идентификационные (идентификация конкретного оборудования, инструмента, набора штампов, пуансонов, которыми осуществлялись нанесение номера либо изменение его содержания). Объекты экспертизы: маркировочные обозначения и поврежденные, уничтоженные и измененные маркировочные обозначения. Примерный перечень вопросов для решения указанных задач: Какой номер имеется на данном предмете? Подвергался ли номер на предмете изменению? Если номер подвергался изменению, то каково его первоначальное содержание? Каким способом уничтожен (изменен) номер на представленном на исследование предмете? Не использовались ли для нанесения или изменения номера инструменты, изъятые у подозреваемого? и др.

Предметом судебной экспертизы идентификационных маркировочных обозначений транспортных средств являются фактические данные, устанавливаемые при исследовании идентификационных маркировочных обозначений транспортных средств, их узлов и агрегатов, с целью решения вопросов, интересующих инициатора экспертизы. Основной задачей является – установление факта изменения первоначальных маркировочных обозначений транспортных средств. Основными вопросами для решения указанной задачи будут – Изменялся ли идентификационный номер представленного транспортного средства? Если да, то каким способом? Каково его первоначальное содержание?

Таким образом, при общих положениях и направлениях исследований, имеются и отличия по предмету исследования, объектам и задачам, решаемым в ходе каждого из исследований.

Подводя итог, хотелось бы отметить, что владение предметом исследования, объектами, задачами, решаемыми в рамках каждого из исследований, знание возможностей экспертных исследований, позволит инициатору грамотно действовать при назначении соответствующей экспертизы в каждой конкретной ситуации.

ВИДЫ ИНФОРМАЦИОННЫХ СИСТЕМ, ИХ ОСОБЕННОСТИ: ПРОБЛЕМЫ КРИМИНАЛИСТИКИ

Шабанов В. Б.

Белорусский государственный университет,
пр. Независимости, 4, 220030 Минск, Беларусь, lawcrim@bsu.by

Исследуется специфика решаемых с помощью информационных систем задач, виды информационных систем, их классы. Рассматриваются средства поражения компьютерных систем и их классификация, а также разновидности информационных угроз.

Ключевые слова: информационные системы; компьютерные преступления; угроза безопасности; компьютерные вирусы; информация

Специфика решаемых с помощью информационных систем задач, различная сложность их создания, модификации, сопровождения, интеграции с другими

информационными системами и т.п., позволяют разделить информационные системы на следующие виды: открытые (для общего пользования) или закрытые (для ограниченного круга); государственные или негосударственные (корпоративные); национальные или международные; малые, средние и крупные информационные системы и т.п.

К классу малых информационных систем относятся системы уровня небольшого объема, основными признаками которых являются: непродолжительный жизненный цикл; ориентация на массовое использование; невысокая цена; практическое отсутствие средств аналитической обработки данных; наличие возможности незначительной модификации без участия разработчиков; отсутствие средств обеспечения безопасности. Признаками средних информационных систем являются: длительный жизненный цикл (возможность роста до крупных систем); наличие аналитической обработки данных; наличие штата сотрудников, осуществляющих функции администрирования аппаратных и программных средств; наличие средств обеспечения безопасности; тесное взаимодействие разработчиков программного обеспечения по вопросам сопровождения компонентов информационной системы.

Основными признаками крупных информационных систем являются: длительный жизненный цикл; миграция унаследованных систем; разнообразие используемого аппаратного обеспечения, жизненный цикл которого меньше, чем у создаваемой системы; разнообразие используемого программного обеспечения; масштабность и сложность решаемых задач; пересечение множества различных предметных областей; ориентация на аналитическую обработку данных; территориальная распределенность.

К особенностям этих сетей можно отнести: сети построены на базе современного оборудования с коммутацией пакетов; характеристика сетей (скорость передачи, достоверность) и предоставляемые ими услуги достаточно однородны; сети охватывают территорию практически всей страны, а многие из них взаимодействуют с однородными сетями зарубежных стран; операторы этих сетей находятся в конкретных отношениях, что способствует улучшению качества предоставляемых услуг, но из-за автономности их развития и отсутствия достаточной координации качество может снижаться, если взаимодействующие пользователи находятся в разных сетях.

