МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИСТОРИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра источниковедения

КУЛЬБИЦКИЙ
Денис Вячеславович

Роль обеспечения информационной безопасности в архивах организаций Республики Беларусь

Магистерская диссертация

Научный руководитель:
доцент кафедры источниковедения
к.и.н. Липницкая Ольга Львовна

Минск, 2019

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ИТ – Информационные технологии

ИБ – Информационная безопасность

СУИБ (ISMS) – Система управления информационной безопасности (Information security management system)

CRAMM (CCTA Risk Analysis and Management Method) – метод CCTA анализа и контроля рисков

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – оценка критичных угроз, активов и уязвимостей

COBIT (Control Objectives for Information and Related Technologies) – задачи управления для информационных и смежных технологий

ГА – Группа анализа

International Organization for Standardization (ISO) – Международная организация по стандартизации;

ГоСУОК – Государственная система управления открытыми ключами
ЕСИФЮЛ – Единая система идентификации физических и юридических лиц

ВВЕДЕНИЕ

Широкое использование информационных технологий, позволяет эффективно организовать систему управления в различных организациях, частью которой являются информационное обеспечение, работа с документированной информацией. Процессы информационной глобализации, идеи формирования «информационного общества», «электронного правительства», «цифровой организации» стало мировой тенденцией. Вместе с тем современные информационные технологии – это не только новые возможности, но и в определенной мере вызов, проверка готовности организаций эффективно применять эти технологии на практике.

Возникают теоретические и практические вопросы перехода от бумажного к электронному документообороту, которые нуждаются в дальнейшей проработке, а впоследствии в нормативном регулировании и учете в реальной управленческой деятельности. Главная проблема – это организация архивного хранения документированной информации, созданной в электронной форме. И вторая порблем – это правовой статус электрнонного документа и содержшейся в нем информации и юридических последствий.

Повсеместно происходит внедрение электронного архива в организациях по всей Беларусии, но только в Белорусском научно-исследовательском центре электронной документации (далее – БелНИЦЭД) функционирует специализированный архив для хранения документированной информации, созданной в электронной форме.

В таких организациях как ОАО «Банк БелВЭБ», «Приорбанк» ОАО, Государственный Комитет по науке и технологиям Республики Беларусь проходит только подготовка к аттестации электронного архива.

Мировое сообщество признало необходимость принять новые законы, позволяющие использовать электронные документы в качестве доказательства и, более того, разрешать заключение договоров, а также представление административных документов и запросов в электронной форме. Возможно, наиболее важным из законов является (ЮНСИТРАЛ) Типовой закон о международной коммерческой и согласительной процедуре Комиссии ООН 2002 г. [107] Типовой закон представляет собой законодательный текст, который рекомендуется государствам для включения в их национальное право. Инкорпорируя текст типовых законодательных положений в свою правовую систему, государство может изменить или исключить некоторые положения. В той или иной форме этот закон был принят по меньшей мере в 31 стране. Другие страны приняли законодательство о цифровой подписи, которое, как правило, разработано по образцу Типового закона ЮНСИТРАЛ об электронных подписях 2001 г., что также влияет на использование электронных

документов для установления деловых отношений и взаимодействия с другими юридическими и физическими лицами.

Для обеспечения приемлемости и надежности электронных документов необходимо выполнить определенные правовые требования и обязательства. Например, в соответствии с Типовым законом ЮНСИТРАЛ об электронной торговле 1996 г. при оценке доказательного веса электронного документа учитывается надежность способов создания, методов передачи и хранения, которыми целостность информации поддерживалась в соответствии с тем, каким образом идентифицирован ее источник, и любым другим соответствующим фактором

Несоблюдение соответствующих мер информационной безопасности в отношении электронных документов может представлять собой нарушение правовых обязательств в некоторых странах и привести к штрафам. Так, например, в соответствии с Законом Боснии и Герцеговины об электронных документах к нарушениям, на которые налагается штраф в размере до 7500 евро, относятся:

- Предотвращение проверки подлинности и целостности электронных документов;
- Архивирование электронных документов в таком виде и с использованием таких технологий и процедур, которые не обеспечивают разумной гарантии их подлинности и целостности в течение всего срока хранения;
- Применение информационных систем с неадекватной защитой персональных данных в соответствии с положениями закона, регулирующего защиту персональных данных и др.

Для соблюдения правовых требований, касающихся сохранения подлинности и целостности электронных документов на протяжении всего жизненного цикла, организациям следует создать систему управления информационной безопасности (СУИБ), основанную на учете рисков, например, чтобы избежать проблем с использованием электронных документов в случае судебных разбирательств.

Слабая защита информации может привести к финансовым потерям, навредить репутации предприятия и принести ущерб коммерческим операциям. Именно поэтому разработка системы управления информационной безопасностью и ее внедрение в организации является столь важным. [20]

Сегодня наиболее распространенными и опасными угрозами информационной безопасности являются кража информации, халатность сотрудников организаций, вредоносные программы, саботаж, хакерские атаки, финансовое мошенничество, спам, аппаратно-программные сбои, кража оборудования. [34, 115]

По официальным данным Министерства внутренних дел Республики Беларусь. (Приложение А) [104] по направлению деятельности подразделений в сфере высоких технологий в январе – декабре 2018 года в сравнении с прошлым годом свидетельствует о значительном увеличении (+53%; с 3099 до 4741) количества зарегистрированных киберпреступлений ().

При этом число выявленных подразделениями РПСВТ уголовно наказуемых деяний увеличилось во всех регионах, наиболее значительно в Брестской (в 2,1 раза; с 343 до 728), Минской (+92,2%; с 396 до 761) и Гомельской (+52,2%; с 370 до 563) областях.

От общего числа зарегистрированных уголовно наказуемых деяний к категориям особо тяжких и тяжких относятся 62 или 1,3% (2017 г. – 68 или 2,2%), менее тяжких – 3 699 или 78,0% (2017 г. – 2 484 или 80,1%), не представляющих большой общественной опасности – 980 или 20,7% (2017 г. – 547 или 17,7%).

Более двух третьих преступлений (75,6% или 3 585; 2017 г. – 74,8% или 2 318), выявленных в сфере высоких технологий, относятся к хищениям путем использования компьютерной техники (ст. 212 УК). Число таких преступлений, относящихся к категориям особо тяжких и тяжких, увеличилось (+2,3%; с 43 до 44). Большинство данных преступлений выявлялось в г. Минске – 22, Витебской – 6 и Гродненской – 5 областях.

Количество выявленных преступлений против информационной безопасности (ст.ст. 349 – 355 УК) увеличилось в целом по республике (+48,0%; с 781 до 1 156), в т. ч. в Брестской (в 2,9 раза; с 88 до 252), Минской (в 2,1 раза; с 77 до 160) областях, г. Минске (+42,9%; с 245 до 350), Могилевской (+22,0%; с 82 до 100) и Гомельской (+12,1%; со 116 до 130) областях. При этом число таких преступлений, относящихся к категориям особо тяжких и тяжких, уменьшилось (-28,0%; с 25 до 18). Большинство данных преступлений выявлялось в Минской – 7, Брестской – 6 областях, г. Минске и Могилевской области – по 2 в каждом регионе.

Рост числа уголовно наказуемых деяний против информационной безопасности обусловлен увеличением количества преступлений, связанных с несанкционированным доступом к компьютерной информации (+97,4%; с 462 до 912).

В результате проведенных оперативно-розыскных мероприятий сотрудниками подразделений РПСВТ установлено 1 283 лица (2017 г. – 1 052), виновных в совершении преступлений. К уголовной ответственности привлечено 1 139 (2017 г. – 956) граждан, в т. ч. 369 (2017 г. – 294), имеющих судимость, 849 (2017 г. – 683) неработающих и неучащихся, 35 несовершеннолетних (2017 г. – 34).

Сумма установленного материального ущерба от совершения квалифицированных преступлений составила 1 228,4 тыс. рублей (2017 г. – 3 193,3 тыс. рублей).

Число преступлений по направлению деятельности сферы высоких технологий (по оконченным расследованием уголовным делам) совершенных лицами, имеющими судимость, увеличилось (+20,6%; с 384 до 463). При этом уменьшилось количество данных уголовно наказуемых деяний, совершенных несовершеннолетними и при их соучастии (-45,8%; со 120 до 65) и группой лиц (-44,2%; со 199 до 111).

Во многом неожиданный трехкратный рост объема скомпрометированных данных свидетельствует о растущей день ото дня ценности данных в цифровом виде. Злоумышленники поняли это раньше, чем владельцы информации, которые до сих пор не всегда готовы оценить в деньгах свои информационные активы. Между тем очевидно, что дальнейшее развитие подходов к обеспечению информационной безопасности данных неизбежно потребует оценки стоимости активов, ясного представления, прежде всего, от владельцев информации, относительно того, какие данные для них важны, каковы финансовые потери в случае утечки этих данных.

Наиболее «привлекательными» для злоумышленников и, как следствие, уязвимыми отраслями оказались: сегмент высоких технологий, торговля, финансовый сектор. Наибольший объем скомпрометированных данных пришелся на интернет-сервисы. Средний бизнес по-прежнему в большей степени подвержен утечкам персональных данных, чем крупные компании.

