0}, h_c^2 = \frac{E_c}{N_0}$$

Сравним характеристики качества КАМ и ФМ для заданного объема сигналов M . Оба типа сигналов являются двумерными.

Аппроксимация вероятности ошибки на символ M -позиционной ФМ выглядит следующим образом [7]

$$P_{\sqrt{m}\text{ФМн}} \approx 2Q\left(\sqrt{2\gamma_s} \sin \frac{\pi}{m}\right).$$

Аппроксимация вероятности ошибки на символ M -позиционной КАМ представлена в виде [7]

$$P_{m\text{КАМ}} = 2\left(1 - \frac{1}{\sqrt{m}}\right) Q\left(\sqrt{\frac{3}{m-1} \frac{E_{cp}}{N_0}}\right).$$

Отношение двух аргументов Q -функции [7]

$$K_m = P_{m\text{КАМ}} / P_{\sqrt{m}\text{ФМн}} = \frac{3/(M-1)}{2\sin^2(\pi/M)}$$

Заключение

В ходе работы предложено для оценки защищенности цифровых каналов утечки информации использовать в качестве измерительных двоичные ортогональные когерентные и некогерентные сигналы, зависимости вероятности ошибки от отношения мощности сигнала к мощности шума которых находятся вблизи границы Шеннона. Установлены зависимости для сигналов сложной формы КАМ, АФМ, а также зависимости для двоичных и многопозиционных сигналов. Это позволяет оценивать защищенность систем передачи информации по единому нормированному показателю – вероятности ошибки на бит информации.

Литература:

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие / В.К. Железняк; ГУАП. – СПб., 2006. – 188 с.

2. Зюко, А.Г. Помехоустойчивость и эффективность систем связи / А.Г. Зюко. – М.: Связьиздат, 1963. – 320 с.

3. Ключев, Н.И. Информационные основы передачи сообщений / Н.И. Ключев. – М.: Московская типография № 10 Главполиграфпрома, 1966. – 360 с.

4. Стейн, С. Принципы современной теории связи и их применение к передаче дискретных сообщений / С. Стейн, Дж. Джонс, отв. редактор Л.М. Финк. – М.: «Связь», 1971. – 376 с.

5. Дядюнов, А.Н. Адаптивные системы сбора и передачи аналоговой информации. Основа теории / А.Н. Дядюнов, Ю.А. Онищенко, А.И. Сенин – М.: Машиностроение, 1988. – 288 с.

6. Варакин, Л.Е. Теория систем сигналов / Л.Е. Варакин. – М.: «Сов.радио», 1978. – 304 с.

7. Савищенко, Н.В. Многомерные сигнальные конструкции: их частотная эффективность и потенциальная помехоустойчивость приема / Н.В. Савищенко, под ред. Д.Л. Бураченко. – СПб.: Изд-во Политехн. ун-та, 2005. – 420 с.

Abstract

The optimum signal for an estimation of security of digital channels of information leakage is investigated. The technology of technical protection of the information forms the generalized requirements to the theory and techniques of transfer of systems of signals. The system of signals used for an information transfer as set of signals, united by a uniform rule of construction is considered. It is known, that a noise stability – one of the basic requirements to transfer system. The optimum system of signals providing the maximum noise stability at the minimum relations of energy of bit to spectral density of capacity of noise in channels of information leakage, methods of an estimation of security of discrete systems of signals in information leakage channels are offered at influence of noise of high level of type white Gaussian noise, and also a choice and a substantiation of an optimum signal which will allow to estimate security of digital channels of information leakage.

Поступила в редакцию 18.05.2013 г.

СПОСОБ ПОДАВЛЕНИЯ ЗАШУМЛЕННЫХ ИМПУЛЬСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПУТЕМ КОМПЕНСАЦИИ

УДК 621.397.7:004.056.57

В.К. Железняк, А.В. Барков,
ПГУ, г. Полоцк

Аннотация

Рассматривается обнаружение периодических импульсных последовательностей и их подавление путем компенсации в канале утечки информации. Задачей является обнаружение периодической импульсной последовательности из аддитивных шумов высокого уровня с целью последующего её подавления. Обнаружение основано на быстром преобразовании Фурье и накоплении сигнала в частотной области. Сравнение и оценку обнаружения производят при помощи оптимального приема и порогового детектирования. Выбор

порога осуществляют по известным критериям оптимальности в задачах обнаружения сигналов. Подавление импульсных последовательностей в канале утечки информации решается их компенсацией воспроизведением противофазного обнаруженного сигнала. Эксперименты проведены моделированием периодической импульсной последовательности с добавлением аддитивных шумов, таких как белый шум, хаотическая импульсная последовательность, телеграфный сигнал. Предложен способ обнаружения и компенсация зашумленных импульсных последовательностей. Проанализированы известные

способы, что позволило выявить ряд преимуществ предложенного способа.

Введение

Основные информационные процессы – передача, прием, распространение, преобразование, запоминание – были интересны всегда, на современном этапе развития техники и информационных технологий возросла видимая (открытая) часть интересов к вопросам добычи, утечки, сохранности и защиты информации. На расстояние информация передается в подавляющем преимуществе по каналам электро- и радиосистем в виде сообщений в аналоговой или цифровой форме. Многообразие существующих способов обеспечения информационной безопасности показывает возможность различных подходов к вопросу обеспечения защиты информации и необходимость разработки более совершенных способов защиты информации от утечки. [1]. Синхронизация используется при передаче цифровых сообщений, которые имеют логическую форму двоичных единиц и нулей [2, с. 84].

Проанализированы известные решения [3, 4], данные способы не рассматривают возможность обнаружения сигнала в шумах высокого уровня, в маскирующих помехах в виде белого шума, учитывают только влияния мешающих импульсных последовательностей.

В работе [5] предложен способ измерения и подавления физических полей самонастраивающимся опорным полем. Недостатками способа является невозможность обнаружения сигнала в шумах высокого уровня.

Задачей предлагаемого способа является обеспечение обнаружения и компенсации зашумленных импульсных последовательностей в канале утечки информации (КУИ) в шумах высокого уровня.

Обнаружения периодической импульсной последовательности

Обнаружение сигналов в шумах может быть основано на накоплении сигнала с целью выделения его из шума. В работе [3] представлен принцип выделения сигналов, основанный на совпадении сигналов, и реализуется с применением накопителей на линиях задержки с положительной обратной связью. В [3] показано накопление сигнала во временной форме. Сигнал по линии обратной связи поступает на вход приемного устройства с квазипериодом T . Таким образом, для накопления сигнала и улучшения отношения сигнал-шум в [3] требуются априорные данные о сигнале – период повторения сигнала.

Предложен способ обнаружения периодических импульсных последовательностей и оценки их периода, который измеряет и оценивает параметры зашумленного сигнала, выделяет сигнал из шума без априорных данных о сигнале.

Периодическая импульсная последовательность $x(t)$, смешанная с аддитивным шумом $n(t)$ в КУИ, моделирует сигнал в КУИ $s(t)$:

$$s(t) = x(t) + n(t), \quad (1)$$

Произведем разделение сигнала на отрезки равной длительности и преобразование Фурье каждого отрезка, суммируем результаты преобразования по формуле:

$$S = \sum_0^{N-1} FFT(S_n), \quad (2)$$

где N – количество отрезков сигнала равной длины, S_n – сигнал указанной длины, FFT – быстрое Фурье-преобразование сигнала, S – накопленное Фурье преобразование отрезков сигнала.

По данным преобразования Фурье, которое получили в результате накопления, формируют спектр амплитуд зашумленного сигнала, по которому определяют гармонику с наибольшей амплитудой A_{max} , не учитывая значения нулевой гармоники. Частоту гармоники с наибольшей амплитудой f_{max} принимаем за период следования импульсов. Обнуляем в спектре амплитуд составляющие, не кратные частоте следования импульсов f_{max} и нулевую гармонику, получаем:

$$A_k = \begin{cases} 0, & \text{для } k \neq M \cdot m, m = (1..K-1); \\ A_k, & \text{для } k = M \cdot m, m = (1..K-1) \end{cases} \quad (3)$$

где A_k – k -ая гармоника Фурье-преобразования, K – количество гармоник Фурье-преобразования, M – номер гармоники с частотой f_{Amax} .

Получаем спектр сигнала S' , состоящий из отфильтрованных по формуле (4) гармоник A_k без шума, т.е. остались только гармоники периодической импульсной последовательности.

Производим обратное дискретное преобразование Фурье IFFT обработанного (после обнуления) сигнала, получаем восстановленный сигнал $x'(t)$:

$$x'(t) = IFFT(S'), \quad (4)$$

Сравниваем полученный сигнал с исходным, из которого удалена его постоянная составляющая. Сравнение и оценку обнаружения производят при помощи оптимального приема и порогового устройства, выбор порога осуществляем по известным критериям оптимальности решений в задачах обнаружения сигналов, а за оценку периодов обнаруженных импульсных последовательностей принимают частоту f_{Amax} гармоники спектра амплитуд с наибольшей амплитудой A_{max} , частота которой соответствует частоте следования импульсов.

Компенсация периодических импульсных последовательностей в канале утечки информации

Ряд сигналов (например, видео, цифровой) являются синхронными. При наличии информации о периоде сигнала есть возможность его синхронного накопления и улучшения отношения сигнал-шум. Для невозможности синхронного накопления требуется решить задачу по разрушению сигналов синхронизации.

Компенсация периодических импульсных последовательностей происходит после их обнаружения в шумах представленным выше способом.

Если определили наличие сигнала в шумах, то необходимо его разрушить.

Сигнал восстанавливается способом представленным ранее. Компенсацию осуществляем поворот восстановленного сигнала в противофазе, который при сложении с зашумленным сигналом разрушит посредством компенсации периодическую импульсную последовательность, которая была в зашумленном сигнале.

Покажем результаты моделирования обнаружения и компенсации.

Входным параметром является зашумленный сигнал, который может содержать периодическую импульсную

последовательность $x(t)$ с неизвестными параметрами (рисунок 1).

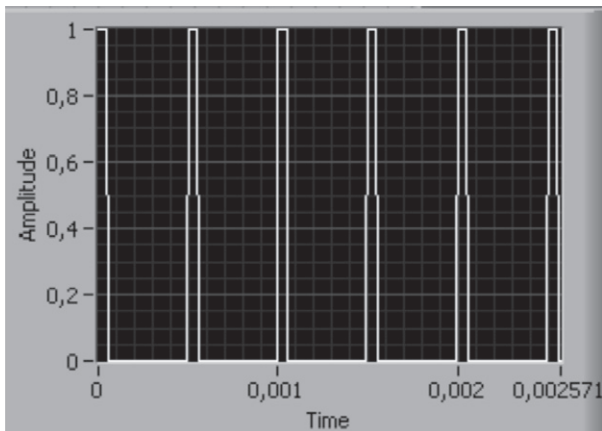


Рисунок 1 – Последовательность прямоугольных импульсов

Формируем аддитивную смесь сигнала с белым гауссовым шумом. Задача заключается в том, чтобы принять решение о наличии или отсутствии периодической импульсной последовательности с неизвестными параметрами в шумах (рисунок 2).