Мировой опыт и статистический анализ случаев компьютерных преступлений в банковской и финансовой сфере показывает превалирующую долю краж денег, услуг, информации, подделки данных, вымогательства, нанесения ущерба программам; нанесения ущерба оборудованию; помех нормальной работе. В связи с этим, противодействие преступности с использованием данных систем имеет решающее значение.

По наличию умысла угрозы подразделяются на преднамеренные (с умыслом) и непреднамеренные (случайные). Злоумышленные действия можно разделить на четыре основных категория:

1) прерывание – прекращение нормальной обработки информации, например, вследствие разрушения вычислительных средств. Такая категория действий

может вызывать весьма серьезные последствия, если даже информация при этом не подвергается никаким воздействиям;

2) кража – чтение или копирование информации, хищение носителей информации с целью получения данных, которые могут быть использованы против интересов владельца (собственника) информации;

3) модификация информации – внесение несанкционированных изменений в данные, направленные на причинение ущерба владельцу (собственнику) информации;

4) разрушение данных – необратимое изменение информации, приводящее к невозможности ее использования.

Обобщая данные анализа, можно констатировать, что вероятность реализации случайных угроз выше, чем преднамеренных, но финансовый ущерб больше от реализации последних.

По этому критерию все угрозы могут быть отнесены к одному из следующих видов:

1. Вмешательство человека в работу информационной системы. Сюда относят организационные средства нарушения безопасности информационных систем (кража носителей информации, несанкционированный доступ к устройствам хранения и обработки информации, порча оборудования и т.д.) и осуществление нарушителем несанкционированного доступа к программным компонентам системы (все способы несанкционированного проникновения в системы, а также способы получения пользователем-нарушителем незаконных прав такого доступа). Меры, противостоящие таким угрозам, носят организационный характер (охрана, режим доступа к устройствам системы), а также включают в себя совершенствование систем ограничения доступа и системы обнаружения попыток атак (например, попыток подбора паролей).

2. Аппаратно-техническое вмешательство в работу информационной системы – нарушение безопасности и целостности информациив системе с помощью технических средств. Защита от таких угроз, кроме организационных мер, предусматривают соответствующие аппараттные (экранирование излучений аппаратуры, защита каналов передачи информации от прослушивания) и программные (шифрация сообщений в каналах связи) меры.

3. Разрушающее воздействие на программные компоненты информационной системы с помощью разрушающих программных средств. К таким средствам поражения информационных компьютерных систем относят следующие:

1) компьютерные вирусы, среди разнообразия которых различают (загрузочные (бутовые) вирусы, заражающие загрузочные сектора дискет и винчестеров; файловые вирусы; загрузочно-файловые вирусы; вирусы, заражающие файлы данных);

2) средства подавления информационного обмена в телекоммуникационных сетях, его фальсификации, передачи по каналам государственного и военного управления противника необходимой информации;

3) средства, позволяющие внедрять программные закладки в государственные и корпоративные информационные системы (особенно постоянно действующие в режиме реального времени) и управлять ими на расстоянии (от внедре-

ния микропроцессов и других компонентов в электронную аппаратуру и линии связи противника до создания международных сетей и систем, курируемых заинтересованными организациями). К таким средствам относят, например, нейтрализатор тестовых программ, обеспечивающих невозможность выявления естественных и искусственных недостатков программных средств специальными тестовыми программами.

Средства поражения компьютерных систем эксперты классифицируют по следующим критериям:

1) управляемость (возможность или невозможность дистанционного или непосредственного управления);

2) происхождение (самостоятельные, специально созданные или модифицированные программные средства);

3) объект воздействия (поражают системные или прикладные программы, дезорганизуют работу средств управления и др.);

4) время действия (разового или длительного действия);

5) способ ввода в действие (немедленного или отложенного действия);

6) способность к самовоспроизводству;

7) целевое предназначение (для поражения объектов информационного воздействия или для перераспределения данных).