Сообщения об утечках не сходят со страниц СМИ, что связано как с масштабом явления (сотни миллионов скомпрометированных данных), так и с громкими именами компаний, пострадавших от утечек: Amazon, Apple, Blizzard Entertainment Inc, BMW, Dell, eBay, Facebook, Google, McDonald’s, Microsoft, MySpace, Nokia, T-Mobile, Tumblr, Twitter, Uber, Valve, VTech, Yahoo.

За I полугодие 2017 года Аналитическим центром InfoWatch зарегистрировано 840 случаев утечки конфиденциальной информации. Это на 16% больше, чем за аналогичный период 2016 года (723 утечки). [26]

В исследовании отмечали, что современная глобальная картина утечек данных с незначительными изменениями воспроизводится во всех странах, где оперируют информацией в электронном виде. Причем субъективно воспринимаемая ценность информации (как для злоумышленников, так и для владельцев) зависит не от географии, а от степени развития экосистемы, построенной вокруг данных – от уровня «дигитализации» (возможности преобразовать физические и отсканированные материалы в информацию, легко поддающуюся электронному поиску и категоризации региона.

В странах, где персональные данные в электронном виде позволяют быстро и удобно получить государственные и прочие услуги, заменяют

бумажные документы, велика вероятность, что эти данные будут использоваться неправомерно. Пример – США, где кража личности (англ. Identity theft) — преступление, при котором незаконно используются персональные данные человека для получения материальной выгоды. Английский термин появился в 1964.) давно превратилась в обыденное преступление. Причем за кражей личности стоят, как правило, не квалифицированные хакеры, а обычные люди – медсестры, официанты, полицейские, которые всего лишь хотят подзаработать немного денег на использовании чужих данных.

В менее развитых регионах ситуация иная. В количественном выражении утечек значительно меньше, но их масштаб, характер вполне сопоставим с «лучшими образцами» западного мира.

Проблемой внедрения качественной системы управления безопасностью в той или иной компании, является следствие того, что наряду с ограниченными финансовыми возможностями предприятий в Республике Беларусь, недостаточно информации о преимуществах и практиках внедрения систем менеджмента безопасности и её документационного обеспечения.

В этой работе рассматриваются различные аспекты данной проблемы и предлагаются решения путем предоставления требований, основанных на различных международных стандартах и практиках.

В работе используются такие термины, как информационная безопасность (далее – ИБ), защита информации, система управления информационной безопасности (далее – СУИБ). Автор при их определении использует определения, зафиксированные в СТБ ISO27000-2012: *информационная безопасность* – состояние сохранности информационных ресурсов и защищенности, законных прав личности и общества в информационной сфере, или это процесс (деятельность) обеспечения конфиденциальности, целостности и доступности информации; *защита информации* – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации; [87] *СУИБ* – набор политик, процедур, руководств и связанных активностей, ресурсов, поддерживаемых организацией для защиты информации. [49]

Объектом исследования является электронный архив организации. Предметом данного исследования является информационно-документационное обеспечение информационной безопастности.

Цель магистерской диссертации: оценить существующую в архивных организациях систему информационной безопасности и предложить рекомендации по документационному обеспечению системы управления

информационной безопасностью в архивах организаций Республики Беларусь.

Для достижения поставленной цели, были поставлены следующие задачи:

1. установить степень исследования и современные подходы к организации систем управления информационной безопасностью в целом;
2. сравнить и выявить особенности зарубежных стандартов и стандартов Республики Беларусь в области информационной безопасности;
3. определить виды угроз, рисков при организации электронного архива и варианты управления ими;
4. разработать комплекс мероприятий по усовершенствованию документационного обеспечения системы управления информационной безопасности для архивов организаций.

Хронологические рамки исследования определяются периодом с 2012 по 2019 год.

Работа состоит из четырех глав.

Первая глава освещает вопросы, связанные с источниками и историографией данной проблемы.

Во второй главе внимание уделяется анализу видов угроз, рисков при организации электронного архива и варианты управления ими.

Третья глава посвящена обзору и сравнению семейства стандартов информационной безопасности и выявления основных тенденции в информационной безопасности.

В четвертой главе рассматриваются вопросы управления и документационное обеспечение СУИБ и организация работы с документами в электронном виде в архивах организаций.

Теоретическая значимость диссертационного исследования состоит в реализации комплексного подхода при разработке политики информационной безопасности для архивов организации.

Практическая значимость работы определяется тем, что ее результаты позволяют повысить степень защиты информации в архивах организации путем грамотного проектирования политики информационной безопасности.

.

ГЛАВА 1. ИСТОЧНИКИ, ИСТОРИОГРАФИЯ И МЕТОДЫ ИССЛЕДОВАНИЯ

1.1 Источники

Правовое обеспечение в сфере информационной безопасности в Республике Беларусь включает в себя огромной комплекс нормативных правовых актов.

Источниковая база исследования состоит из нормативных правовых актов (далее – НПА), технических нормативные правовых акты (далее – ТНПА), и международных договоров в области информационной безопасности, которые в той или иной степени затрагиваюТ вопросы менеджмента информационной безопасности.

В Основном законе государства – Конституции Республики Беларусь от 15 марта 1994 г. гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды; и указывается, что пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав. [57, ст. 34]

Приоритетным направлением в обеспечении информационной безопасности в Республике Беларусь было и остается развитие законодательства в этой сфере. К международным нормативным правовым документам в области информационной безопасности следует отнести Модельный закон «О безопасности»», который был принят 15 октября 1999 г. № 9-9 Постановлением Межпарламентского комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан, Модельный закон «Об информации, информатизации и обеспечении информационной безопасности»», принятый Постановлением Межпарламентской Ассамблеи государств - участников Содружества Независимых Государств (далее – МПА СНГ) 18 ноября 2005 года № 26-7 и уточненный постановлением МПА СНГ № 41-1 от 28 ноября 2014 года. [105]

Межпарламентская ассамблея государств – участников Содружества Независимых Государств рекомендовала направить этот модельный закон в парламенты государств - участников МА СНГ для использования в национальном законодательстве в сфере безопасности с целью их гармонизации. [79, 81]

В соглашениях 2017 года между Правительством Республики Беларусь и Правительством Российской Федерации и Республики Казахстан были выработаны понятия, основные направления сотрудничества, общие принципы сотрудничества, основные формы и механизмы сотрудничества Разработан перечень основных угроз в области международной информационной безопасности, их источников и признаков. [100]

Целью Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. [101] является проведение совместных скоординированных мероприятий, направленных на обеспечение информационной безопасности в государствах – участниках данного Соглашения. При этом его государства-участники будут взаимодействовать, и сотрудничать по следующим основным направлениям:

- сближение нормативных правовых актов и нормативно-методических документов, регламентирующих отношения в сфере обеспечения информационной безопасности;
- нормативное правовое обеспечение развития производства программно-технических средств и средств защиты информации;
- разработка межгосударственных стандартов в области информационной безопасности, совместимых с международными стандартами;
- реализация согласованных мероприятий, направленных на недопущение несанкционированного доступа к информации информационных систем и ее утечки по техническим каналам;
- обобщение, распространение и внедрение передового опыта;
- организация и проведение научных конференций, симпозиумов и совещаний и др.

При разработке структуры системы в сфере информационной безопасности необходимо классифицировать правовые нормы, затрагивающие вопросы по обеспечению информационной безопасности, по отраслям законодательства.

Примером могут являться нормы, относящиеся к ответственности за нарушение законодательства в рассматриваемой сфере.

Кодифицированные нормативные правовые акты включают существенное количество правовых норм, затрагивающих различные вопросы по обеспечению информационной безопасности. [15, с. 40]

В Гражданском кодексе Республики Беларусь содержатся нормы, касающиеся служебной и коммерческой тайны, закрепляется такая форма отношений, как информационные услуги, электронная подпись признается как средство, подтверждающее подлинность сторон в сделках, предусматривается ответственность за незаконное использование информации. [30, ст. ст. 140, 161, 733, 1011]

В Уголовном кодексе Республики Беларусь закрепляется ответственность за преступления против информационной безопасности (гл. 31), а также иные составы преступлений в информационной сфере (хищение путем использования компьютерной техники (ст. 212), умышленное разглашение государственной тайны (ст. 373), разглашение государственной тайны по неосторожности (ст. 374), умышленное разглашение служебной тайны (ст. 375) и т.д.). [110, ст. ст. 212, 349-355, 373-375]

Кодексом Республики Беларусь об административных правонарушениях определяются административно-правовые санкции за правонарушения в информационной сфере. К таким правонарушениям относятся: отказ в предоставлении гражданину информации (ст. 9.6), несанкционированный доступ к компьютерной информации (ст. 22.6), нарушение правил защиты информации (ст. 22.7) и т.д. [54, ст. ст. 9.6, 22.6, 22.7]

Трудовым кодексом Республики Беларусь для работников устанавливается обязанность хранить государственную и служебную тайну, не разглашать коммерческую тайну нанимателя, коммерческую тайну третьих лиц, к которой наниматель получил доступ. [109, ст. 53]

Налоговый кодекс Республики Беларусь (общая часть) включает нормы, определяющие порядок защиты различных видов конфиденциальной информации. [69]

Среди основных нормативных правовых актов в области информационной безопасности особое место принадлежит законам Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» и от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи». [86, 89]

Закон «Об информации, информатизации и защите информации» является комплексным нормативным правовым актом. Он регулирует важнейшие области для информационного общества: доступ к информации и защиту информации. Закон устанавливает принципы правого регулирования информационных отношений, свободы поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, пользования информацией; принцип установления ограничений распространения и (или) предоставления информации только законодательными актами Республики Беларусь; а также принцип защиты информации о частной жизни физического лица и персональных данных. Кроме этого в законе определена обязанность государственных органов, общественных объединений, должностных лиц предоставлять гражданам возможность ознакомления с информацией, затрагивающей их права и законные интересы, а также право граждан на получение, хранение и распространение полной, достоверной и своевременной информации о

деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни.