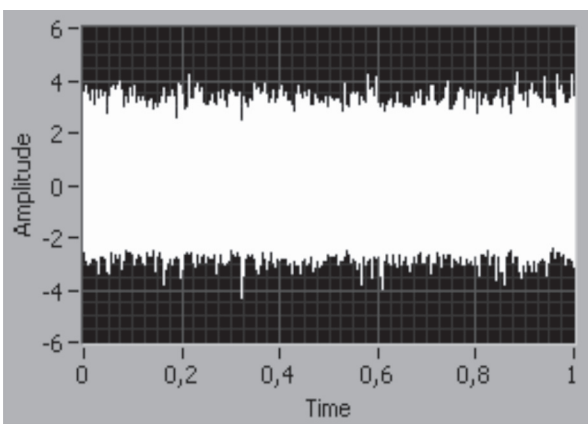


Рисунок 2 – Зашумленная периодическая импульсная последовательность

Последовательность (пачка) прямоугольных импульсов характеризуется длительностью импульса, периодом следования импульсов и общим числом импульсов в пачке. [6, с. 316]

Обнаружение периодической импульсной последовательности производим способом, описанным ранее.

При моделировании периодической импульсной последовательности исходные параметры эксперимента: частота следования импульсов 2000 Гц, амплитуда импульсов 1В, скважность 10.

Представим зашумленную импульсную последовательность в частотной области $F\{x\}$. Спектр амплитуд зашумленного сигнала представлен на рисунке 3.

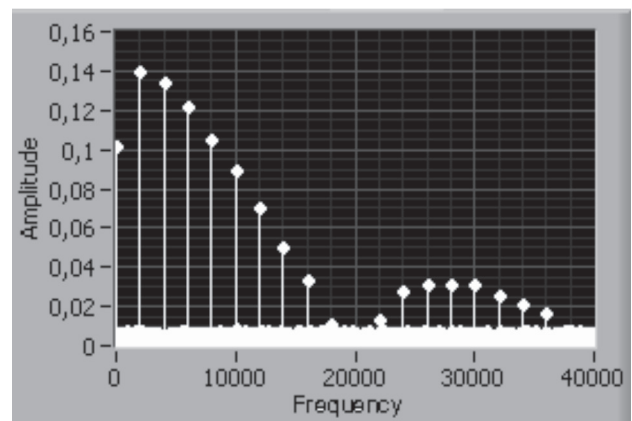


Рисунок 3 – Спектр зашумленного сигнала

По спектру амплитуд определяют гармонику с наибольшей амплитудой. Рисунок 4 показывает, что будет выделена гармоника с амплитудой 0,14 и частотой 2000 Гц. За частоты следования импульсов f обнаруженной периодической импульсной последовательности принимают частоту гармоники спектра амплитуд с наибольшей амплитудой, производим выделение этой гармоники в данном случае это гармоника на частоте 2000 Гц. Этот параметр носит информативный характер, при правильном обнаружении данная частота соответствует частоте следования импульсов f .

Производим фильтрацию спектра, обнуляя составляющие, не кратные основной частоте следования импульсов f (значение этой частоты определили по спектру амплитуд ранее). Кратность частот определяем по формуле:

$$fk = f * k, \quad (5)$$

где $k = 0, 1, 2 \dots N$ – номер гармоники, f – частота следования импульсов.

Спектр амплитуд после фильтрации представлен на рисунке 4.

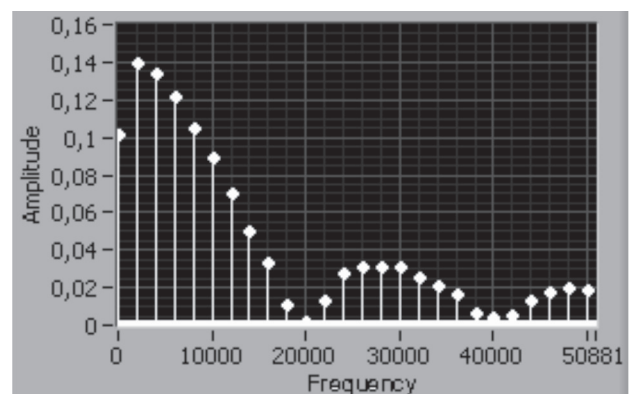


Рисунок 4 – Спектр зашумленного сигнала после фильтрации

Спектр амплитуд периодической импульсной последовательности исходного сигнала $x(t)$ и восстановленного сигнала после фильтрации незначительно отличаются амплитудами.

Выполняем ОДПФ (обратное дискретное преобразование Фурье) и производят нормирование амплитуд восстановленной импульсной последовательности по формуле

$$Sig = InvFFT\{S\} / N, \quad (6)$$

где $InvFFT\{S\}$ – обратное дискретное преобразование Фурье; N – количество отрезков сигнала равной длины, получаем восстановленный сигнал $x1(t)$.

Получаем восстановленную импульсную последовательность. Если сравнить импульсную последовательность из исходного сигнала (рисунок 1) и восстановленную импульсную последовательность после обратного дискретного преобразования Фурье (рисунок 5), видно, что импульсная последовательность восстановлена с некоторыми искажениями по форме, однако значительно отличается от зашумленного сигнала (рисунок 2).

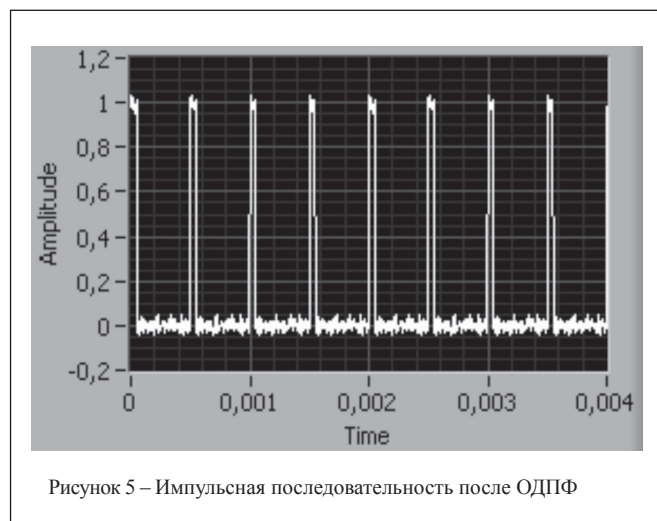


Рисунок 5 – Импульсная последовательность после ОДПФ

Сравниваем импульсные последовательности рисунок 1, принимаем решение о соответствии восстановленной импульсной последовательности и исходной. Соответствие сигнала исходному определяем с помощью оптимального приема и порогового устройства. Выбор порога осуществляется по известным критериям оптимальности решений в задачах обнаружения сигналов [7, с. 33]. За оценку частоты следования периодической импульсной последовательности принимаем значение равное 2000 Гц, что соответствует значению частоты следования импульсов в исходном сигнале.

Осуществляем поворот восстановленного сигнала $x1(t)$ (рисунок 5) в противофазе, получаем сигнал $x1r(t)$, таким образом, при сложении с зашумленным сигналом $x(t)$ этот сигнал разрушит посредством компенсации периодическую импульсную последовательность, которая была в зашумленном сигнале.

Если определили наличие сигнала в шумах, то необходимо его разрушить. Производим сложение сигналов $x(t)$ и $x1r(t)$, на выходе получаем разрушенный сигнал $x2(t)$, в котором скомпенсирована периодическая импульсная последовательность. Рисунок 6 представляет спектр разрушенного сигнала, который значительно отличается от спектра зашумленного сигнала (рисунок 3) и в нем отсутствуют признаки наличия сигнала в шумах, что говорит об успешном разрушении сигнала.

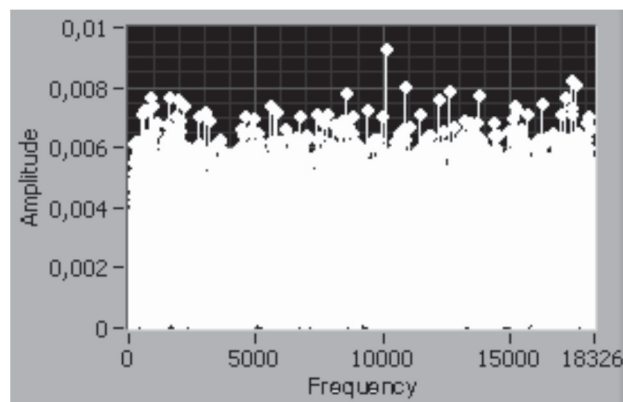


Рисунок 6 – Спектр разрушенного сигнала в канале утечки информации

Моделирование отсутствия периодической импульсной последовательности с неизвестными параметрами в шумах производится после ее разрушения.

Обнаружение синхросигналов в шумах при оценке защищенности информации представляет признак, по которому принимают решение о наличии канала утечки. Считается, что цифровое сообщение имеет логическую форму двоичных единиц и нулей и с целью передачи проходят этап импульсной модуляции, в результате чего преобразуются в низкочастотные (импульсные) сигналы, или видеоимпульсы. Видеоинформацию накапливают, используя полученные данные о параметрах синхронизации, так же накопление информации позволяет улучшить отношение сигнал/шум. Выделение синхронизирующих импульсов позволяет проводить синхронное накопление информации, например в виде видеокадров.

Предложенный способ является универсальным, так как при различных структурах маскирующих сигналов результаты обработки аналогичны.

Заключение

Исследовано обнаружение и компенсация периодических импульсных последовательностей и импульсов синхронизации в шумах высокого уровня при воздействии различных помех и выделение их из аддитивной смеси с шумом.

Показана возможность обнаружения периодических импульсных последовательностей из шумов, принимать решение о соответствии восстановленного сигнала исходному сигналу, разрушение сигнала в канале утечки информации путем компенсации исходного сигнала восстановленной импульсной последовательностью.

Предложенный способ обладает следующими преимуществами: обнаружение и компенсация периодических импульсных последовательностей в шумах высокого уровня без априорных данных о сигнале при воздействии факторов помех, таких как белый шум, хаотическая импульсная последовательность, телеграфный сигнал, возможность накопления сигнала с неизвестными параметрами в частотной области, обнаружение импульсных последовательностей в аддитивной смеси с шумом, в которой может меняться амплитуда сигнала за счет наложения шума.

Литература:

1. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД Диа Софт, 2002. – 688 с.
2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.
3. Лезин, Ю.С. Оптимальные фильтры и накопители импульсных сигналов. – М.: «Сов.радио», 1969. – 320 с.
4. Патент Российской Федерации 2251704, МПК G01R23/02, опубл. 10.05.2005
5. Патент Российской Федерации 2391678, МПК G01R29/08, опубл. 27.01.2010
6. Ван Трис Г. Теория обнаружения, оценок и модуляции. Том III. Обработка сигналов в радио- и гидролокации и прием случайных гуссовых сигналов на фоне помех. Нью-Йорк, 1971. Пер. с англ. Проф. В.Т. Горяинова. М.: «Сов.радио», 1977. – 664 с.
7. Помехоустойчивость информационных радиосистем управления: Учеб. пособие / А.Г. Охонский, А.А. Елисеев, Н.В. Каплунова, А.Н. Кулин, Э.В. Минько. – М.: МГАП «Мир книги», 1993. – 216 с.

Abstract

We consider the detection of periodic pulse sequences and their suppression by compensation in the channel information leakage. The task is to detect the periodic pulse sequence of high level of additive noise to its subsequent suppression. The detection is based on a fast Fourier transform and the accumulation of a signal in the frequency domain. Comparison and evaluation of the detection is carried out with the best reception and the threshold of detection. Thresholding performed by well-known criteria of optimality in problems of signal detection. Suppression pulse sequences in the channel leak solved their compensation playback antiphase signal detection. Experiments were carried out simulations of the periodic pulse sequence with the addition of additive noise such as white noise, chaotic pulse sequence, telegraph signal. We propose a method of detecting and compensating for noisy pulse sequences. The known methods, which revealed a number of advantages of the proposed method.

Поступила в редакцию 18.05.2013 г.