Удаленные атаки можно классифицировать по следующим признакам:

1. По характеру воздействия – активное и пассивное. Под активным воздействием на сетевую систему понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации сети, нарушение работы сети и др.) и нарушающее политику безопасности, принятую в системе. Основная особенность удаленного активного воздействия заключается в принципиальной возможности его обнаружения (естественно, с большей или меньшей степенью сложности). Пассивным воздействием на сетевую систему называется воздействие, которое не оказывает непосредственного влияния на работу сети, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети привод к тому, что пассивное удаленное воздействие практически невозможно обнаружить.

2. По цели воздействия – перехват информации и искажение информации. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации (например, прослушивание канала в сети). Возможность искажения информации означает полный контроль над информационным потоком (например, ложный сервер).

3. По условию начала осуществления воздействия различают три вида условий начала осуществления атаки:

– атака по запросу от атакуемого объекта (атакующая программа, запущенная на сетевом компьютере, ждет посылки от потенциальной цели атаки определенного типа запроса, который и будет условием начала осуществления атаки);

– атака по наступлению определенного события на атакуемом объекте (атакующая программа ведет наблюдение за состоянием операционной системы удаленного компьютера и при возникновении определенного события в системе начинает осуществлять воздействие);

– безусловная атака (атака осуществляется немедленно после запуска атакующей программы).

4. По расположению субъекта атаки относительно атакуемого объекта – внутрисегментное, межсегментное воздействие.

По данным глобального опроса, самая распространенная угроза безопасности в мире – это компьютерные вирусы. Они вызывают нарушение работоспособности системы различными путями и в различных формах. Нарушение работоспособности системы – это угроза отказа служб (несанкционированное и некорректное изменение режимов работы системы, их модификация либо ложная подмена может привести к получению неверных результатов, отказу системы от обработки потока информации или значительным задержкам ее доставки, а также отказам в обслуживании).

Здесь различают внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные в документации на эти изделия, в том числе разработка и распространение программ, нарушающих нормальное функционирование систем (например, системы защиты информации); уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи; нарушение технологии обработки информации.

По способу воздействия на объект угрозы включают:

непосредственное воздействие на объект атаки, например, непосредственный доступ к набору данных, программе, как в результате ошибки, так и преднамеренно;

воздействие на систему разграничения полномочий и разрешений (в том числе захват привилегий).

При этом способе несанкционированные действия выполняются относительно прав пользователей, а сам доступ к объекту осуществляется впоследствии законным путем; опосредованное воздействие (через других пользователей); «маскарад», когда пользователь присваивает себе каким-либо образом полномочия другого пользователя; «использование вслепую», когда один пользователь заставляет другого выполнить необходимые действия, причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться компьютерный вирус либо программная закладка.

По уровню информационной системы потенциальные угрозы могут быть систематизированы в отношении:

оборудования пользователя (должностных лиц, операторов);

оборудования локальных сетей;

оборудования транспортной сети, обеспечивающего передачу информации по каналам связи.

Угрозы, связанные непосредственно с оборудованием пользователя могут включать в себя:

чтение информации с экрана посторонним лицом (во время отображения информации на экране законным пользователем или при отсутствии законного пользователя на рабочем месте);

чтение информации с документов; хищение носителей информации;

подключение к соответствующим устройствам либо к их составным частям (платам, блокам) специально разработанных аппаратных средств, копирующих информацию или программное обеспечение с последующим снятием;

несанкционированный доступ к операционной системе и программному обеспечению;

копирование информации из электронной памяти посторонним лицом;

нарушение конфиденциальности информации посторонним лицом;

несанкционированное стирание информации из архива до истечения срока ее хранения;

несанкционированное копирование, модификация, уничтожение программного обеспечения;

хищение носителей ключевой и парольной информации либо их несанкционированное копирование;

несанкционированное обращение к базам данных.

В пределах локальной сети комплекс угроз может включать в себя следующие механизмы: нарушение конфиденциальности информации, т.е. ее передача без шифрования либо переадресация; перехват информации при ее передаче по соединительным линиям; извлечение открытой либо зашифрованной информации при ее промежуточном хранении в технических средствах обработки и коммутации; уничтожение (стирание) открытой, зашифрованной информации при долговременном хранении ее в центрах обработки. Данный комплекс угроз требует трансформации программного обеспечения (включения программных закладок) либо применения специальной аппаратуры.