Закон «Об электронном документе и электронной цифровой подписи» направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

Важную роль в правовом регулировании в области обеспечения информационной безопасности играют указы Президента Республики Беларусь и постановления Совета Министров Республики Беларусь. Среди данных правовых актов можно выделить основные блоки нормативных правовых актов: о защите информации (в том числе технической защиты); о доступе граждан к информации; о компетенции органов государственной власти в сфере защиты информации; о международном сотрудничестве в данной сфере, включая государства-члены Содружества Независимых Государств. [15] К таким законодательным актам можно отнести: указы Президента Республики Беларусь.

Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 утверждена Концепция национальной безопасности Республики Беларусь. [88] В документе развит ряд важнейших направлений обеспечения национальной безопасности, использованы принципиально новые подходы.

Уточнены и расширены ключевые понятия. Основные сферы национальной безопасности дополнены научно-технологической и демографической сферами. Определена роль и место Республики Беларусь в условиях глобализации международных отношений. Определены основные национальные интересы, представляющие собой совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства. Существенно расширена характеристика текущего состояния национальной безопасности.

Указ Президента Республики Беларусь от 01 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» [80] регламентирует вопросы, связанные с передачей данных, в том числе через сеть Интернет.

Принятие Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» [83] направлено на повышение эффективности деятельности государственных органов и организаций при осуществлении государственной информационной политики, создание единой системы оказания

государственных услуг в электронной форме, совершенствование регулирования в сфере информационно-коммуникационных технологий (далее – ИКТ).

По Указу Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» [84], создается Государственный реестр критически важных объектов информатизации, и определен порядок отнесения объектов информатизации к критически важным и обеспечения безопасности критически важных объектов информатизации.

Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» [85] утверждено Положение о технической и криптографической защите информации в Республике Беларусь. Положение определяет правовые и организационные основы технической и криптографической защиты информации в Республике Беларусь.

Следует упомянуть постановление Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645 «О некоторых вопросах интернет-сайтов государственных органов и организаций», которое признав утратившим силу постановление Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192» [82], утвердило Положение о порядке функционирования интернет-сайтов государственных органов и организаций.

В положении определен порядок функционирования официальных сайтов государственных органов, государственных организаций, в глобальной компьютерной сети Интернет, а также требования к содержанию этих интернет-сайтов.

Необходимую терминологию и информацию по менеджменту информационной безопасности содержат ряд принятых Республикой Беларусь ТНПА. Среди них:

– СТБ ISO/IEC 27000-2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь», в котором представлены общий обзор серии стандартов системы менеджмента информационной безопасности; введение в СУИБ; краткое описание процесса "Планируй – Делай – Проверяй – Действуй" (Plan-Do-Check-Act); термины и определения, используемые в серии стандартов СУИБ; [49]

– СТБ ISO/IEC 27001-2011, «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», который содержит требования к разработке, внедрению, обеспечению функционирования, мониторингу, анализу, поддержке и улучшению документально оформленной СУИБ в контексте

общих бизнес-рисков организации. Стандарт устанавливает требования к внедрению средств управления безопасностью с учетом потребностей конкретных организаций и их подразделений; [50]

– СТБ ISO/IEC 27002-2012, «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности». Этот стандарт устанавливает общие правила планирования, реализации, сопровождения и улучшения информационной безопасности в организации и может служить в качестве практического руководства по разработке стандартов организаций по информационной безопасности и реализации эффективного менеджмента безопасностью, а также для обеспечения конфиденциальности при меж организационном взаимодействии. [47]

Выполнение требований ISO/IEC 27001 2013 позволяет организациям формализовать и структурировать процессы управления информационной безопасностью по следующим направлениям: разработка политики безопасности, организация информационной безопасности, организация управления внутренними активами и ресурсами, составляющими основу ключевых бизнес-процессов, защита персонала и снижение внутренних угроз, физическая безопасность и безопасность окружающей среды, управление средствами связи и эксплуатацией оборудования, управление и контроль доступа, разработка и обслуживание аппаратно-программных систем, управление непрерывностью бизнес-процессов, соответствие требованиям стандарта и соблюдение правовых норм по безопасности. Цели и механизмы контроля стандарта ISO/IEC 27001 2013 по каждому из направлений работ заимствованы из стандарта ISO/ IEC 17799 2005 (разделы 5-15) и перечислены в его Приложении А – Control objectives and controls. [78]

– Стандарт ISO 15489-1:20016 «Информация и документация – управление документами. Часть 1: Общие принципы» занимает главное место стандартизации управления документами, он определяет основные принципы управления документами независимо от видов носителей и используемых технологий.

На его основе был разработан и утвержден белорусский стандарт СТБ ISO 15489-1:2016 «Информация и документация – управление документами. Часть 1: Общие принципы», который распространяется на управление документами (всех форматов и на всех носителях), создаваемыми или получаемыми организацией в процессе ее деятельности либо лицом, на которого возложены обязанности по созданию и обеспечению сохранности документов. В нем содержатся рекомендации по определению ответственности организаций за документы, политику и порядок управления документами, документные системы, а также за процессы, связанные с ними. Стандарт предназначен для

применения руководителями организаций, специалистами по управлению документами, информацией и технологиями, иными работниками организаций и лицами, на которых возложены обязанности по созданию и обеспечению сохранности документов. [113]

Анализируя принятые стандарты по информационной безопасности в Республике Беларусь, можно сказать, что они отвечают европейским требованиям, но существует ряд отличий.

Также следует отметить, что отсутствует отраслевой стратегический документ, регулирующий основы государственной политики в сфере информационной безопасности. Нормирование отдельных областей реализуется, как правило, не в единой системе и, как следствие, не взаимосвязано. Это приводит к несогласованности норм, и как следствие может привести к беспорядку и появлению новых рисков в сфере информационной безопасности.

1.2. Историография

Информатизация деятельности архивной отрасли в Беларуси начала развиваться с 2000-х годов и продолжается и по настоящее время. На сегодняшний момент основными задачами научных исследований – это поиски путей повышения эффективности делопроизводство и архивного дело путем внедрения информационных технологий.

Для реализации данных задач в 1998 г. в структуре архивной отрасли был создан Белорусский научно-исследовательский центр электронной документации (БелНИЦЭД). [97]

Приоритетными направлениями в исследованиях БелНИЦЭД является: создание информационных систем по учету документов национального архивного фонда; создание и ведение автоматизированного научно-справочного аппарата; формирование тематических архивных ресурсов и организация доступа к ним; возможности применения интернет-технологий; создание электронных архивов и решение проблемы приема на постоянное хранение электронных документов; проблемы обеспечения сохранности архивных документов (в том числе с помощью применения информационных технологий оцифровки, компьютерной реставрации и создания электронных фондов пользования).

В 1998 году в БелНИЦЭД был создан отдел автоматизации архивных технологий. Отдел разработал 12 прикладных информационных систем, подготовлены методические рекомендации по созданию и использованию информационных технологий в архивном деле, а также Концепция информатизации архивной отрасли Республики Беларусь.

В 2000 году был создан первый специализированный архив, который обеспечивал сохранности электронных документов. Основными объектами его комплектования стали архивные копии информационных ресурсов (баз данных и интернет-сайтов). Управление архивом обеспечивает автоматизированная информационная система архива электронных документов (АИС архива ЭД), разработанная по заказу архивной службы республиканским унитарным предприятием «Агат-Систем» [75]

Параллельно велось создание нормативно-методической базы, позволяющей передавать на хранение документированной информации, созданной в электронной форме в государственные учреждения.

На развитие информатизации архивной отрасли и научных исследований повлияла Государственная программа информатизации Республики Беларусь на 2003-2005 годы и на перспективу до 2010 года «Электронная Беларусь», утвержденная постановлением Совета Министров Республики Беларусь 27 декабря 2002 г. № 1819, основное внимание в которой было сосредоточено на управлении данными, в информационных системах, а также применению

электронных документов, обеспечению сохранности электронных документов, передаваемых на государственное хранение. [29]

В 2002 г. функции по разработке программного обеспечения для нужд отрасли были переданы БелНИЦЭД. Важным этапом стало принятие в 2005 г. Стратегии автоматизации архивной отрасли на ближайшую перспективу/ [75] Рассчитанная на период до 2010 г. включительно, она предусматривала создание типовой информационной системы – АИС архива, автоматизирующей все основные виды деятельности архивистов. Сейчас эта система введена в эксплуатацию практически во всех государственных архивах (5 центральных и 25 областных и зональных). Продолжается ее совершенствование, создаются новые версии некоторых модулей.

В БелНИЦЭД занимаются вопросами создания цифровых копий бумажных документов, научно-справочного аппарата к ним, а также обеспечения доступа к архивной информации посредством интернет-технологий.

Первые попытки сканирования архивных документов начались в Беларуси в середине 1990-х гг. Поучительным оказался опыт создания цифровых копий документов партизанского движения, хранящихся в ГУ «Национальный архив Республики Беларусь». [75] При отборе документов для оцифровки, выборе разрешения графических файлов, создании описательных метаданных был допущен ряд методологических просчетов. В результате созданные копии практически не использовались.