40-ЛЕТНИЙ ЮБИЛЕЙ ПД ИТР

УДК 519.6

В.К. Железняк,
ПГУ, г. Полоцк

В статье рассматриваются этапы развития и пути совершенствования государственной системы защиты информации противодействия иностранным техническим разведкам (ПД ИТР). Уровень развития этого направления по праву позволяет отнести его к научному направлению информатики. Эффективность применения разработанных в предвоенный период отечественных радиолокационных станций позволило во время Великой Отечественной войны принять Постановление о развитии радиолокации, в послевоенный (1952) – о создании НИИ Автоматики для развития науки и техники, криптографических методов безопасности, включающих наряду с военной, научной, экономической, политической и другие виды информации. И наконец, в 1973 году принято важнейшее постановление о развитии ПД ИТР.

Научное направление деятельности формировалось в ЦНИРТИ, созданном Постановлением ГКО 4 июля 1943 г. №ГОКО-368сс «О радиолокации», подписанным И.В. Сталиным. Главный инициатор подготовки и принятия постановления ГКО выдающийся ученый Герой Социалистического Труда инженер-адмирал академик Аксель Иванович Берг – первый директор ордена Ленина ЦНИИ 108 МО [1]. В лаборатории радиоприемных устройств разрабатывал УПЧ и УНЧ для самолетной ОКР «Ласточка» (главный конструктор Ю.Н. Мажоров в дальнейшем зам. директора по науке и директор ЦНИРТИ) ОПЧ и УНЧ для космической ОКР К8 (главный конструктор Плешаков П.С. директор ЦНИРТИ и в дальнейшем Министр радиопромышленности СССР).

Опыт разработки самолетной, космической аппаратуры радиотехнической разведки повысил научный потенциал. Опыт по созданию РЭА пригодился в дальнейшем, работая по переводу в НИИ 110 г. Киев. Проработав в филиале

ЦНИИ 108 (ВЧ 25757) 4 года инженером, старшим инженером, начал работать по космической тематике, через короткое время назначен ведущим инженером и заместителем главного конструктора двух ОКР «Пион 2» и «Пион 4» по морской тематике. Пригодился опыт предыдущей работы по летным экспериментальным работам в интересах космической тематики (ОКР «Кортик» гл. конструктор В.Л. Гречка Лауреат Ленинской премии за эту разработку).

Далее работал начальником НИЛ и начальником НИО, разрабатывая специальную измерительную аппаратуру.

После выхода Постановления ЦК КПСС и Совмина СССР от февраля 1973 г. № 903-903 и приказа МПСС СССР назначен в марте 1973 г. начальником головной НИЛ специальных исследований. Это определило второй и последний этап деятельности по ПД ИТР.

Новая эра началась выступлением в Москве Председателя Гостехкомиссии СССР Маршала Огаркова Н.В., который обосновал важность Постановления, исходя из возможностей и намерений предполагаемых противников. Стройное построение единой общегосударственной системы ПД ИТР дало положительные результаты в разработке В и ВТ. Эти работы базировались на научной основе, оснащении разработчиков самой современной аппаратурой контроля. Ежеквартальные семинары по научным вопросам в НИИ Автоматики г. Москва давали возможность внедрять в разработки самые современные научные достижения. В период работы по этой тематике в НИИ 110 выполнено более 20 фундаментальных НИОКР, что позволяло прогнозировать наши возможности и предполагаемых противников. Выполнен ряд работ по формированию маскирующих сигналов, слабым магнитным полям, разработаны ОКР «Гранит XVI», а «Гранит IV» с Вильнюсским КБ магнитной записи, ряд работ непосредственно для эксплуатации



Рисунок 1 – 30-летний юбилей ПД ИТР

в Кремле и других Ведомствах. По аналогичной тематике работал в ВНИИ РПА им. А.С. Попова.

Федеральное государственное унитарное предприятие «Государственное научно-производственное предприятие «Информационная» создано решением концерна «ТЕЛЕКОМ» и Всесоюзного научно-исследовательского института радиовещательного приема и акустики (ВНИИРПА) им. А.С. Попова 26 декабря 1991 г. для выполнения всех обязанностей, закрепленных за ВНИИРПА им. А.С. Попова в головной роли по направлению техники, определенной приказом Министра промышленности средств связи СССР № 67 от 25.04.90 г. и в головной роли по противодействию акустической речевой разведке (АРР), закрепленной решением Государственной технической комиссии СССР № 85-3 от 20.03.90 г., а также для выполнения всех работ по этим основным направлениям, закрепленных за концерном «ТЕЛЕКОМ». Директором назначен В.К. Железняк.

Согласно приказу №26 от 12.02.1999 г. Председателя Гостехкомиссии России объявлена благодарность директору ФГУП ГНПП «Информационная» «за большой личный вклад в решении научных проблем защиты информации от иностранных технических разведок и ее утечки по техническим каналам» и в связи с этим он приглашен на юбилейную встречу 30 летнего юбилея ПД ИТР в г. Москве (рисунок 1).

Ведомственная принадлежность ФГУП «ПРОПП «Информационная» - Российское агентство по системам управления. Указом президента РФ ФГУП «ПРОПП «Информационная» входила в перечень стратегических предприятий.

Министерством промышленности, науки и технологий РФ выдано «Свидетельство о государственной аккредитации

научной организации» № 5523 от 1 марта 2004г. о соответствии с Федеральным законом «О науке и государственной научно-технической политике».

Научная деятельность ФГУП «ГНПП «Информационная» осуществляется по следующим направлениям:

78.25 Вооружение и военная техника.

Работы, выполняемые в рамках исполнения 707 раздела. Программы вооружения и 10 раздела Программы развития базовых военных технологий.

47.05 Теоретическая радиотехника.

90.27 Измерение акустических величин.

47.14 Проектирование и конструирование электронных приборов и радиоэлектронной аппаратуры.

Разработка новых технологий обеспечения информационной безопасности.

Разработка специальных систем защиты информационных объектов.

Аттестация объектов информатизации.

Сертификационные испытания средств защиты информации.

По результатам исследований с 2001 по 2007 г.г. выполнено 21 НИОКР, опубликовано более 50 работ.

Основные темы научно-технических и опытноконструкторских работ по профильным направлениям деятельности

Основные научно-технические результаты исследований по наиболее важным направлениям:

78.25 Вооружение и военная техника.

Научно обоснован и разработан пакет нормативно-методических документов, включающий нормы противодействия акустической речевой разведке (АРР), методику

расчета показателя противодействия АРР и методику инструментального контроля выполнения норм противодействия АРР.

47.05 Теоретическая радиотехника.

Развит статистический подход к оценке разборчивости речи. Предложена зависимость слоговой разборчивости от величины среднеквадратического искажения, вычисленной инвариантно от времени задержки и масштабного коэффициента.

Исследованы возможности повышения эффективности методов анализа сигналов за счет использования техники совместного спектрально-временного представления сигналов, шумов, помех и каналов передачи информации.

Разработаны алгоритмы программы многомерного частотно-масштабно-временного анализа сигналов полей рассеивания различной физической природы для автоматизированной системы измерительного контроля каналов утечки информации.

На основе исследований в области теории и синтеза сигналов предложены пути дальнейшей модернизации элементов аппаратно-программного комплекса контроля каналов утечки информации.

90.27 Измерения акустических величин.

Проведены научные исследования по разработке теоретических основ и методов измерений акустических сигналов в условиях сильных помех и шумов.

Разработаны методы и средства измерения акустических величин акустического давления (интенсивности) слабых акустических полей (в шумах высокого уровня акустической речевой информации), высокочувствительных преобразователей акустических сигналов в электрические сигналы, используемых в автоматизированных системах оценки разборчивости речи (в каналах утечки акустической речевой информации), обеспечивающих высокую точность, воспроизводимость и достоверность результатов с учетом влияющих факторов.

47.14 Проектирование и конструирование электронных приборов и радиоэлектронной аппаратуры.

На базе использования цифровых сигнальных процессоров разработаны и внедрены устройства контроля каналов утечки информации в средах с априорно-неизвестными

параметрами (система измерительная автоматизированная К6-6 ТРАП-Н50: Сертификат Госстандарта России №127793 от 13.08.2002 г., Сертификат Гостехкомиссии №717 от 20.01.2003 г.). Разработаны приемники трех-программные (МРАМОР ПТ-101 и МРАМОР ПТ-102) с каналом оповещения, защищенные от утечки информации. Разработано устройство активного вибро- и акустического зашумления, генератор маскирующего шума "Мрамор ГШ-101-2-03" (шифр "Равнина-2К", Сертификат Гостехкомиссии №689 от 5.12.2002 г.) (рис. 2). Комплекс активной защиты «Класс ЗИ» обеспечивает пространственное низкочастотное зашумление НЧ магнитных и электрических информационных полей, защиту цепи питания и цепи заземления.

Разработка новых технологий обеспечения информационной безопасности.

Проведены научные исследования, на базе которых разработаны:

- Высокопроизводительная измерительная система (СИА), позволяющая выявлять и оценивать по критерию «разборчивость речи» акустические, виброакустические, электромагнитные и электрические каналы утечки информации в условиях воздействия шумов высокого уровня.

- эталон магнитного поля (совместно с ВНИИМ) на базе колец Максвелла, обеспечивающий калибровку магнитных измерительных преобразователей в неэкранированных помещениях с высокой точностью;

- эталон электрического поля, обеспечивающий калибровку электрических измерительных преобразователей;

- акустическая измерительная система, обеспечивающая компенсации паразитных низкочастотных магнитных полей.

Разработка специальных систем защиты информационных объектов.

Разработано устройство активного зашумления для акустического и виброакустического каналов, отличительной особенностью которого является контроль качества шума, основанный на учете выбросов случайных процессов при различных уровнях в заданный интервал времени.

Разработан корреляционный метод разборчивости речи (авторы ФГУП «ГНПП «Информационика»: Железняк, Комарович, Колесников).

Исследование разборчивости речи акустического речевого сигнала корреляционным методом направлено на повышение точности разборчивости, при высоком уровне шума и низком уровне сигнала (предельное значение ОСШ = минус 30 дБ). Зависимость коэффициента разборчивости речи от ОСШ аппроксимирована интегральной кривой. Интегральная кривая при ОСШ меньше минус 10 дБ идет практически параллельно оси абсцисс.

График коэффициента разборчивости речи перенесен на вероятностную бумагу и представлен линейной зависимостью. Представление интегральной кривой на вероятностной бумаге в виде прямой линии резко снижает методическую погрешность оценки коэффициента разборчивости речи и соответственно слоговую и словесную разборчивости.

Полученные результаты использованы в автоматизированной интеллектуальной измерительной системе (СИА) разборчивости речи.



Рисунок 2 – Электронные приборы и радиоэлектронная аппаратура, разработанная ФГУП «ГНПП «Информационика»

Исследована аналитическая зависимость дальности приема речевого сигнала от уровня шумов с использованием ненаправленного и направленного звукоприемника, получены численные значения коэффициентов дальности приема и маскирования. Исследована передача речи по УЗК и ИК каналам, предложены методики оценки разборчивости речи и дальности приема по побочному каналу ультразвуковой и инфракрасной аппаратурой.

Проведены исследования и разработана методика получения информационной составляющей ПЭМИН с применением цифрового метода обработки сигнала.

В Республике Беларусь в Полоцком государственном университете создана научно-исследовательская лаборатории технической защиты информации (рис. 2), в которой выполнено совместно с НИИ ТЗИ г. Минск ОКР «ФИЛИН А» (рис. 3) по программе Союзного государства, намечается ряд других работ.



Одной из приоритетных целей НИИ ТЗИ является подготовка научных кадров. В апреле 2013 г. первый из аспирантов Раханов К.Я. успешно защитил кандидатскую диссертацию, которая легла в основу разработанного программно-аппаратного комплекса «ЕРМАК» (рисунок 4).