Следует отметить, что приведенный комплекс угроз в отношении оборудования пользователя и вычислительной сети, за исключением угроз, связанных с электромагнитным излучением, возможен в основном со стороны персонала при их несанкционированных действиях либо со стороны разработчиков программно-технических средств, преднамеренно использующих программно-аппаратные закладки.

В транспортной сети угрозы возникают ввиду наличия внешних и внутренних угроз к сообщениям, а при хранении информации – угроз хранилищу данных. Внешние угрозы сообщениям исходят от несанкционированных пользователей со стороны канала связи и могут проявляться следующим образом: перехватом сообщений; модификацией сообщений; повторным воспроизведением сообщений; уничтожением сообщений; формированием ложных сообщений; переадресацией сообщений; анализом трафика с целью раскрытия характера и объема передаваемых данных, частоты передачи и т.д.

Целью комплекса внешних угроз является дезорганизация работы сети, включая навязывание ложной информации пользователю при приеме или создание эффекта «затруднения» связи.

Угрозы хранилищу данных возникают в оборудовании транспортной сети (в центрах коммутации пакетов, сообщений) при реализации режима отлаженной доставки информации пользователю и включают в себя: модификацию маршрутизации информации, когда несанкционированные изменения содержимого справочника могут привести к неправильной маршрутизации сообщений при их

потере; модификацию адресной части хранимого сообщения, которая приводит к упомянутым выше последствиям; несанкционированный доступ к сообщениям; преждевременное воспроизведение, когда несанкционированный пользователь создает копию сообщения задержанной доставки и посылает эту копию заданному получателю, пока оригинал еще удерживается для доставки. Преждевременное получение сообщения либо его двукратное получение может запутать получателя.

Рассмотренный комплекс угроз хранилищу данных требует защиты от несанкционированной модификации сетевого и системного программного обеспечения, а также защиты от несанкционированного доступа к хранящимся сообщениям.

О НЕКОТОРЫХ СПОСОБАХ И ПРИЕМАХ ВЫЯВЛЕНИЯ И ПРОВЕРКИ АЛИБИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Шишковец И. И.

УО ФПБ «Международный университет «МИТСО»
ул. Казинца, д. 21, к. 3, 220099, г. Минск, Беларусь, clamrb@yandex.by

Исследуются способы и приемы выявления и проверки алиби в процессе расследования преступлений. На основании результатов анализа взглядов исследователей и современной практики разработан алгоритм проверки алиби, обоснованы актуальные способы проверки алиби путем проведения следственных действий (проверка показаний на месте, очная ставка, допрос), наблюдения за поведением подозреваемого, обвиняемого), а также такие тактические приемы выявления алиби, как постановка внезапных вопросов; детализация показаний; создание у допрашиваемого представления о полной осведомленности следователя; последовательное и усиливающее предъявление допрашиваемому доказательств; прямая и обратная аргументация и др. Автором обоснованы предложения по дополнению ст. 6 Уголовно-процессуального кодекса Республики Беларусь, а также разработке «Методических рекомендаций для использования в работе следственных органов при заявлении алиби подозреваемым (обвиняемым)».

Ключевые слова: алиби; расследование преступлений; выявление и проверка алиби; ложное алиби; проверка показаний на месте; очная ставка; допрос; детализация показаний

Выявление и проверка алиби на предмет разоблачения лжи в ходе раскрытия и расследования преступлений была актуальной на всех исторических этапах борьбы с преступностью. Традиционно алиби (от лат. Alibi – где-либо в другом месте) определяется как применяемый в уголовно-процессуальном праве термин, определяющий невиновность и непричастность обвиняемого или подозреваемого к инкриминируемому преступлению в силу того, что во время его совершения они не могли находиться на месте совершения преступления, так как находились в ином месте [1].

Отдельные исследователи справедливо указывают на двойственную юридическую природу алиби: уголовно-процессуальную, которая обеспечивает доказывание в уголовном процессе, критерии допустимости доказательств и др.,