В 2001 г. БелНИЦЭД разработал Концепцию цифрового копирования документов Национального архивного фонда. [75] В ней были проанализированы основные вопросы, связанные с созданием цифровых копий, хранящихся в государственных архивах бумажных документов, их хранением и использованием, изучен международный опыт, а также имевшийся к тому времени опыт оцифровывания документов в белорусских архивах. С выводами, содержащимися в Концепции, были ознакомлены все архивы, в некоторых из них состоялось ее широкое обсуждение. Это позволило архивистам ознакомиться со специфической терминологией и уяснить основной круг проблем, связанных с предстоящей задачей, психологически подготовиться к ее решению.

В архивной отрасли Беларуси активно внедряются современные информационные технологии, включая оцифровку документов и предоставление онлайн-доступа к архивной информации в Интернете.

Информационное пространство рассматривается как один из видов общения и представляет собой социально обусловленное явление с основной функцией — воздействие через смысловую и оценочную информацию при помощи различных коммуникативных каналов. Современное общество выработало ряд технических средств, обеспечивающих возможность

Примечание [L1]: Номер ссылки и в список!!!

Примечание [L2]: Номер ссылки и в список!!!

Примечание [L3]: Номер ссылки и в список!!!

коммуникации. Во-первых — это средство массовой информации (периодическая печать, радио, телевидение и тд.). Во-вторых — средства массового воздействия (кино, театр, литература и тд.). Они не отличаются регулярностью коммуникации, по сравнению со средствами массовой информации, из-за меньшего охвата территории. В-третьих — технические средства коммуникации (телефон, радиоаппаратура и т.д.). Данные технические средства раньше не имели массового охвата территории, но с развитием современного общества и использования на сегодняшний день новейших информационных технологий захватили весь мир

В совместной работе Е.М. Гришанова, Я.С. Артамонова, И.А. Чиликин «Информационная безопасность и информационные коммуникации» выделяют четыре информационные революции, определяющие возникновение и развитие информационной безопасности общества. [31]

Изобретение письменности ознаменовало начало первой информационной революции. Начиная с этого периода, появляется возможность фиксации и передачи знаний на материальном носителе от поколения к поколению.

Вторая информационная революция (середина XVI в.) обусловлена изобретением книгопечатания, которое существенно повлияло на культуру и организацию деятельности. С этого времени появляется активная возможность не только распространения информации, но и ее копирование.

В конце XIX в. произошла третья информационная революция. Она связана с изобретением электричества, благодаря которому появились телеграф, телефон, и, наконец, радио. Все эти устройства позволяют эффективно передавать на большие расстояния информацию, а также содействует ее накоплению.

В 70-е годы XX в. наступила четвертая информационная революция. Она связана с изобретением микропроцессорной технологии и появлением персонального компьютера, компьютерных сетей, систем передачи данных (так называемых информационных коммуникаций). Произошел переход от механических и электрических средств преобразования информации к электронным.

Выделение четырех информационных революций позволяет предположить, что от уровня развития общества зависит его информационная безопасность, которая определяется объемом и доступностью к информации, а также возможностью ее непосредственного использования.

Возникновение первого этапа условно можно обозначить, начиная с древнейших времен, становления и развития человеческой цивилизации и до 1816 г. Он характеризуется использованием так называемых "естественно возникавших средств информационных коммуникаций". Основная задача информационной безопасности в этот период заключалась в защите сведений о

событиях, фактах, имуществе, местонахождении и других данных, имевших важное значение для общества или лично для человека.

Второй этап охватывает период с 1816 г. и длился по 1935 г. Он связан с началом использования искусственно создаваемых технических средств электросвязи и радиосвязи. Так, например, в 1866 г. американский дантист Махлон Лумис (Mahlon Loomis) заявил о том, что открыл способ беспроволочной связи; в 1879 г. — Дэвид Хьюз при работе с индукционной катушкой обнаружил эффект электромагнитных волн (однако позднее коллеги убедили его, что речь идёт лишь об индукции). В 1888 г. — немецкий физик Г. Герц доказал существование электромагнитных волн. В 1891 г. Никола Тесла (Сент-Луис, штат Миссури, США) описал принципы передачи радиосигнала на большие расстояния. Бразильский священник и учёный Роберто Ланделл де Мора с 1893 по 1894 гг. проводил эксперименты по передаче радиосигнала, данные результаты он не оглашал до 1900 г., но впоследствии получил бразильский патент. На заседании Русского физико-химического общества в Санкт-Петербурге 7 мая 1895 г. Александр Степанович Попов прочитал лекцию «Об отношении металлических порошков к электрическим колебаниям», а в 1898 г. Русское Техническое Общество присудило А.С. Попову премию за изобретение приемника электромагнитных колебаний и приборов для телеграфирования без использования проводов и т.д.

Данный период информационной безопасности базировался на достижениях первого периода и достижений конкретно взятого в историческом аспекте второго периода в области информационной безопасности на более высоком технологическом уровне, а именно — применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения.

Третий этап (1935-1946 гг.) связан с появлением радиолокационных и гидроакустических средств. В качестве основного способа обеспечения информационной безопасности в этот период было сочетание технических и организационных мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

Четвертый этап (1946-1965 гг.) обусловлен изобретением и развитием в практической деятельности электронно-вычислительных машин, компьютеров. Задачи информационной безопасности в этот период решались, в основном, методами и способами, направленными на ограничение физического доступа к оборудованию средств получения, обработки и передачи информации.

Пятый этап (1965-1973 гг.) связан с созданием и внедрением локальных информационно-коммуникационных сетей. В 1969 г. Министерство обороны

США посчитало, что на случай войны стране нужна надёжная система передачи информации. Агентство передовых исследовательских проектов (ARPA) предложило разработать для этого компьютерную сеть. Разработка сети была поручена четырем научным учреждениям: Калифорнийскому университету в Лос-Анджелесе, Стэндфордскому исследовательскому центру, Университету штата Юта и Университету штата Калифорния в Санта-Барбаре. В 1969 г. на линии вышла компьютерная сеть под названием ARPANET (от англ. Advanced Research Projects Agency Network). В рамках проекта сеть объединила четыре указанных научных учреждения, была открыта для исследовательских центров, сотрудничавших с Министерством обороны США. Все работы финансировались за счет Министерства обороны США.

В 1973 году к сети были подключены первые иностранные организации из Великобритании и Норвегии через трансатлантический телефонный кабель, с этого момента сеть стала международной.

Основные задачи информационной безопасности для пятого этапа сводились в большинстве случаев к методам и способам физической защиты средств получения, переработки и передачи информации, объединенных в локальную сеть путем администрирования и управления доступом к сетевым ресурсам. [53 с.327]

Шестой этап (1973-1985 гг.) связан с использованием сверхмобильных и коммуникационных устройств с широким спектром задач. В 1983 г. сеть ARPANET (от англ. Advanced Research Projects Agency Network) раскололась на ARPANET, посвященную научным исследованиям и MILNET (от англ. Military Network), ориентированную на военное применение. В этот период произошло подключение Национального научного фонда к созданию другой научной сети — NSFNet (от англ. National Science Foundation Network) и в сотрудничестве с International Business Machines еще одной сети для специалистов в социальных и гуманитарных науках – Because It’s Time (далее – BITNET). Все эти сети использовали ARPANET как коммуникационную систему. В 1980-х годах сформировалась сеть сетей, названная ARPAINTERNET, а затем и просто INTERNET. В этот период она работала в рамках Национального научного фонда и по-прежнему финансировалась Министерством обороны США. Угрозы информационной безопасности стали гораздо серьезнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Однако, параллельно с попытками Пентагона и большой науки в США возникла и начала распространяться компьютерная контркультура. Важным элементом этой системы были люди, являющиеся пионерами этой культуры. Образовалось сообщество людей — хакеров (хакер, от англ. hack — разрубать). Этим термином обозначают компьютерных специалистов особого

типа, так называемых компьютерных преступников, осуществляющих неправомерный доступ к компьютерам и информации, основной целью которых было и есть нанесение ущерба информационной безопасности, как отдельных пользователей, так и организаций. Постепенно информационный ресурс становится важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности социума (государства). По мнению ряда, ученых: М.А. Лапина, А.Д. Ревина, И.Л. Бачило, Н.Н. Ковалева, в этот период формируется информационное право — новая отрасль международной правовой системы. [18]

Седьмой этап начинается с 1985 г. Он связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств снабжения. Очередной этап развития информационной безопасности, возможно, может быть связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. [18]

Таким образом, в рамках этой классификации возникновение и развитие информационной безопасности связано в первую очередь с появлением и развитием технических средств в истории развития человеческой цивилизации. Именно технический прогресс определяет каждый новый шаг развития информационной безопасности общества. В этом случае главный упор в понимании понятия информационная безопасность переносится в первую очередь на состояние защищенности информационной среды, на защиту информации в техническом аспекте (технических систем, используемых для сбора, обработки и распределения информации) и представляет собой деятельность по предотвращению утечки защищаемой информации, от несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Данная работа написана на основе анализа работ таких ученых и специалистов, занимающихся проблематикой информатизации архивного дела и документационного обеспечения управления: В.И. Тихонова, В.Л. Носевич В.М. Ларина, В.Н. Гармаш, Л.Л. Левченко, М.Н. Костомарова, О.А. Михайлова, О.И. Рыскова, О.Ю. Жук, Т.С. Кабочкиной. [108, 74 – 77, 116, 58, 25, 98, 38 – 40, 67, 108, 62] В области права, таких как И.Л. Бачило, С.В. Лазовский, В.Н. Лопатин и др. [18, 61], в области информационной безопасности: Б. Исабаев, А.К. Нурпеисова, М.С. Соколов, В.М. Арсентьев, В.И. Байков, А.В. Дорофеев, А.А. Марков и др. [102, 35, 36]. Вопросы теоретических и прикладных проблемы информационной безопасности, затрагивают работы таких авторов,