Полученные научные результаты деятельности регулярно представляются на международных научных конференциях, выставках.



Литература:

1. 60 лет ЦНИРТИ, 1943-2003. Коллектив авторов. Под ред. В.К. Бирюкова д.т.н. Б.Д. Сергиевского, Т.С. Лоскутовой. – М.: ЦНИРТИ, 2003. – 196 с.

Abstract

The article examines the stages of development and how to improve the state of information security systems counteract foreign technical intelligence (PD TDI). The level of development in this direction by the right allows you to take it to the scientific field of computer science. The effectiveness of the developed during the interwar period, domestic radar allowed during the Great Patriotic War, adopted a resolution on the development of radar in the post-war (1952) - the establishment of Institute of Automation for the development of science and technology, the security of cryptographic techniques, which include, along with the military, scientific, economic, political and other kinds of information. Finally, in 1973, made important decisions about the development of PD TDI.

Поступила в редакцию 18.05.2013 г.

СТАНДАРТИЗАЦИЯ АЛГОРИТМОВ РАЗДЕЛЕНИЯ СЕКРЕТА В РЕСПУБЛИКЕ БЕЛАРУСЬ

УДК 004.056.53 (003.26)

Н.Н. Шенец,
НИИ ППМИ БГУ, г. Минск

Аннотация

Рассматриваются алгоритмы разделения секрета. Указываются изменения, внесенные в проект стандарта Республики Беларусь СТБ 34.101.60 «Информационные технологии и безопасность. Алгоритмы разделения секрета».

Введение

Теория разделения секрета зародилась в работах А. Шамира [1] и Г. Блейкли [2] в связи с решением следующей задачи. Пусть имеется некоторая важная информация (секрет) S , доступ к которой нельзя доверить одному лицу, а требуется так распределить ее в виде частичных секретов между пользователями, чтобы лишь заранее определенные подмножества этих пользователей (разрешенные подмножества), объединяя свои частичные секреты, могли восстановить исходный секрет. Остальные подмножества пользователей называются запрещенными и не могут восстановить секрет. Алгоритмы, решающие данную задачу, называются схемами разделения секрета.

В настоящее время данная теория нашла много применений: протоколы электронного голосования, пороговая криптография (пороговые схемы электронной цифровой подписи), помехоустойчивое кодирование, широкополосное шифрование и распределенные секретные вычисления. Были разработаны критерии качества схем разделения секрета [3], наиболее важными из которых являются совершенность и идеальность. Совершенность означает, что запрещенные подмножества пользователей, объединив свои частичные секреты, не получают никакой информации об исходном значении секрета, кроме априорной. Идеальными называются совершенные схемы разделения секрета, в которых размеры частичных секретов совпадают с размером секрета.

В НИИ ППМИ был разработан предварительный стандарт Республики Беларусь СТБ П 34.101.60 2011 «Информационные технологии и безопасность. Алгоритмы разделения секрета» [4], действие которого прекращается летом текущего года. В этой связи в нашей организации ведутся работы по переводу данного предварительного стандарта в стандарт Республики Беларусь. При этом в проект стандарта внесены существенные изменения и дополнения. Данные изменения учитывают то обстоятельство, что некоторые компании уже реализовали алгоритмы из предварительного стандарта и даже провели их экспертизу.

Основная часть

Предварительный стандарт СТБ П 34.101.60 2011 основывается на идеальной модулярной схеме разделения секрета в кольце многочленов от одной переменной над двоичным полем [5–6]. Эта схема разделения секрета состоит из алгоритмов генерации параметров, алгоритма разделения секрета и алгоритма восстановления секрета. Она является пороговой, т.е. среди n пользователей разрешенными подмножествами являются любые подмножества, состоящие из t или более пользователей. Число t называется пороговым числом.

Параметрами схемы разделения секрета являются: общее число пользователей n , пороговое число t , длина секрета l в битах, общий открытый ключ M_0 и открытые ключи пользователей $M_1, \dots, M_n$ длиной l битов каждый. Открытые ключи необходимо генерировать либо задавать из таблиц.

В СТБ П 34.101.60 2011 определено два алгоритма генерации открытых ключей, а также приведены таблицы возможных ключей для $l \in \{128, 192, 256\}$. Оказалось, что предложенные в предварительном стандарте алгоритмы не являются, на сегодняшний день, оптимальными. В проекте стандарта данные алгоритмы заменены новыми, которые имеют лучшую вычислительную скорость. Более того, генерация общего открытого ключа вынесена в отдельный алгоритм, добавлен алгоритм генерации открытого ключа пользователя по идентификатору пользователя, что, несомненно, будет востребовано на практике.

Изменения коснулись также и параметра l . Если в СТБ П 34.101.60 2011 допускалось выбирать произвольное число l , кратное 8, то в проекте стандарта зафиксировано 3 значения $l \in \{128, 192, 256\}$. Это связано, в первую очередь, с тем, что в современной криптографии данные длины наиболее часто используются. Кроме того, скорость алгоритмов разделения и восстановления секрета напрямую зависит от параметра l и с его увеличением заметно возрастает. Фиксация параметра l упрощает программную реализацию алгоритмов стандарта.

Алгоритмы разделения и восстановления секрета остались в неизменном виде, что, безусловно, важно разработчикам, уже реализовавшим данные алгоритмы. Однако в проект стандарта в качестве приложений добавлено два новых режима использования схемы разделения секрета.

Первый из них касается свойства проверяемости секрета после его восстановления. Если частичные секреты некорректны, то восстановленное значение также не будет совпадать с истинным значением секрета. Поэтому с целью обнаружения такого события в проекте стандарта предлагается использовать функцию хэширования. При этом на частичные секреты разделяется пара $(S, h, (S))$, и каждый пользователь i получает пару значений S_i, H_i . После восстановления секрета пользователи проверяют, что вторая половинка восстановленного значения является хэшем от первой. Если это не так, то какие-то частичные секреты пользователей некорректны, а восстановленное значение не является секретом.

Второй режим связан с тем обстоятельством, что в реальных системах может не быть стороны (дилера), которая знает секрет и самостоятельно его разделяет, а затем распределяет частичные секреты. В этой ситуации необходим протокол одновременной выработки секрета пользователями и разделения его на частичные секреты. Такой протокол существует, и он предложен в одном из приложений проекта стандарта.

Заключение

Таким образом, в НИИ ППМИ разработан стандарт по разделению секрета, востребованный в Республике Беларусь. Отметим, что в настоящее время ни в одной стране мира пока не принят аналогичный стандарт. Единственным известным нам аналогом является интернет-драфт [7], который действовал в 2009 году в течение полугода. Он основан на схеме Шамира и в вычислительном аспекте лучше нашего стандарта, однако при этом общее число пользователей в системе не должно быть больше 255, за счет чего и достигается выигрыш в скорости.

Литература:

1. Shamir, A. How to share a secret. – Comm. ACM, 1979. – V. 22. – P. 612–613.
2. Blakley, G. Safeguarding cryptographic keys. – Proc. AFIPS Nat. Comp. Conf., 1979. – V. 48. – P. 313–317.
3. Stinson D. R. Cryptography: Theory and Practice. – CRC Press, 2002.

4. СТБ П 34.101.60–2011 «Информационные технологии и безопасность. Алгоритмы разделения секрета», Госстандарт 2011, URL: <http://nnpa.by/KartochkaDoc.php?UrlRN=261838&UrlIDGLOBAL=359544>.

5. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets. – SYNASC'2008 IEEE Comp. Soc., CPS, Los Alamitos, 2009. – P. 197–200.

6. Шенец, Н.Н. Об информационном уровне модулярных схем разделения секрета / Н.Н. Шенец // Докл. Нац. акад. наук Беларуси, сер. физ.-мат. наук, 2010. – Т. 54, № 6. – С. 9–12.

7. Threshold Secret Sharing: draft-mcgrew-tss-02, URL: <http://tools.ietf.org/html/draft-mcgrew-tss-02>.

Abstract

The secret sharing algorithms are considered. Modifications of the Belarusian standard STB 34.101.60-2011 «Information technology and security. Secret sharing algorithms» are specified.

Поступила в редакцию 18.05.2013 г.

СТАНДАРТИЗАЦИЯ ПРОТОКОЛА TLS В РЕСПУБЛИКЕ БЕЛАРУСЬ

УДК 004.056.55 (003.26)

С.В. Агневич, О.В. Соловей,
НИИ ППМИ БГУ, г. Минск

Аннотация

Протокол TLS стандартизируется в Республике Беларусь. В разрабатываемый стандарт будут включены дополнительные криптонаборы TLS, основанные на отечественных криптографических алгоритмах. В работе описываются дополнительные криптонаборы, а также связанные с ними методы аутентификации.

Введение

Для защиты соединений между клиентом и сервером в сети Интернет в большинстве случаев применяется протокол TLS (Transport Layer Security). TLS обеспечивает взаимную аутентификацию сторон протокола, конфиденциальность и контроль целостности передаваемых между сторонами данных. Последняя на сегодняшний день редакция TLS определена в RFC 5246 [1]. Стандартизация этой редакции завершается сейчас в Республике Беларусь. Предполагается, что в текущем году будет введен в действие стандарт, определяющий как собственно TLS, так и использование в TLS отечественных криптографических алгоритмов. Рабочее название стандарта – BTLSTLS является объединением нескольких субпротоколов, разбитых на два уровня. На нижнем уровне действует протокол Record, обеспечивающий шифрование и имитозащиту данных. На верхнем уровне действуют 3 протокола, основным из них является протокол Handshake. С помощью Handshake стороны согласуют применение определенных криптографических алгоритмов, формируют общий ключ, строят ключи для протокола Record, проводят аутентификацию друг друга. Применяемые алгоритмы оформляются в TLS в виде криптонабора (cipher suite). В TLS предусмотрено расширение перечня криптонаборов и методов аутентификации сторон.

BTLSTLS определяет следующие семейства дополнительных криптонаборов:

– RDPFOK_WITH_GOST два криптонабора на основе алгоритмов ГОСТ 28147 (шифрование, имитозащита), СТБ 1176.1 (хэширование), СТБ 1176.2 (ЭЦП) и протоколов формирования общего ключа в простых полях, определенных в [2];

– BIGN_WITH_BELT девять криптонаборов на основе алгоритмов СТБ 34.101.31 (шифрование, имитозащита, хэширование), СТБ 34.101.45 (ЭЦП, транспорт ключа).

Криптонаборы RDPFOK_WITH_GOST были рассмотрены в [3]. В работе рассматриваются новые криптонаборы BIGN_WITH_BELT и связанные с ними методы аутентификации.

Криптонаборы

Криптонабор определяет, какие алгоритмы шифрования, имитозащиты, генерации псевдослучайных данных и формирования общего ключа будут использоваться в сессии TLS.

Алгоритмы шифрования. В TLS могут использоваться алгоритмы шифрования трех типов: поточные алгоритмы, блочные алгоритмы и алгоритмы одновременного шифрования и имитозащиты (AEAD-алгоритмы в обозначениях [1]). В криптонаборах BIGN_WITH_BELT поддержаны все эти типы:

– алгоритм шифрования СТБ 34.101.31 в режиме счетчика (belt-ctr) используется в качестве поточного;

– алгоритмы шифрования СТБ 34.101.31 в режиме сцепления блоков (belt-cbc) используются в качестве блочных;

– алгоритмы одновременного шифрования и имитозащиты СТБ 34.101.31 (belt datawrap) используются как AEAD-алгоритмы.

Алгоритм имитозащиты. В TLS данные, зашифрованные с помощью поточных или блочных алгоритмов, должны сопровождаться имитовставками. В BIGN_WITH_BELT в необходимых случаях применяется алгоритм вычисления имитовставки, определенный в СТБ 34.101.31 (belt-mac).