как В.Н. Лопатин, М.С. Соколов, О.А. Городов, В.И. Ярочкин, В.А. Галатенко, В.К. Левин, А.Н. Асаул. [18, 102, 28]

Среди Российских исследований по информатизации архивного дела и документационного обеспечения управления интересны работы В.М. Ларина [116], занимающегося разработкой основных принципов и подходов к управлению документацией в России. Отдельные исследования В.М. Ларина посвящены также изучению западного и, в частности, американского опыта управления документацией. Достаточно актуальны теоретические изыскания Тихонова В.И., в которых собраны рекомендации по обеспечению сохранности электронных документов. [108]

Также интересна работ украинской исследовательницы Л.Л. Левченко по проблемам управления документацией в США «Обеспечение сохранности электронных документов в Национальном архиве Соединенных Штатов Америки». В данном исследовании Л.Л. Левченко изучает нормативно-правовую база американской системы управления документацией, принципов работы с электронными документами. [62]

Крупный вклад в развитие теории и практики работы с документами в электронном виде и обеспечение их защиты при архивном хранении озвучены в работах Белорусских исследователи В.Л. Носевича и О.Ю. Жук.

В.Л. Носевич изучает основные направления деятельности белорусских архивов по внедрению современных информационных технологий, организация работы с документами в электронном виде в архивах. [74 –77]

В работах О.Ю. Жук представлена информация о проблемах информационной безопасности организации, которая внедряет систему электронного документооборота (далее – СЭД), рассмотрены уровни СЭД, которые необходимо защищать, а также определены основные способы и механизмы обеспечения защиты электронных документов при архивном хранении. [38 – 40]

В работах И.Л. Бачило «Информационное право», М.С. Соколова «Информационная безопасность. К вопросу о содержании понятия информационная безопасность», С.В. Лазовского «Понятие информационной безопасности государства и ее место в правовой системе Республики Беларусь» уделяется внимание термину информационная безопасность, который остается не определенным ни в науке, ни в законодательстве. Существуют его различные трактовки, но единого подхода нет. [18, 102, 63, 105]

В работах Dirk Proske «Catalogue of Risks – Natural, Technical, Social and Health», А.А. Маркова «Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе» рассматривт понятие информационного риска и его концепции. Проблемы защиты и

страхования от информационных рисков рассматриваются в практике компании «ИнфоОборона» и ОСАО «Ингосстрах». [3, 65]

Информационный риск может стать причиной появления информационной опасности – угрозы. Понятие угрозы рассматриваются в таких работах авторах как: А.А. Марков «Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе», В.В. Барабин «Военно-политическая деятельность государства в системе национальной безопасности», Н.П. Ващекин «Безопасность и устойчивое развитие России» и др. [63, 17, 21]

Анализ рассматриваемой литературы по данной теме свидетельствует, что информационные угрозы представляют в общем понятийном смысле ту категорию, которая прямо влияет на информационную безопасность. В определение «информационная угроза» многими авторами вкладывается и суть определений «информационная опасность» и «информационный риск», и отдельно ими не рассматривается, для упрощения общей конструкции, либо по причине относительной малозначительности воздействия на информационную безопасность.

Но на сегодняшний день недостаточно ограничиться характеристикой информационных угроз. Следует квалифицировать все эти определения, и в дальнейшем, по мере совершенствования информационного общества и его информационной безопасности, эти определения должны стать самостоятельными понятиями и будут анализироваться как самостоятельные категории.

Классификация угроз может быть различной, и рассматривалась авторами в работах: В.Ю. Гайкович, Д.В. Ершов «Основы безопасности информационных технологий» [23], Ю.В. Романец, П.А. Тимофеев «Защита информации в компьютерных системах и сетях» [96], А.А. Тепляков, И.В Гваева, А.В. Орлов «Обеспечение безопасности и надежности информационных систем» [106], Дж. Уолрэнд «Телекоммуникационные и компьютерные сети» [111], А.В. Дорофеев, А.С. Марков «Менеджмент информационной безопасности: основные концепции». [35] Довольно подробные каталоги угроз подготовлены немецким федеральным агентством по информационной безопасности «IT-Grundschutz Catalogues. Bundesamt für Sicherheit in der Informationstechnik». [13]

Одной из основных угроз информационной безопасности, является возможность реализации различных уязвимостей в ресурсах информационных систем. Подход уязвимостей в системе управления информационной безопасности рассмотрен автором А.В. Кубаревым в работе «Подход к формализации уязвимостей информационных систем на основе их классификационных признаков». [59]

Автор в своей работе отмечает, что возможность реализации уязвимости в ресурсах информационных систем, является одной из основных угроз ИБ в них. По его словам, под уязвимостью понимают связанный с ним дефект («слабость»), снижающий уровень защищенности ресурсов от тех или иных угроз. Отмечено, наличие уязвимости становится угрозой, если ее можно реализовать так, что это приведет к недопустимому ущербу организации. Например, наличие сетевых уязвимостей в программном обеспечении изолированного компьютера не является угрозой. [61]

Статья В.А. Матвеева, Н.В. Медведева, И.И. Троицкого, В.Л. Цирлова, посвящена вопросам создания и организации деятельности системы управления информационной безопасности (ISMS) (от англ. information security management system), подходам к бизнес-рискам, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности. В рамках СУИБ авторы рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы. [103]

Методам управления и оценки рисков в информационной безопасности посвящено исследование А.С. Маркова и А.С. Цирлова «Управление рисками – нормативный вакуум информационной безопасности» [65], где сформулированы три варианта обработки рисков. Авторы рассматривают отдельные методологии по управлению и оценке рисков для различных типовых случаев, таких как методы: CORAS, CRAMM (от англ. the UK Goverment Risk Analysis and Managment Method), OCTAVE (от англ. Operationally Critical Threat, Asset, and Vulnerability Evaluation).

Более подробно методам управления и оценки рисков CORAS, CRAMM, OCTAVE посвящены исследования таких авторов: A.G. Bjorn «CORAS, A Platform for Risk Analysis on Security Critical Systems – Model-based Risk Analysis Targeting Security» [1], И. Д. Медведовский «Современные методы и средства анализа и контроля рисков информационных систем компаний» [66], А. Пастоев «Методологии управления информационными технологиями – рисками» [92], С.В. Разумников «Анализ возможности применения методов OCTAVE, RiskWatch, CRAMM для оценки рисков информационных технологии и для облачных сервисов» [95], Г.Н. Ермошкин «Анализ существующих моделей оценки рисков ИБ для частных облачных сред» [37], Е. Нестеркина «Методы реализации стандартной стратегии рисков облачных вычислений» [71], так и остальные авторы, склонен считать что, до принятия решения о внедрении того или иного метода управления рисками следует убедиться, что он достаточно полно учитывает бизнес-потребности организации, ее масштабы, а также соответствует лучшим мировым практикам и имеет достаточно подробное описание процессов и требуемых действий. В своей работе Е. Нестеркина [71] излагает, что рассмотренные методы не

предполагают расчета оптимального баланса различных способов управления, не имеют средств интеграции способов управления и не дают механизмов управления рисками остаточного уровня. Так же во всех трех методологиях не производится оценка качества процесса реагирования на инциденты в области информационной безопасности.

Примечание [L4]: Разнесите ссылки, поставьте за авторами!

Вопросами минимизации выявленных рисков путем внедрения контролей (механизмов), структуры документации системы управления безопасности посвящены работы авторов: А.В. Дорофеева и А.С. Маркова «Менеджмент информационной безопасности: основные концепции», И.Ю. Шахалова «Основы управления информационной безопасностью современной организации» [35, 36].

Обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал. Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Анализ литературы показал, что в Республике Беларусь и за рубежом недостаточно научно обоснованных концепций и моделей менеджмента информационной безопасности. Современная наука о менеджменте организации и отдельных ее областей не дает аргументированных, рекомендаций по решению проблем в указанном контексте. И связано это, в первую очередь, с тем, что нормирование отдельных областей реализуется, как правило, не в единой системе и, как следствие, не взаимосвязано. А для того, чтобы интегрированная система работала эффективно, все ее составляющие должны быть разработаны на базе единого принципа управления. В качестве такой основы и используются международные стандарты Международной организации по стандартизации (от англ. International Organization for Standardization, далее – ISO).

В данный момент в науке утвердились следующие методологические подходы к вопросу о возникновении и развитии информационной безопасности в обществе. Ряд из них связывает основные этапы развития информационного пространства, совпадающие с информационными революциями, а также с проблемой возникновения и развития информационной безопасности в истории человеческой цивилизации.

В рамках первого методологического подхода выделяют следующие основные концепции. Первая концепция, объединяет становление

информационного пространства с возникновением и развитием информационной безопасности общества. Данная концепция представлена в книге Д.С. Робертсона "Информационная революция", в которой ученый выделяет четыре определяющие революции: изобретение языка; письменность; книгопечатание; создание электронно-вычислительной машины (далее – ЭВМ). [14]

По мнению Я.С. Артамонова третий методологический подход, возникновение категории информационная безопасность, обусловлен, в первую очередь, появлением в истории развития человеческой цивилизации двух основных феноменов. Первый – это появление средств информационных коммуникаций между людьми, второй феномен – осознание человеком наличия "своих" и альтернативных социальных систем (человеческих обществах, государств и тд.) определенных интересов, которым может быть нанесен ущерб путем воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между различными элементами общества. Исходя из этого, можно выделить несколько этапов в развитии средств информационных коммуникаций [18].

Информационная безопасность государства предполагает такое состояние, при котором обеспечивается сохранность информационных ресурсов государства и защищенность законных прав личности и общества в информационной сфере. [22, с. 121]

В коллективном труде М.В. Мясниковича и Л.С. Мальцева, понятие информационная безопасность многогранно и комплексно. Оно имеет два основных аспекта: содержательный и технический. К первому относится содержание и направленность всей циркулирующей информации. Ко второму относится совокупность информационно-телекоммуникационных средств, технологий, систем, ресурсов, предназначенных для создания, хранения, распространения, передачи и обработки информации. [70, с. 207]

Определяя содержание понятия «информационная безопасность» некоторые авторы, например, А.Н. Асаул, понимают этот термин, как набор аппаратных и программных средств, для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях. Другие авторы, например, В.И. Ярочкин, уравнивают два разных понятия – «защита информации» и «информационная безопасность». Авторы В.А. Галатенко, В.К. Левин, под безопасностью в информационной сфере понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. [18, с. 590, с. 591]

О.А. Городов, считает, что дальнейшее развитие понятия информационной безопасности будет происходить в заданном доктриной направлении, но возникает проблема, которая требует ответа на вопрос, состоящий в определении баланса интересов отдельной личности и общества в целом. Ведь то, что отвечает интересам отдельного индивида, не всегда отвечает интересам общества в целом; и наоборот, то, что соответствует интересам всего общества, может явно противоречить интересу отдельного индивида. [28, с. 209-210]

М.С. Соколов критикуя отдельные стороны данного определения пришел к следующему выводу, что информационная безопасность Российской Федерации – это состояние защищенности информационной сферы, при котором невозможна реализация известных угроз в отношении информации, информационной инфраструктуры, субъектов и системы регулирования информационных отношений. [102, с. 10, с.14]

В работе «Основы управления информационной безопасностью современной организации» Шахалов, И.Ю., Дорофеев А.В. считают, что доступность обеспечивает возможность использования информации тогда, когда это необходимо. Потеря доступности выражается в нарушении доступа к информации, невозможности ее использования. [36]

Подводя итоги нужно отметить, что имеется огромной комплекс научных трудов в сфере информационной безопасности. Многими учеными предлагаются различные меры по совершенствованию данной сферы. Выдвигаются идеи о выделении информационной безопасности в качестве подотрасли информационного права. На взгляд автора данного исследования, данные предложения являются оправданными.

Ознакомившись с исследованиями по данной теме, можно сделать вывод о том, что большинство авторов стремятся показать важность и необходимость создание в каждой организации эффективной системы управления информационной безопасности, и дальнейшее ее внедрение в интегрированную систему менеджмента.

Ведутся работы по научно-методологическому обеспечению, и совершенствования понятийного аппарата в сфере информационной безопасности. Понятие информационная безопасность является базовым, поскольку ее сущность определяет в конечном итоге политику и деятельность в сфере защиты информации. В то же время эти понятия взаимосвязаны и взаимообусловлены. Между тем и в нормативных документах, и в научной литературе нет единых подходов к определению данных понятий, а, следовательно, и к раскрытию их сущности, ибо определения должны в концентрированном виде выражать сущность понятий. В первую очередь это относится к понятию защита информации, где различие мнений исследователей

в толковании понятия наиболее значительно. При этом различия касаются как содержательной части понятия, так и способа ее реализации.

Из рассмотренного становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Анализ литературы показал, что в Республике Беларусь недостаточно уделено внимание проблеме внедрения СУИБ в организациях, научно-методологическому, нормативно-правовому и документационному обеспечению по защите информации.

1.3. Методы исследования

Работа над магистерской диссертацией велась с соблюдением принципов историзма, объективности, системности и целостности. Применялись общенаучные, общелогичес кие и частнонаучные методы исследования.

Использовались такие общенаучные методы как, системный анализ и синтез для изучения информационно-правовой природы информационной безопасности. Автору потребовалось провести анализ законодательства в сфере информационной безопасности Республики Беларусь, выделить особенности общественных отношений в этой сфере, и с учетом этих особенностей, предложить меры по совершенствованию законодательства для решения возникающих сегодня проблем, таких как преобразования документов из электронной в бумажную форму с сохранением их юридической силы.

Метод сравнительного анализа использовался для установления различий и сходств законодательства в сфере информационной безопасности Республики Беларусь и Российской Федерации, для последующей разработки и совершенствования документационного обеспечения СУИБ.

Из частнонаучных методов в исследовании использовались метод статистического анализа для описания количества инцидентов информационной безопасности с документируемой информации, подлежащей защите.

Метод классификации рисков и угроз документируемой информации, подлежащей защите. Проектно-графическое моделирование для отображения процесса управление документацией в СУИБ, взаимодействие участников между собой с помощью документов.

ГЛАВА 2. МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ АРХИВЕ ОРГАНИЗАЦИИ

2.1 Определение понятий информационная безопастность, актив, угроза, уязвимость, контроль и риск

Проблема защиты информации является многоплановой и комплексной. Вопросу безопасности в информационной сфере, уделяется внимание на государственном и частном уровнях. Залогом успеха является хорошее понимание концепции СУИБ в организации. Но прежде всего, следует разобраться, что стоит за такими понятиями как информационная безопастность, актив, угроза, уязвимость, контроль и риск.

Термин информационная безопасность остается не определенным ни в науке, ни в законодательстве. [105] Существуют его различные трактовки, но единого подхода нет.

В соответствии с Концепцией национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. [88]

Согласно Постановлению Правления Национального Банка Республики Беларусь от 30 ноября 2012 г. № 625 информационная безопасность – многоуровневый комплекс организационных мер, аппаратно-программных и технических средств, обеспечивающих защиту от случайных и преднамеренных угроз, в результате реализации которых возможно нарушение свойств доступности, целостности, подлинности или конфиденциальности обрабатываемой, хранящейся или передаваемой информации. [87]

В Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. информационная безопасность определяется как состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве. [101]

В доктрине информационной безопасности Российской Федерации под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, которые определяются совокупностью сбалансированных интересов личности, общества и государства. [33]

Понятие Информационная безопасность многогранно и комплексно. Оно имеет два основных аспекта: содержательный и технический. К первому относится содержание и направленность всей циркулирующей информации. Ко

второму относится совокупность информационно-телекоммуникационных средств, технологий, систем, ресурсов, предназначенных для создания, хранения, распространения, передачи и обработки информации. [70]

Само понятие «информационная безопасность» можно трактовать про разному, например, как набор аппаратных и программных средств, для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях.

Исходя из выше изложенного, понятие информационная безопасность можно рассматривать как состояние и как деятельность. Если понятие рассматривать как состояние, то качеством объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т.п. А если как деятельность, направленная на обеспечение защищённого состояния объекта, то в этом значении, чаще используется термин «защита информации».

В данной работе информационная безопасность рассматривается как деятельность, так как мы рассматриваем комплекс мер в менеджменте информационной безопасности, которые были закреплены в стандартах информационной безопасности.

Определяющими факторами информационной безопасности являются риск и угроза.

Риск, как понятие, представляет собой возникновение ситуации, характеризующейся неопределенностью результата, вероятным или обязательным наличием неблагоприятных последствий. В.В. Глушенко определяет риск, как действующий/развивающийся фактор процесса, обладающий потенциалом негативного влияния на ход процесса. [27]

Существует достаточное количество определений риска, которые могут быть воспроизведены в различных ситуационных контекстах и различными особенностями применений. Мера риска в определенном смысле пропорциональна как ожидаемым потерям, которые могут быть причинены рисковым событием, так и вероятности этого события. Различия в определениях риска зависят от величины потерь, их оценки и измерения. Если потери оказываются фиксированными, оценка риска фокусируется только на вероятности события, возможных его последствий и связанных с ними обстоятельств. Можно выделить две разновидности риска: теоретический риск и эффективный риск. Эти две точки зрения непрерывно конфликтуют в социальных, гуманитарных и политических науках. В последние годы в связи с появлением нового направления теории вероятностей – эвентологии, возникло понятие эвентологического риска, которое можно рассматривать как первую

серьезную попытку объединить в одном понятии и теоретический, и эффективный риск. [3]

В информационной безопасности риск определяется как функция трех переменных величин:

- вероятность существования информационной угрозы;
- вероятность существования незащищенности;
- потенциальное воздействие.