Алгоритм генерации псевдослучайных данных. В TLS алгоритм генерации псевдослучайных чисел (PRF-алгоритм в обозначениях [1]) используется для построения ключей и синхропосылок, а также для верификации сообщений протокола Handshake. Стандартный PRF-алгоритм последней редакции TLS строится на основе алгоритма HMAC, который, в свою очередь, строится на некотором алгоритме хэширования. Во всех криптонаборах BIGN_WITH_BELT используется стандартный PRF-алгоритм с алгоритмом хэширования СТБ 34.101.31 (belt-hash).

Алгоритмы формирования общего ключа. В протоколе TLS имеется определенная свобода выбора алгоритма (или, точнее, механизма) формирования общего ключа. Тем не менее, в [1] описаны четыре типа таких алгоритмов, которые применяются в большинстве существующих на сегодняшний день решений. Алгоритмы двух типов не обеспечивают защиту от атак типа «противник посередине» и «чтение назад». Поэтому в BTLS были включены алгоритмы только двух оставшихся типов:

- dht-bign – транспорт ключа на основе СТБ 34.101.45 (bign-keytransport);

- dhe-bign – протокол Диффи – Хэллмана с эфемерными ключами, которые подписываются с помощью алгоритмов СТБ 34.101.45 (bign-sign).

Дополнительно в BTLS определен алгоритм формирования общего ключа, соответствующий RFC 4279 [4]:

- dht-psk-bign – транспорт ключа типа DHT_BIGN с использованием предварительно распределенных общих секретов.

В перечисленных алгоритмах формирования общего ключа используется сертификат сервера с открытым ключом СТБ 34.101.45 (bign-pubkey).

Обязательный криптонабор. Любая реализация BTLS должна поддерживать криптонабор с алгоритмом шифрования belt-ctr, алгоритмом имитозащиты belt-mac и алгоритмом формирования общего ключа dht-bign. Поддержка остальных 8 криптонаборов является необязательной.

Методы аутентификации

Аутентификация в BTLS основана на проверке действительности сертификатов открытых ключей сторон и на проверке знания сторонами соответствующих личных ключей. Для криптонаборов с алгоритмом формирования общего ключа

dht-psk-bign дополнительная аутентификация состоит в проверке знания общего секрета (предполагается, что этот секрет был надежно передан сторонам протокола, подлинность которых была предварительно проверена). При аутентификации используются сертификаты, в которых фиксируются открытые ключи алгоритмов СТБ 34.101.45 (bign-pubkey).

Аутентификация сервера. В протоколе Handshake сервер передает клиенту сертификат, который при использовании алгоритма dhe-bign содержит открытый ключ электронной цифровой подписи, а при использовании алгоритмов dht-bign и dht-psk-bign – открытый ключ транспорта. Последующее успешное завершение Handshake означает, что аутентификация сервера проведена успешно.

Аутентификация клиента. В протоколе Handshake сервер запрашивает у клиента его сертификат. В этом запросе указываются возможные типы сертификатов, который должен предоставить клиент, а также типы пар (алгоритм хэширования, алгоритм ЭЦП), которые разрешается использовать при проверке подписи сертификата. Разрешается использовать сертификаты открытых ключей типа bign-pubkey и пару алгоритмов (belt-hash, bign-sign). Сервер может запросить сертификат клиента только после предъявления своего сертификата. Успешное завершение Handshake означает, что аутентификация клиента проведена успешно.

Литература:

1. Dierks, T. The Transport Layer Security (TLS) Protocol. Version 1.2. RFC 5246 / T. Dierks, E. Rescorla. – August, 2008.
2. Проект руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа». – Минск, 1997.
3. Маслов, А.С. Криптонаборы протокола TLS, основанные на отечественных криптографических алгоритмах / А.С. Маслов, С.В. Агиевич, А.В. Федин, Д.В. Шпилевский // Информационные системы и технологии (IST'2010): Материалы VI Междунар. Конф. (Минск, 24-25 ноября 2010 г.). – Минск: А.Н. Варахсин, 2010. – С. 65–68.
4. Eronen, P. Pre-Shared Key Ciphersuites for TLS. RFC 4279 / P. Eronen, H. Tschofenig. – December, 2005.

Abstract

The TLS protocol is under standardization in Republic of Belarus. The future standard will include additional TLS ciphersuites based on domestic cryptographic algorithms. In this paper we describe additional suites and related authentication methods.

Поступила в редакцию 18.05.2013 г.

СТЕГАНОГРАФИЯ: МОДЕЛИ И МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ

УДК 519.2

Ю.С. Харин, Е.В. Вечерко,
НИИ ПМИ БГУ, г. Минск

Аннотация

В статье рассматриваются математические модели вкрапления, возникающие в задачах стеганографии. На основе марковских моделей контейнеров, среднеквадратических ошибок оценивания уровня вкрапления и вероятностей ошибок при проверке гипотез о факте

вкрапления построены оценки надежности. Представлены результаты компьютерных экспериментов.

Введение

Стеганография имеет целью сокрытие сообщений в открытых цифровых данных, называемых контейнерами.

В последние годы стеганография интенсивно развивается и применяется для скрытой передачи сообщений в потоке «безобидных данных» и для скрытой маркировки цифровых данных с помощью цифровых водяных знаков в системах защиты авторских прав DRM (Digital Rights Management) [1–5].

В настоящее время в мировом научном сообществе наблюдается стремительно растущий интерес к проблемам стеганографии: создаются компьютерные стеганографические программы, ежегодно проводятся десятки международных научных конференций по стеганографии, издаются тысячи научных статей. В то же время современный уровень развития стеганографии в основном носит эмпирический характер: отсутствует единая математическая теория построения и анализа стеганографических алгоритмов и систем, подобная теории К. Шеннона в криптографии.

Настоящий доклад посвящен актуальной проблеме стеганографической защиты информации – развитию математической теории оценки надежности стеганографической защиты информации.

Развитие математической теории стеганографической защиты информации невозможно без построения и использования математических моделей контейнеров и стегоконтейнеров, т.е. контейнеров, в которых скрыто сообщение. Перечень используемых и перспективных математических моделей представлен на рисунк 1.



1 Оценка надежности методами статистического анализа вкраплений

Проиллюстрируем применение марковской модели вкраплений для оценки надежности встраивания сообщений.

1.1 Марковская модель вкраплений

Введем обозначения: $V = \{0,1\}$ – двоичный алфавит, V_t – пространство двоичных, t – мерных векторов, N – множество натуральных чисел, $I\{A\}$ – индикатор события A , $u_{t_1}^{t_2} = (u_{t_1}, \dots, u_{t_2}) \in V_{t_2-t_1+1}$ ($t_1, t_2 \in N$, $t_1 \leq t_2$) – двоичная строка из $t_2 - t_1 + 1$ символов, $w(\cdot)$ – вес Хемминга, $L\{\xi\}$ – закон распределения вероятностей случайной величины ξ , $B(\theta)$ – закон распределения вероятностей Бернулли с

параметром $\theta \in [0,1]$.

Будем предполагать, что контейнер для встраивания сообщения есть двоичная последовательность $x_1^T \in V_T$, $x_t \in V$, $t = 1, \dots, T$ длины T , являющаяся однородной двоичной цепью Маркова 1-го порядка с симметричной матрицей вероятностей одношаговых переходов $P = (p_{j_0, j_1})$, $j_0, j_1 \in V$:

$$P = \frac{1}{2} \begin{pmatrix} 1+\varepsilon & 1-\varepsilon \\ 1-\varepsilon & 1+\varepsilon \end{pmatrix},$$

$$p_{j_0, j_1} = P\{x_{t+1} = j_1 \mid x_t = j_0\} = \frac{1}{2} (1 + (-1)^{j_0 + j_1} \varepsilon), \quad |\varepsilon| < 1. \quad (1)$$

Здесь ε – параметр модели: случай $\varepsilon = 0$ соответствует схеме независимых испытаний и исследован в [3]; случай $\varepsilon > 0$ учитывает зависимость типа притяжения, $\varepsilon < 0$ – зависимость типа отталкивания. Отметим, что цепь Маркова (1) удовлетворяет условиям эргодичности [6] и имеет равномерное стационарное распределение вероятностей $\pi = (1/2 \ 1/2)$. Далее будем полагать, что цепь Маркова (1) является стационарной.

Обычно [5] на практике сообщение перед встраиванием в контейнер подвергается криптографическому преобразованию, устраняющему статистическую избыточность, поэтому далее полагаем, что сообщение $\xi_1^M \in V_M$, $M \leq T$, является последовательностью M независимых случайных величин Бернулли: $L\{\xi_t\} = B\{\theta_1\}$, $P\{\xi_t = j\} = \theta_j$, $j \in V$, $\theta_1 = 1 - \theta_0$, $t = 1, \dots, M$. Как правило [5], $\{\xi_t\}$ имеет симметричное распределение вероятностей: $\theta_1 = \theta_0 = 1/2$.

Стегосключ γ_1^T определяет моменты времени, в которые биты сообщения ξ_1^M вкрапляются в последовательность x_1^T . Введем специальную (q, r) -блочную модель стегоключа $(q, r \in N, r \leq q)$, предполагая, что длина последовательности x_1^T кратна q : $T = Kq$. Для этого вначале разобьем последовательность x_1^T на блоки длины q : $x_{(1)} = x_1^q, x_{(2)} = x_{q+1}^{2q}, \dots, x_{(K)} = x_{T-q+1}^T$. Введем вспомогательные независимые случайные величины $\zeta_k \in V$, $L\{\zeta_k\} = B\{\delta\}$, $k = 1, \dots, K$, которые отвечают за выбор блоков $\{x_{(k)}\}$ для вкрапления сообщения: если $\zeta_k = 1$, то в r случайно выбранных бит блока $\{x_{(k)}\}$ вкрапляются r бит сообщения; если $\zeta_k = 0$, то вкрапление не производится. Отметим, что для такой модели стегоключа максимальная пропускная способность стegosистемы уменьшается до $Tr/q = Kr$ бит, а мощность множества всевозможных стегоключей сжимается до $(1 + C_q^r)^K$.

Случайная стегопоследовательность порождается следующим образом:

$$Y_t = \gamma_t \xi_{\tau_t} + (1 - \gamma_t) x_t = \begin{cases} x_t, & \gamma_t = 0, \\ \xi_{\tau_t}, & \gamma_t = 1. \end{cases} \quad (2)$$

Случайные последовательности $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ предполагаются независимыми в совокупности.

Заметим, что с практической точки зрения наибольшего внимания в рамках рассматриваемой здесь марковской модели вкраплений (1)–(2) заслуживает наиболее трудный для обнаружения вкраплений случай, когда $\theta_1 = \theta_0 = 1/2$, так как в этом случае при вкраплении одномерное распределение вероятностей не искажается: $P\{Y_t = j\} = P\{x_t = j\} = 1/2, j \in V$.