Если любая из этих переменных приближается к нулю, то и полный риск приближается к нулю. На наш взгляд, информационный риск представляет собой определенные и осознанные действия субъекта в информационной сфере, предполагающие возникновение возможных негативных последствий. [64] Примером таких рисков может служить: PR-компания/ PR-акция, реклама, информационная война в отношении конкурента, внесение в адресные базы важных конфиденциальных данных, работа с новыми, мало проверенными техническими средствами, и т. д. Заложенные в таком случае информационные риски предполагают наличие осознанности своих действий субъектом, который осознает вероятность возникновения негативных последствий. В настоящее время информационные риски уже являются не только предметом изучения, но и защиты, в том числе страховой. Например, с развитием ИТ, услуга по страхованию информационных рисков становится востребованной и в Республики Беларусь и в других странах СНГ. Первой конкретной страховой программой стал совместный проект компании «ИнфоОборона» и ОСАО «Ингосстрах». [56]

Таким образом, информационный риск является проявлением и следствием добровольной и осознанной деятельности самого субъекта в информационной сфере.

Угрозой называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень информационной безопасности системы, т.е. потенциально способную привести к негативным последствиям и ущербу системы или организации.

Само понятие «угроза» не имеет четкого единого определения и многими авторами трактуется по-разному. Например, угроза определятся как «высказанное в любой форме намерение нанести физический, материальный иди иной вред общественным и личным интересам». [99] Ряд авторов считают, что угроза – это «совокупность факторов и условий, представляющих опасность жизненно важным интересам личности, общества и государства». [21]

Другие считают, что угроза – это «наиболее конкретная и непосредственная форма опасности, создаваемая целенаправленной деятельностью откровенно враждебных сил». [19]

В.В. Барабин представляет угрозу как актуализированную форму опасности в процессе ее превращения из возможности в действительность, субъективированную готовность одних людей причинить ущерб другим. [17]

Последняя позиция нам представляется наиболее убедительным определением понятия угрозы. На наш взгляд, если мы рассматриваем опасность как побуждение к действию, то, собственно говоря, угроза означает непосредственную готовность осуществления такой опасности. Здесь важно понять грань между терминами «намерение» и «готовность». Образно говоря, угрозу можно охарактеризовать как последнее предупреждение, за которым и последует само действие.

Информационная угроза, по сути, представляет собой умысел с целью намеренного нанесения вреда субъекту информационной сферы. В отличие от информационного риска и частично информационной опасности, информационная угроза направлена против интересов субъекта в данной сфере. А учитывая нынешнее развитие информационно-коммуникационных технологий и информационных ресурсов, можно утверждать, что информационные угрозы способны не только воздействовать на информационную безопасность, но также в тех или иных параметрах оказывать деструктивное влияние на национальную, экономическую, экологическую, социальную и ряд других видов безопасности.

Таким образом, квалифицируя исследованные выше информационные риски, опасности и угрозы, можно сделать вывод: информационные риски и отчасти информационные опасности (без наличия умысла) представляют собой потенциально вредные намерения и действия, способные нанести определенный ущерб субъектам информационной сферы. Информационные угрозы являют реальную готовность нанесения вреда и желание наступления негативных последствий для субъектов информационной сферы. При этом следует уточнить: информационные риски и опасности могут стать причиной появления информационной угрозы безотносительно того, умышленны они или нет.

2.2 Угрозы информационной безопасности электронного архива

Очевидно, что именно информационные угрозы представляют наибольшую проблему в обеспечении информационной безопасности субъекта, так как содержат в себе качественные квалифицирующие признаки повышенной потенциальной и реальной деструкции. В то же время анализ имеющейся литературы по данной теме свидетельствует, что лишь информационные угрозы представляют в общем понятийном смысле ту категорию, которая прямо влияет на информационную безопасность. В определение «информационная угроза» многими авторами вкладывается и суть определений «информационная опасность» и «информационный риск», но отдельно ими не рассматривается, чтобы не усложнять общую конструкцию, либо по причине относительной малозначительности воздействия на информационную безопасность. Таким образом, А.А. Марков полагает, что эти определения станут самостоятельными понятиями и будут анализироваться как самостоятельные категории. На сегодняшний день достаточно ограничиться характеристикой информационных угроз. [64]

Классификация угроз может быть различной. Так, исследователи В.Ю. Гайкович и Д.В. Ершов все множество потенциальных угроз по природе их возникновения разделяют на два класса [23]:

- естественные угрозы – угрозы, вызванные воздействиями на КИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека;
- искусственные угрозы – угрозы, вызванные деятельностью человека.

Среди них, исходя из мотивации действий, выделяют:

a) непреднамеренные (случайные) угрозы, вызванные ошибками в проектировании системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала;
b) преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей.

По целям, преследуемым злоумышленником (Ю.В. Романец, П.А. Тимофеев) [69]:

- угрозы конфиденциальности данных и программ;
- угрозы целостности данных, программ, аппаратуры;
- угрозы доступности данных;
- угрозы отказа от выполнения действий.

Относительно объекта защиты (классификация А.А. Теплякова) [106]:

- внешние;
- внутренние.

На основе объектов информационных систем, на которые направлены угрозы (Дж. Уорленд) [111]:

- угрозы компьютерам или серверам;
  a) физическое вмешательство;
  b) заражение вредоносными программами (вирусы);
  c) несанкционированное внедрение в систему.
- угрозы пользователям;
  a) подмена персоналий;
  b) нарушение приватности;
- угрозы электронным документам:

a) нарушение целостности документа;

b) искажение аутентичности отправителя документа (незаконное присвоение идентификатора, повторная передача сообщения, искажение реквизитов документа);

c) непризнание участия (отказ от факта формирования документа, от получения информации или заявление ложных сведений о времени ее получения, утверждение, что получателю в определенное время была послана информация, которая на самом деле не посылалась или посылалась в другое время).

А.В. Дорофеев и А.С. Марков классифицирует угрозы по ряду критериев [35]:

- по причине возникновения (природные или техногенные, в том числе преднамеренные или случайные);
- по расположению источника (внешние или внутренние);
- по компрометируемой подсистеме или сегменту (сетевые, криптографические и др.);
- по этапу формирования в жизненном цикле системы (реализационные и эксплуатационные);
- по результирующему действию (нарушают целостность, конфиденциальность, доступность).

Одной из основных угроз ИБ для элкутронных архивах, это возможность реализации уязвимости в системе. Под уязвимостью понимают реализационный дефект («слабость»), снижающий уровень защищенности системы от тех или иных угроз. [59]

Защищенность электронного архива достигается обеспечением совокупности свойств ИБ: конфиденциальность, целостность, доступность.

Конфиденциальность – необходимость предотвращения утечки какой-либо информации. Конфиденциальность гарантирует, что только уполномоченный персонал может получить доступ к информации. Чаще всего такой информацией может, является служебная тайна или «ноу-хау». [86] Так же, это

свойство системы, определяющее ее защищенность от несанкционированного раскрытия информации.

Термин целостность информации в информатике и теории телекоммуникаций, означает, что данные полны и защиты от несанкционированного изменения или повреждения информации, или обеспечение сохранности информации в том виде, в котором она была создана автором. Потеря целостности означает несанкционированное изменение или повреждение информации. [49] Целостность рассматривают как, свойство определяющее защищенность от несанкционированного изменения.

Доступность обеспечивает возможность использования информации тогда, когда это необходимо. Потеря доступности выражается в нарушении доступа к информации, невозможности ее использования. [36] С доступностью часто связывают такую характеристику системы как готовность – способность к выполнению заявленных функций в установленных технических условиях.

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности электронных документов осуществляется путем применения мер (механизмов) безопасности.

Механизмы могут иметь технический, организационный и физический характер. Под понятие «технические механизмы» подпадают программные и программно-аппаратные средства защиты, такие как антивирусы, межсетевые экраны, системы обнаружения вторжений, средства шифрования данных и т. п. В качестве «организационных механизмов» выступают правила, обязательные для исполнения сотрудниками. Механизмы могут придерживаться различных целей, например, быть превентивными, детективными, корректирующими, восстанавливающими и другими. Применение различных видов и типов «механизмов» тесно связано с концепцией эшелонированной обороны, представляющей идеологию проектирования систем защиты с несколькими уровнями «механизмов» безопасности, позволяющими обеспечить эффективную защиту даже в случае «пробивания» обороны на одном уровне.

2.3 Методы оценки рисков информационной безопасности в организации

Система управления информационной безопасности (СУИБ, ISMS) организации основывается на подходе бизнес-риска и предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ. В рамках СУИБ рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Концепция СУИБ определяется в международном стандарте ISO/IEC 27001. В предыдущих редакциях стандарта требования к СУИБ были довольно явно сопоставлены с элементами модели Шухарта-Деминга «Планирование (Plan) – Реализация (Do) – Проверка (Check) – Совершенствование (Act)» (PDCA). [50] По сути, цикл PDCA отражает руководство здравым смыслом при внедрении какого-либо процесса: прежде чем что-нибудь сделать мы планируем, затем это выполняем, после чего контролируем, что то сделали, соответствует тому, что хотели, а выявленные недостатки и отклонения устраняем. Из новой версии стандарта, вышедшей в 2013-м году, данная модель изъята, чтобы не ограничивать организации в выборе концепций управления процессами. [103]

Стандарт ISO 27001:2013 содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности.

В первую очередь необходимо определить контекст, в котором работает организация и четко понимать потребности и ожидания всех сторон, заинтересованных в функционирующей системе управления информационной безопасностью.

Важно, что стандарт дает возможность внедрить СУИБ «вокруг» определенных критичных бизнес-процессов, а затем уже при необходимости расширять область действия СУИБ на другие процессы.

Внедрение СУИБ невозможно без реальной поддержки со стороны топменеджмента организации, определяющего четкую политику информационной безопасности, включающую цели и обязательства выполнять все применимые требования (законодательства, партнеров, клиентов и т.п.).