1.2 Статистическое оценивание параметров модели вкраплений

Разобьем множество V_t двоичных t -мерных векторов на $t+1$ непересекающихся подмножеств: $V_t = \Gamma_0^{(t)} \cup \Gamma_1^{(t)} \cup \dots \cup \Gamma_t^{(t)}$, где $\Gamma_0^{(t)} = \{u_t^t \in V_t : u_t = 1\}$, $\Gamma_1^{(t)} = \{u_t^t \in V_t : u_t = u_{t-1} = 0\}$, $\Gamma_j^{(t)} = \{u_t^t \in V_t : u_t = 0, u_{t-1} = \dots = u_{t-j+1} = 1, u_{t-j} = 0\}$, $1 < j < t$, и $\Gamma_t^{(t)} = \{u_t^t \in V_t : u_t = 0, u_{t-1} = \dots = u_1 = 1\}$. Такое разбиение порождает разбиение всевозможных траекторий фрагментов стежоключа $\gamma_t^t = u_t^t \in V_t$. Определим функции двоичных переменных $u_t^t \in V_p$, $y_t^t \in V_r$:

$$\varphi_t(u_t^t, y_t^t) = \begin{cases} \theta_{y_t^t}, & u_t^t \in \Gamma_0^{(t)}, \\ (1 + (-1)^{y_t^t + y_{t-j}^t} \varepsilon^j) / 2, & u_t^t \in \Gamma_j^{(t)}, 1 \leq j \leq t-1, \\ 1/2, & u_t^t \in \Gamma_t^{(t)}. \end{cases} \quad (3)$$

С учетом введенных обозначений функция правдоподобия для модели вкраплений (1)–(2) имеет вид:

$$L(\varepsilon, \delta) = \sum_{u_t^t \in V_r} I\{ \sum_{h \in \{0, r\}} b_h(u_t^t) = 0 \} (1 - \delta)^{b_0(u_t^t)} (\delta / C_q^r)^{b_r(u_t^t)} \prod_{t=1}^T \varphi_t(u_t^t, y_t^t), \quad (4)$$

где $y_t^t \in V_r$ – наблюдаемая стегопоследовательность, $b_h(u_t^t) = \sum_{k=1}^{T/q} I\{w(u_{q(k-1)+1}^{qk}) = h\}$, $h \in \{0, \dots, q\}$. Согласно определению (4), вычисление одного значения функции правдоподобия $L(\varepsilon, \delta)$ при фиксированных параметрах ε, δ имеет вычислительную сложность порядка $O(T(1 + C_q^r)^{T/q})$, то есть экспоненциальную сложность относительно длины стегопоследовательности T .

Оценки максимального правдоподобия $\hat{\varepsilon}, \hat{\delta}$ параметров ε, δ определяются как решение экстремальной задачи: $L(\varepsilon, \delta) \rightarrow \max_{\varepsilon \in (-1, 1), \delta \in [0, 1]}$. Решение этой задачи возможно только численными методами (например, методом табулирования $L(\varepsilon, \delta)$ на сетке или методом градиентного спуска), требующими вычисления функции правдоподобия для заданной последовательности точек.

Заметим, что если $q > r$, то $P\{\gamma_t^t \in \bigcup_{j=2r+2}^t \Gamma_j^{(t)}\} = 0$, $t > 2r+1$, и стегопоследовательность $\{Y_t^t\}$, определяемая в (2), при фиксированной последовательности $\{\gamma_t^t\}$ является управляемой цепью Маркова условного порядка $s_t \in \{0, \dots, 2r+1\}$, причем порядок s_t зависит от ключевой последовательности $\{\gamma_t^t\}$: $s_t = j$, если $u_t^t \in \Gamma_j^{(t)}$. Это свойство позволяет построить полиномиальный относительно T алгоритм вычисления значения функции правдоподобия $L(\varepsilon, \delta)$ для (q, r) -блочной модели вкраплений при $q > r$.

Приведем примеры частотных оценок параметров модели вкраплений (1)–(2) при фиксированных значениях параметров (q, r) . Обозначим $f_{j_0, \dots, j_{s-1}} = \sum_{t=1}^{T-s+1} I\{y_t^{t+s-1} = j_0^{s-1} \dots j_{s-1}^{s-1}\}$ абсолютную частоту s -граммы, $j_0^{s-1} \in V_s$.

Статистические оценки $\hat{\varepsilon}, \hat{\delta}$ параметров (1,1)-блочной модели вкраплений, для которой множество всевозможных стежоключей длины T совпадает с V_p , имеют вид:

$$\hat{\delta} = \begin{cases} 0, & g > 1, \\ 1 - g^{1/2}, & g \in [0, 1], \\ 1, & g < 0, \end{cases}$$

$$\hat{\varepsilon} = \frac{f_{00} + f_{11} - f_{01} - f_{10}}{(1 - \delta)^2 (T - 1)}, \quad (5)$$

где $g = \frac{(f_{00} + f_{11} - f_{01} - f_{10})^2 (T - 2)}{(f_{000} + f_{111} + f_{010} + f_{101} - f_{001} - f_{110} - f_{011} - f_{100})(T - 1)^2}$. Для модели вкраплений (1)–(2) статистики (5) являются состоятельными при $T \rightarrow \infty$ оценками параметров модели δ, ε соответственно.

Аналогично, построены статистические оценки для (2,1)-блочной модели вкраплений.

Для (1, 1)-блочной модели вкраплений методом Монте-Карло вычислены среднеквадратические ошибки $v\{\hat{\delta}\} = 1/N \sum_{n=1}^N (\hat{\delta}^{(n)} - \delta)^2$, $v\{\hat{\varepsilon}\} = 1/N \sum_{n=1}^N (\hat{\varepsilon}^{(n)} - \varepsilon)^2$ оценивания параметров модели на основе частотных статистик (5) при следующих значениях параметров: $\varepsilon = 0,3$, $\delta = 0,15$ число прогонов $N = 10^3$. На рисунке 2 изображены графики зависимостей $v\{\hat{\delta}\}, v\{\hat{\varepsilon}\}$ от длины стегопоследовательности T .

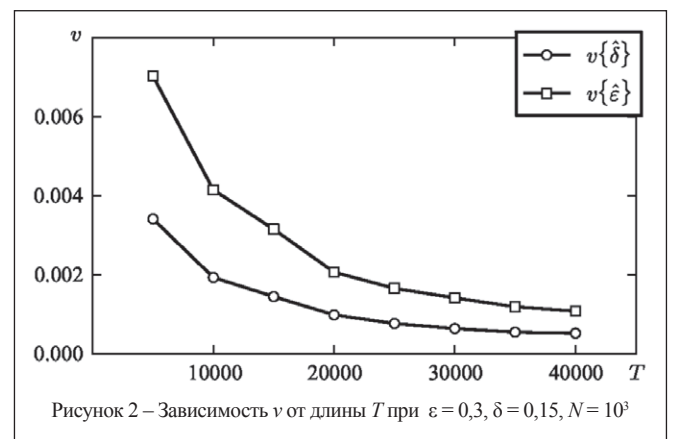


Рисунок 2 – Зависимость v от длины T при $\varepsilon = 0,3$, $\delta = 0,15$, $N = 10^3$

1.3 Оценка надежности вкрапления

Условимся говорить, что встраивание сообщения (вкрапление) является надежным (необнаруживаемым стегоаналитиком) при данном объеме материала (длине наблюдения) T , если среднеквадратическая ошибка оценивания уровня вкраплений δ достаточно велика: $E\{(\frac{\hat{\delta} - \delta}{\delta})^2\} \geq 1$, или, что эквивалентно, вариация оценки $\hat{\delta}$ удовлетворяет неравенству:

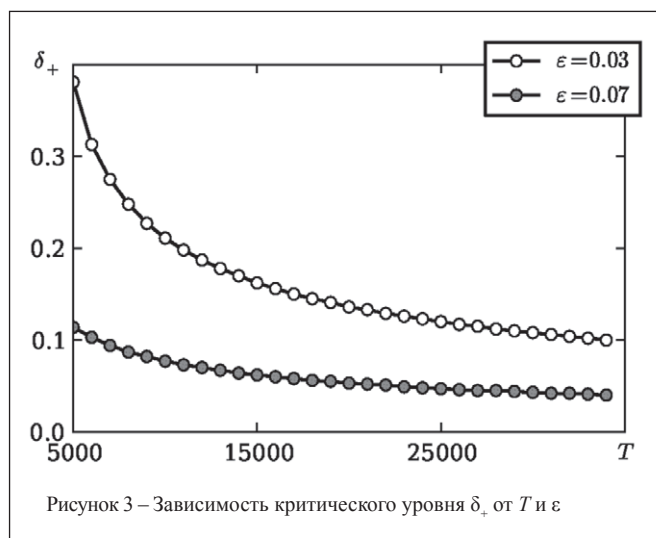
$$v\{\hat{\delta}\} = E\{(\hat{\delta} - \delta)^2\} \geq \delta^2. \quad (6)$$

Решая неравенство (6) относительно δ , находим критическую область допустимых уровней вкраплений: $\delta \in [0, \delta_+]$, где δ_+ – критический уровень вкраплений.

Для оценки $\hat{\delta}$, определяемой (5), при $T \rightarrow +\infty$ справедливо следующее выражение асимптотической дисперсии:

$$v\{\hat{\delta}\} = f(\varepsilon, \delta, T) = \frac{1}{T-1} \left(\frac{1}{2} - \frac{3}{4}(1-\delta)^2 + \frac{1}{4\varepsilon^2(1-\delta)^2} \right). \quad (7)$$

Решая неравенство (6) с учетом (7), получаем зависимость критического уровня вкраплений δ_+ от длины наблюдения T и параметра контейнера ε : $\delta_+ = \delta_+(T, \varepsilon)$. На рисунке 3 построены графики этих зависимостей. Область под каждой кривой соответствует надежному встраиванию сообщений.



Укажем еще один подход к количественной оценке надежности стеганографического алгоритма, основанный на теории статистической проверки гипотез. Определим гипотезу $H_0 = \{\delta = 0\}$ о том, что контейнер не содержит вкраплений, и альтернативу $H_1 = \bar{H}_0 = \{\delta > 0\}$, означающую, что наблюдаемый поток данных $y_1^T \in V_T$ представляет собой стегоконтейнер. Предположим, что для проверки гипотез H_0, H_1 построен оптимальный тест $d = d_0(y_1^T) \in V$, который минимизирует вероятность ошибки II рода $\beta = P_{H_1}\{d = 0\} = \beta(\epsilon, \delta, T; \alpha_0)$ среди всех тестов, вероятность ошибки I рода для которых не превосходит некоторый заданный уровень $\alpha_0 \in (0, 1) : P_{H_0}\{d = 1\} \leq \alpha_0$. Функция $\beta(\cdot) \in [0, 1]$ характеризует вероятность того, что факт вкрапления в ситуации ϵ, δ, T не будет обнаружен «самым лучшим стегоаналитиком». Являясь характеристикой не-

обнаруживаемости вкрапления, функция $\beta = \beta(\epsilon, \delta, T; \alpha_0)$ может быть принята в качестве характеристики надежности стеганографического алгоритма. Емкость заполнения контейнера δ при заданных значениях его размера T , параметра ϵ и уровня ложных тревог α_0 следует выбирать из условия гарантированного уровня надежности $\beta_{\min} \in (0, 1)$:

$$\beta = \beta(\epsilon, \delta, T; \alpha_0) \geq \beta_{\min}. \quad (8)$$

Литература:

1. Pevny, T. Steganalysis by subtractive pixel adjacency matrix / T. Pevny, P. Bas, J. Fridrich // Proceedings of the 11-th ACM Multimedia and Security Workshop. – Princeton, 2009. – P. 75–84.
2. Bas, P. Break Our Steganographic System – the ins and outs of organizing BOSS / P. Bas, T. Filler, T. Pevny // Proceedings of Information Hiding Conference. – Prague, 2011.
3. Пономарев, К.И. Параметрическая модель вкрапления и ее статистический анализ. Дискретная математика. – Т. 21, вып. 4. – 2009. – С. 148–157.
4. Харин, Ю.С. О некоторых задачах статистической проверки гипотез в стеганографии / Ю.С. Харин, Е.В. Вечерко // Вести НАН Беларуси. Серия физ.-мат. наук. – Вып. 4. – 2010. – С. 5–12.
5. Харин, Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Новое знание, 2003.
6. Кемени, Дж. Конечные цепи Маркова / Дж. Кемени, Дж. Снелл. – Наука, 1982.

Abstract

In this paper we describe some important mathematical models of embedding. Estimators of securely embedding based on markov models are constructed. The results of computer experiments are presented.

Поступила в редакцию 18.05.2013 г.

ОПРЕДЕЛЕНИЕ ОБЛАСТЕЙ ИЗОБРАЖЕНИЙ ДЛЯ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

УДК 004.056.5

М.С. Абрамович, М.Н. Мицкевич,
НИИ ППМИ БГУ, г. Минск

Аннотация

В статье описывается алгоритм встраивания цифровых водяных знаков в графические изображения. На основании визуальной характеристики определяются области изображений с высокой детализацией для встраивания данных.

Введение

Цифровые водяные знаки (ЦВЗ) предназначены для маркировки мультимедийной информации с целью ее идентификации, аутентификации, а также мониторинга ее распространения и копирования. ЦВЗ представляет собой определенную информацию, которая добавляется к цифровому объекту и может быть обнаружена или извлечена для предъявления прав на этот объект. В системах с ЦВЗ, так же как и в стеганографии, применяются методы, с помощью которых одни данные скрываются в других.

Незаметность ЦВЗ является общим требованием для всех систем ЦВЗ. Это означает, что искажения, которые вносятся водяными знаками, должны оставаться ниже определенного порога «видимости».

В связи с этим важной практической задачей при встраивании ЦВЗ в графические изображения является задача определений областей графических изображений, встраивание ЦВЗ в которые не приведет к визуальным искажениям изображений [1].

Классификация областей изображения

При встраивании данных в изображение классифицируем точки изображения на три группы. Эта классификация построена на простейших свойствах системы человеческого зрения (СЧЗ):

– точки текстур, которые не существенны для СЧЗ. В сильно текстурированные области (области которые

состоят из мелких деталей и, следовательно, имеют высокочастотный характер) можно встроить много информации. В данном случае высокочастотные мелкие элементы изображения маскируют встроенные данные;

– точки текстур, которые существенны для СЧЗ. Одним из основных свойств СЧЗ является свойство фиксировать свое внимание на отдельных частях изображения, оставляя без внимания остальные. Как правило, такими точками являются отдельные точки текстур, такие как точки контуров. Поэтому необходимо встраивать меньше данных в точки, заметные для СЧЗ;

– точки, в окрестности которых изображение нетекстурировано. СЧЗ хорошо различает высокочастотные изменения на низкочастотном фоне, по этой причине ЦВЗ в окрестности таких точек также должен иметь низкочастотный характер. С другой стороны для СЧЗ незаметен лишь небольшой объем данных, встроенных в низкочастотную область изображения.

Для разделения изображения на три определенных выше области используем детектор текстур и детектор точек важных для СЧЗ. С помощью детектора текстур получаем матрицу текстурированности в точках изображения:

$$T = (t_{i,j})_{i=0,j=0}^{M_I-1,N_I-1}.$$

С помощью детектора важных для СЧЗ точек получаем матрицу K значимости точек контуров изображения:

$$K = (k_{i,j})_{i=0,j=0}^{M_I-1,N_I-1}.$$

В качестве матрицы текстурированности T используем матрицу локальных дисперсий в точках изображения. Значения ее элементов задаются следующим образом:

$$t_{i,j} = \sum_{l,m=-N_a}^{N_a} (f_{i+l,j+m} - \bar{f}_{i,l,j+m})^2,$$

$$\bar{f}_{i,j} = \frac{1}{(1+2N_a)^2} \sum_{l,m=-N_a}^{N_a} f_{i+l,j+m},$$

где N_a, N_a – некоторые целые положительные числа.

Для нахождения матрицы $K = (k_{i,j})_{i=0,j=0}^{M_I-1,N_I-1}$ используется алгоритм детектирования контуров Канни [2]. Алгоритм Канни решает проблему получения фильтра, оптимального по критериям выделения, локализации и минимизации нескольких откликов одного контура. Канни ввел понятие Non-Maximum Suppression (подавление не-максимумов), которое означает, что пикселями границ объявляются точки, в которых достигается локальный максимум градиента в направлении вектора градиента.

Алгоритм состоит из следующих пяти шагов:

- 1) Сглаживание. Размытие изображения для удаления шума.
- 2) Поиск градиентов. Границы отмечаются там, где градиент изображения приобретает максимальное значение.
- 3) Подавление не-максимумов. Только локальные максимумы отмечаются как границы.
- 4) Двойная пороговая фильтрация. Потенциальные границы определяются порогом.
- 5) Трассировка области неоднозначности. Итоговые границы определяются путем подавления всех краев, несвязанных с определенными (сильными) границами [3].

Алгоритм встраивания ЦВЗ

Для встраивания ЦВЗ будем использовать изображение размером $N_I \times M_I$:

$$f = (f_{i,j})_{i=0,j=0}^{M_I-1,N_I-1}.$$

Предположим, что все размеры изображения N_I, M_I кратны некоторым степеням двойки N, M , т. е.

$$N_I = 2^{Nn},$$

$$M_I = 2^{Mm},$$

где $N, M > 0, N, M \in \mathbb{N}$.

Рассмотрим алгоритм для встраивания ЦВЗ с использованием матрицы текстур T (локальных дисперсий) и матрицы значимостей K , которая определяется алгоритмом Канни.

Разобьем изображение на блоки $(B_{l,m})_{l=0,m=0}^{N_I-1,M_I-1}$ размером $2^N \times 2^M$ следующим образом:

$$B_{l,m} = \begin{pmatrix} f_{l \cdot 2^N, m \cdot 2^M} & \dots & f_{l \cdot 2^N, (m+1) \cdot 2^M - 1} \\ \dots & \dots & \dots \\ f_{(l+1) \cdot 2^N - 1, m \cdot 2^M} & \dots & f_{(l+1) \cdot 2^N - 1, (m+1) \cdot 2^M - 1} \end{pmatrix}$$

Данные будут встраиваться в блоки $B_{l,m}$.

1) Для каждого блока $B_{l,m}$ вычислим его визуальную характеристику $V_{l,m}$ с использованием матрицы текстур T , матрицы значимостей K и некоторого положительного числа β , характеризующего влияние матрицы значимостей K по формуле:

$$V_{l,m} = \frac{1}{2^{N+M}} \sum_{i=-N, j=-M}^{N, M} h(t_{\ln+i, m+j} - \beta k_{\ln+i, m+j})$$

где $h(x)$ – индикаторная функция:

$$h(x) = \begin{cases} x, & x > 0, \\ 0, & x < 0. \end{cases}$$

2) Определим биты блоков $B_{l,m}$, в которые будут встроены данные. Для этого зададим два непересекающихся множества битов S_1 и S_2 для встраивания. Первое множество S_1 задает те биты блока $B_{l,m}$, встраивание в которые данных можно считать незаметным для СЧЗ независимо от характеристик самого блока. Очевидно, что эти биты должны быть наименее значимыми среди тех, из которых могут быть восстановлены встроенные данные. Второе множество S_2 задает те биты блока $B_{l,m}$, встраивание в которые данных незаметно на достаточно текстурированных и незначимых частях изображения. Эти множества определяются конкретным алгоритмом встраивания ЦВЗ.

3) Встраивание данных происходит в 2 этапа:

– сначала встраиваются данные по очереди во все блоки. В каждом отдельном блоке заменяем биты заданные в множестве S_1 битами ЦВЗ.

– задается некоторый порог T . Затем поочередно для каждого блока проверяется выполнение условия:

$$V_{l,m} > T. \quad (1)$$

Если для блока выполняется условие (1), то в нем заменяются биты, заданные в множестве S_2 .

4) Процедура встраивания битов пометок. В процедуре встраивания данных блоки разбивались по объему встраи-

ваемых данных на 2 группы в соответствии с критерием (1). Для обеспечения устойчивости необходимо встраивать в каждый блок один бит $p_{l,m}$, который бы указывал на то, была ли встроена в блок дополнительная информация.

Для встраивания пометок повторяется та же процедура, что и для встраивания данных.

При извлечении данных алгоритм выполняется в обратном порядке. Сначала извлекаются биты пометок. Затем из каждого блока извлекается информация из заданных в множестве S_1 битов. Если бит пометки равен 1, то из этого блока также извлекается информация из битов, заданных в множестве S_2 . Таким образом, при извлечении данных не требуется определять визуальные характеристики областей изображения.

Заключение

В статье предложена классификация точек изображения по отношению к чувствительности системы человеческого зрения. Разработан алгоритм встраивания

цифровых водяных знаков, использующий предложенную классификацию. Разработаны методы оценки визуальных характеристик областей изображений на основе матрицы текстурованности и матрицы контуров.

Литература:

1. Cox, I.J. Digital watermarking and steganography / I.J. Cox, et al. // Second Edition. – Morgan Kaufmann, 2007. – 624 p.
2. Canny, J.F. A computational approach to edge detection / J.F. Canny // IEEE Transaction on Pattern Analysis and Machine Intelligence, 1986. – №6. – P. 679–698.
3. Анисимов, Б.В. Распознавание и цифровая обработка изображений. – М.: Высш. школа, 1983. – 295 с.

Abstract

Algorithm for embedding digital watermarks is described in the paper. Areas on the images with high detailing are determined by visual characteristic.

Поступила в редакцию 18.05.2013 г.

НОВОСТИ

ВОЗОБНОВЛЯЕМАЯ ЭНЕРГЕТИКА



Ассоциация «Возобновляемая энергетика» (Беларусь) к расширению международного сотрудничества через «Проект по повышению потенциала Ассоциации».

Минск, Май 2013 года. Ассоциация «Возобновляемая энергетика» (АВЭ) объявляет о запуске «Проекта по повышению потенциала АВЭ».

Проект финансируется международной организацией – Центрально-Европейской Инициативой – благодаря гранту Правительства Италии по инициативе Европейского банка реконструкции и развития. Проект предполагает предоставить уникальную возможность для дальнейшего развития в Беларуси возобновляемой энергетики с выходом на новый уровень международного сотрудничества.

В ближайшие 15 месяцев группа итальянских и белорусских экспертов – в тесном сотрудничестве с Ассоциацией – объединят усилия в целях достижения основных целей и задач проекта.

Основной целью проекта является развитие международного сотрудничества Ассоциации «Возобновляемая энергетика» с повышением осведомленности и привлечения интереса иностранных инвесторов к растущему белорусскому рынку возобновляемой энергетики. Развитие рынка возобновляемой энергетики в Беларуси подкреплено на уровне законодательства. Принят Закон «О возобновляемых источниках энергии», разрабатывается вторичное законодательство.

Это позволит иметь более широкую диверсификацию топливно-энергетических ресурсов и увеличить использование имеющихся местных энергоресурсов.

«Сектор возобновляемых источников энергии в нашей стране ждет импульса к развитию. Мы должны укреплять и поддерживать имеющийся местный потенциал и привлекать международный опыт. Я уверен, что «Проект по повышению потенциала Ассоциации «Возобновляемая энергетика» сделает это возможным. Команда международных и местных консультантов сможет решить эти задачи с привлечением широкого международного опыта и ноу-хау ...», – говорит Владимир Петрович Нистюк, исполнительный директор Ассоциации.

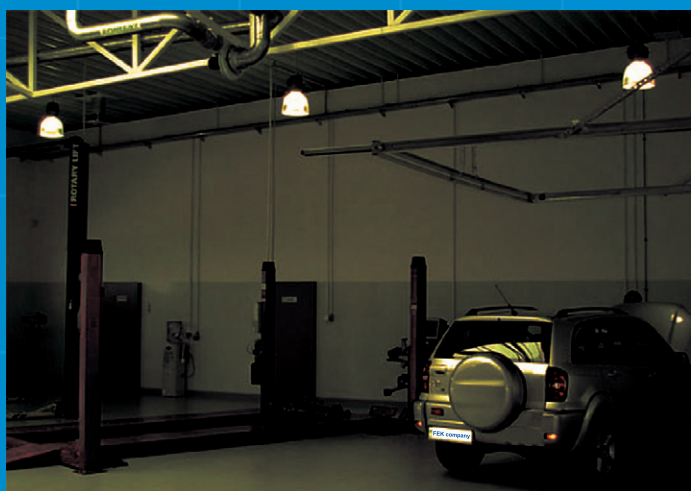
Ассоциация «Возобновляемая энергетика» была создана в 2009 году как некоммерческое объединение юридических лиц и индивидуальных предпринимателей. Фокусировка деятельности Ассоциации включает в себя внедрение технологий по использованию: энергии ветра, воды, солнечной энергии, энергии биомассы, геотермальной энергии. В настоящее время в состав Ассоциации входят 57 членов. Это государственные и частные компании и организации, индивидуальные предприниматели из Беларуси, России, Германии, Австрии и других стран ЕС. Число членов неуклонно растет. Целью деятельности Ассоциации является обеспечение правовой, информационной, консультативной и рекламной поддержки членов Ассоциации в области энергоэффективности и возобновляемых источников энергии, а также оказания сопутствующих услуг. Деятельность Ассоциации также направлена на установление и расширение международных связей и обмен передовым опытом между отечественными и зарубежными организациями, работающими в области возобновляемых источников энергии в сотрудничестве с государственными и частными организациями.

www.energy-aven.org

НАИМЕНОВАНИЕ ТОВАРА	ЦЕНА	НАЗВАНИЕ ОРГАНИЗАЦИИ	АДРЕС, ТЕЛЕФОН
ЭЛЕКТРОТЕХНИЧЕСКАЯ ПРОДУКЦИЯ			
Индукционные лампы Saturn 40, 80, 120, 150, 290, 300W. В комплекте электронный балласт	80-380 у.е.	ООО «ФЭК»	г. Минск. Тел./ф.: 200-34-23, тел.: 200-04-96. E-mail: lighting@fek.by
Индукционные лампы Smart Dragon 40, 80, 120, 150, 200, 300W.	80-380 у.е.		
Дроссели, ЭПРА, ИЗУ, пусковые конденсаторы, патроны и ламподержатели для люминесцентных ламп	Договор	ООО «Альфалидер групп»	г. Минск. Тел./ф.: 391-02-22, тел.: 391-03-33. www.alider.by
Мощные светодиоды (EMITTER, STAR), сборки и модули мощных светодиодов, линзы ARLIGHT	Договор	ООО «СветЛед решения»	г. Минск. Тел./ф.: 214-73-27, 214-73-55. E-mail: info@belaist.by www.belaist.by
Управление светом: RGB-контроллеры, усилители, диммеры и декодеры			
Источники тока AC/DC для мощных светодиодов (350/700/100-1400 mA) мощностью от 1W до 100W ARLIGHT			
Источники тока DC/DC для мощных светодиодов (вход 12-24V) ARLIGHT			
Источники напряжения AC/DC (5-12-24-48V/ от 5 до 300W) в металлическом кожухе, пластиковом, герметичном корпусе ARLIGHT, НАІТАІК			
Светодиодные ленты, линейки открытые и герметичные, ленты бокового свечения, светодиоды выводные ARLIGHT			
Светодиодные лампы E27, E14, GU 5.3, GU 10 и др.			
Светодиодные светильники, прожектора, алюминиевый профиль для светодиодных изделий			
КВАРЦЕВЫЕ РЕЗОНАТОРЫ, ГЕНЕРАТОРЫ, ФИЛЬТРЫ, ПЬЕЗОКЕРАМИЧЕСКИЕ ИЗДЕЛИЯ			
Любые кварцевые резонаторы, генераторы, фильтры (отечественные и импортные)	от 0,10 у.е.	УП «Алнар»	г. Минск. Тел./ф.: 209-69-97, тел. (029) 644-44-09. E-mail: alnar@alnar.net www.alnar.net
Кварцевые резонаторы Jauch под установку в отверстия и SMD-монтаж	от 0,10 у.е.		
Кварцевые генераторы Jauch под установку в отверстия и SMD-монтаж	от 0,50 у.е.		
Термокомпенсированные кварцевые генераторы	от 2,20 у.е.		
Резонаторы и фильтры на ПАВ			
Пьезокерамические резонаторы, фильтры, звонки, сирены	от 0,04 у.е.		
СПЕЦПРЕДЛОЖЕНИЕ			
Большой выбор электронных компонентов со склада и под заказ	Договор	ЧТУП «Чип электроникс»	г. Минск. Тел./ф.: 269-92-36. E-mail: chipelectronics@mail.ru www.chipelectronics.by
Широчайший выбор электронных компонентов (микросхемы, диоды, тиристоры, конденсаторы, резисторы, разъемы в ассортименте и др.)	Договор	ООО «Альфалидер групп»	г. Минск. Тел./ф.: 391-02-22, тел.: 391-03-33. www.alider.by
Мультиметры, осциллографы, вольтметры, клещи, частотомеры, генераторы отечественные и АКІП, APPA, GW, LeCroy, Tektronix, Agilent	1-й поставщик	ООО «Приборо-строительная компания»	г. Минск. Тел./ф.: 284-11-18, тел.: 284-11-16. E-mail: 4805@tut.by

ИНДУКЦИОННЫЕ ЛАМПЫ – НОВОЕ ЭНЕРГОЭФФЕКТИВНОЕ РЕШЕНИЕ В СВЕТОТЕХНИКЕ!

ВЫ ПЛАТИТЕ ТОЛЬКО ЗА КОМФОРТ!



Стандартное освещение

Комфортное освещение

ОСНОВНЫЕ ДОСТОИНСТВА ИНДУКЦИОННЫХ ЛАМП:

Срок службы: **> 60 000 часов.**

Светоотдача: **> 80лм/Вт.**

Энергоэффективность: эффективнее натриевых ламп на **50%**, ртутных ламп – на **70%**.

Высокий индекс цветопередачи (CRI): **Ra > 80.**

Мгновенное включение/выключение.

Неограниченное количество циклов включения/выключения.

Диапазон рабочих температур: **-40°C~+60°C.**

Экологичность продукта достигается за счет специальной амальгамы с содержанием твердотельной ртути **< 0,25мг.**



ГАРАНТИЙНЫЙ СРОК: 5 ЛЕТ.

FEK

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ФЭК»

Адрес: 220015, Республика Беларусь, г. Минск, пр. Пушкина, 29Б,
тел./факс: +375 (17) 200-34-23, +375 (29) 370-90-92, +375 (29) 274-17-13,
www.fek.by, e-mail: info@fek.by, lighting@fek.by



ЭЛЕКТРОКОНТИНЕНТ
КОНТРАКТНОЕ ПРОИЗВОДСТВО
ЭЛЕКТРОНИКИ

БЕЛОРУССКИЙ
ПРОИЗВОДИТЕЛЬ
ЭЛЕКТРОНИКИ

Контрактное производство электроники

- Автоматический и ручной монтаж печатных плат
- Поставка печатных плат
- Поставка электронных компонентов
- Поставка трафаретов из нержавеющей стали
- Разработка электроники на заказ
- Светодиодная продукция:
светодиодные экраны
светодиодные табло
светодиодные вывески
табло «бегущие строки»
информационные табло
светодиодная продукция для освещения

СОВРЕМЕННОЕ ОБОРУДОВАНИЕ
ПЕРЕДОВЫЕ ТЕХНОЛОГИИ
БОЛЬШОЙ ПОЛОЖИТЕЛЬНЫЙ ОПЫТ
ОПТИМАЛЬНЫЕ СРОКИ
ПРИЕМЛЕМЫЕ ЦЕНЫ

Республика Беларусь, 220026
г. Минск, пер. Бехтерева, 8, офис 35
тел.: (+375 17) 205 06 94, 296 31 61
VELCOM (+375 29) 115 35 75
e-mail: info@elcontinent.com
WWW. ELCONTINENT.BY



ВСЁ НЕОБХОДИМОЕ ДЛЯ АВТОМАТИЗАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И ВСТРАИВАЕМЫХ СИСТЕМ

Группа компаний **ЭЛТИКОН**

- Промышленные компьютеры, серверы, центры обработки и хранения данных;
- Встраиваемые и бортовые вычислительные системы, в т.ч. для жестких условий эксплуатации;
- ПЛК и микроконтроллеры, распределенные системы управления и сбора данных;
- Средства операторского интерфейса: мониторы, панели оператора, консоли управления, клавиатуры, трекболы, указательные устройства, информационные табло и мониторы для уличных применений;
- Устройства локального и удаленного ввода-вывода сигналов, АЦП, ЦАП, решения для управления движением, нормализаторы сигналов;
- Сетевое и коммуникационное оборудование для различных сетей, шлюзы данных, коммутаторы Ethernet, медиа-конвертеры, сетевые контроллеры, модемы, удлинители сетей, преобразователи интерфейсов, протоколов и т.п.;
- Датчики для различных применений;
- Источники вторичного электропитания для промышленных, медицинских, бортовых и специальных применений, инверторы электропитания, программируемые источники питания;
- Решения на основе полупроводниковых источников света для уличного освещения и архитектурной подсветки;
- Специализированные датчики, контроллеры и устройства для «умного дома»;
- Корпуса, конструктивы, субблоки в стандарте евромеханика, шкафы, стойки, компьютерные корпуса;
- Крепежные элементы, клеммы, монтажный инструмент, провода и кабели, кабельные вводы, соединители;
- Программное обеспечение всех уровней АСУТП, SCADA-система Genesis, OPC-серверы и средства их разработки

ADVANTECH

ADLINK
TECHNOLOGY INC.

XP

ProSOFT
АВТОРИЗОВАННЫЙ ДИЛЕР

Akiwa Technology, Inc.
SPECIALIZED CUSTOMER SERVICE AND SUPPORT

iKey

OCTAGON
SYSTEMS

Getac

iconics

LITEMAX

BELDEN
SENDING ALL THE RIGHT SIGNALS

TDK-Lambda

APC
by Schneider Electric

iBASE

IEE

Transcend

PEPPERL+FUCHS
ELCON

EtherWAN

rttd

SCAIME
L'INFINITIE PRECISION INFINITE PRECISION

WEINTEK

innoDisk
Beyond your imagination

Schroff

CEHCOOP

ifm electronic



WAGO

PLANAR

XLight

Fastwel



DATAFORTH

mcn
mikro elektronik
gmbh - nürnberg

VIPA
art of automation

InduKey
Industrial Input Devices

TRI-M
ENGINEERING

- ✓ Более 50 вендоров в программе поставок
- ✓ Широкий диапазон продукции "из одних рук"
- ✓ Сервисный центр и послегарантийное обслуживание продукции

- ✓ Компетентный анализ технических решений с гарантией совместимости и работоспособности конфигурации
- ✓ Наличие сертификатов и ГТД

- ✓ Развитая система логистики, нестандартные схемы поставок, склады в Минске, Москве и Гамбурге
- ✓ Производство промышленных компьютеров, шкафов автоматики, сборка телекоммуникационных шкафов

220125 Минск, пр-т Независимости, 183 • Тел. (017) 289-6333 • Факс (017) 289-6169 • E-mail: info@elticon.ru • Web: www.elticon.ru

УНП 191092652