На этапе планирования внедрения СУИБ в первую очередь формализуется процесс оценки рисков информационной безопасности. Методология оценки рисков в первую очередь должна определять критерии оценки и условия принятия рисков.

В соответствии с ISO 27001:2013 в ходе процесса анализа рисков необходимо в первую очередь идентифицировать риски ИБ и определить

владельцев рисков. Затем провести анализ рисков, в ходе которого определить вероятность риска, размер ущерба и соответственно определить уровень рисков. После чего провести оценивание риска относительно установленных критериев принятия рисков и задать приоритеты для обработки рисков.

Помимо уже упомянутого принятия риска, заключающегося в том, что организация соглашается с возможной реализацией угрозы и принимает последствия, вариантами обработки рисков являются [65]: минимизация риска посредством внедрения контролей, передача риска, которая может заключаться как в его страховании, так и передаче подрядчику (в совокупности с процессами, передающимися на аутсорсинг), избежание риска, которое может заключаться в изменении процесса таким образом, что риск становится неактуальным.

Необходимо отметить, что в результате обработки риска остается так называемый остаточный риск, который принимается менеджментом компании (владельцами рисков).

Выделяют две основные группы методов оценки рисков безопасности. Первая группа позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности.

Вторая группа методов оценки рисков базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита.

При проведении полного анализа рисков необходимо [24]:

- определить ценность ресурсов;
- добавить к стандартному набору список угроз, актуальных для исследуемой информационной системы;
- оценить вероятность угроз;
- определить уязвимость ресурсов;
- предложить решение, обеспечивающее необходимый уровень ИБ.

Методология CORAS разработана в рамках программы InformationSocietyTechnologies. Ее суть состоит в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как Event-Tree-Analysis, цепи Маркова, HazOp и FMECA. [1]

Метод CORAS использует модель UML (Unified Modeling Language) унифицированный язык моделирования – язык графического описания для объектного моделирования в области разработки программного обеспечения.

Для документирования промежуточных результатов и для того, чтобы представить полные заключения об анализе рисков информационной безопасности, используются специальные диаграммы CORAS, которые встроены в UML. Метод CORAS – это компьютеризированный инструмент, который поддерживает документирование, создание отчетов о результатах анализа путем моделирования риска. Все работы относительно рисков проводятся посредством следующих процедур [112]:

- подготовительные мероприятия – сбор общих сведений об объекте анализа;
- представление клиентом объектов, которые необходимо проанализировать;
- детализированное описание задачи аналитиком;
- проверка корректности и полноты документация, представленной для анализа;
- мероприятия по выявлению рисков, (осуществляется, например, в форме семинара) возглавляемые аналитиками;
- оценка вероятностей и последствий инцидентов информационной безопасности;
- выявление приемлемых рисков и рисков, которые должны быть представлены на дальнейшую оценку для возможного устранения;
- устранение угроз, с целью сокращения вероятности и / или последствий инцидентов в области информационной безопасности.

Метод CRAMM (CCTA Risk Analysis and Management Method –метод CCTA анализа и контроля рисков) был разработан в 1985 г. Центральным агентством по компьютерам и телекоммуникациям Великобритании (CCTA - Central Computer and Telecommunications Agency UK) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта. [112]

В методе CRAMM анализ рисков осуществляет идентификацию и вычисление уровней (мер) рисков основываясь на оценках, присвоенных ресурсам, уязвимостям и угрозам ресурсов.

Контроль рисков заключается в идентификации и выборе контрдействий, позволяющих понизить риски до требуемого уровня.

Основанный на этой концепции формальный метод позволяет убедиться, что защита охватывает всю систему и создает уверенность в том, что:

- все существующие риски определены;
- уязвимости идентифицированы и оценены их уровни;
- угрозы определены и их уровни оценены;
- контрмеры показывают себя эффективно;
- расходы, связанные с информационной безопасностью, оправданы.

Исследование состояния информационной безопасности системы с применением метода CRAMM осуществляется в три стадии [66]:

1) на первой стадии производится определение ценности защищаемых ресурсов. По завершению стадии заказчик исследования должен знать, хватает ли для защиты системы возможностей базового уровня защиты с традиционными функциями безопасности, или стоит провести более детальный анализ;

2) на второй рассматриваются вопросы, относящиеся к оценке уровней угроз для групп ресурсов и их уязвимостей. В конце этой стадии заказчик получает для своей системы идентифицированные и оцененные уровни рисков;

3) на третьей стадии производится поиск адекватных противомер. Фактически это поиск варианта системы безопасности, который лучшим образом удовлетворит требования заказчика. В конце данной стадии заказчик будет знать, как следует улучшить систему для уклонения от риска, а также какие специальные меры противодействия ведут к снижению и минимизации остальных рисков.

К недостаткам метода CRAMM можно отнести следующее [66]:

- Использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;
- Аудит по методу CRAMM — процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;
- Программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;
- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся;
- Возможность внесения дополнений в базу знаний CRAMM недоступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации;
- Программное обеспечение CRAMM существует только на английском языке;
- Высокая стоимость лицензии.

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation – оценка критичных угроз, активов и уязвимостей) – метод оперативной оценки критических угроз, активов и уязвимостей. Методика

подразумевает создание группы анализа, которая изучает безопасность. Группа анализа (ГА) включает сотрудников бизнес-подразделений, эксплуатирующих систему, и сотрудников отдела информационных технологий. [92]

Метод OCTAVE реализуется трехэтапный подход оценки рисков информационной безопасности.

На первой стадии осуществляется оценка организационных аспектов. Во время выполнения этой стадии ГА определяет критерии (показатели) оценки ущерба (неблагоприятных последствий), которые позже будут использоваться при оценке рисков. Здесь же осуществляется определение наиболее важных организационных ресурсов и оценка текущего состояния практики обеспечения безопасности в организации.

На второй стадии проводится высокоуровневый анализ ИТ-инфраструктуры организации, при этом обращается внимание на степень, с которой вопросы безопасности решаются и поддерживаются подразделениями и сотрудниками, отвечающими за эксплуатацию инфраструктуры.

На третьей стадии проводится разработка стратегии обеспечения безопасности и плана защиты информации. Этот этап складывается из определения и анализа рисков и разработки стратегии обеспечения безопасности и плана сокращения рисков. В процессе определения и анализа рисков оценивают ущерб от реализации угроз и устанавливают вероятностные критерии оценки угроз.

В процессе разработки стратегии обеспечения безопасности и плана сокращения рисков: описывают текущую стратегию безопасности, выбирают подходы сокращения рисков, разрабатывают план сокращения рисков, определяют изменения в стратегии обеспечения безопасности, определяют перспективные направления обеспечения безопасности.

До принятия решения о внедрении того или иного метода управления рисками следует убедиться, что он достаточно полно учитывает бизнес-потребности компании. В качестве критериев оценки при сравнении методологий управления рисками целесообразно воспользоваться стандартом COBIT. Аббревиатура COBIT (Control Objectives for Information and Related Technologies) подразумевает под собой набор документов, в которых изложены принципы управления и аудита, основанные на лучших мировых практиках. В качестве критериев оценки методов управления рисками можно использовать инструкции COBIT по аудиту процесса «Оценка рисков». [37]

Используя COBIT для анализа методов управления рисками, следует учитывать, что существуют некоторые ограничения. Например, методология OCTAVE предусматривает адаптацию к конкретным условиям применения, а COBIT нет. При выборе методов управления рисками не последнюю роль играют стоимость и время внедрения. Метод сравнительного анализа не

учитывает объем, в котором компания планирует внедрение методологии. Согласно стандарту COBIT, концепция управления рисками подразумевает обход риска, его снижение или принятие. Такой способ управления рисками, как их перенос (т.е. страхование), не рассматривается. Перенос риска обычно используется в тех случаях, когда вероятность наступления нежелательного события мала, а потенциальный ущерб относительно высок.

Рассмотренные методы не предполагают расчета оптимального баланса различных способов управления, не имеют средств интеграции способов управления и не дают механизмов управления рисками остаточного уровня. Так же во всех трех методологиях не производится оценка качества процесса реагирования на инциденты в области информационной безопасности. [71]

Ни один из методов не дает подробных рекомендаций по поводу составления расписания проведения повторных оценок рисков, и в двух методологиях совершенно упущено из виду обновление величин рисков. В случае если требуется выполнить только разовую оценку уровня рисков в компании любого размера, целесообразно применять методологию CORAS. Для управления рисками на базе периодических оценок на техническом уровне лучше всего подходит CRAMM. Методология OCTAVE предпочтительна для использования в крупных компаниях, где предполагается внедрение управления рисками на базе регулярных оценок на уровне не ниже организационного и требуется разработка обоснованного плана мероприятий по их снижению.

На практике для большинства выявленных рисков принимается решение об их минимизации путем внедрения контролей (механизмов). Стандарт ISO 27001:2013 [50] содержит Приложение А, в котором приведены 114 контролей, распределенных по следующим 14-ти доменам [1] : А.5 Политики информационной безопасности, А.6 Организационные аспекты информационной безопасности, А.7 Вопросы безопасности, связанные с персоналом, А.8 Управление активами, А.9 Управление доступом, А.10 Криптография, А. 11 Физическая безопасность и защита от угроз окружающей среды, А.12 Безопасность операций, А.13 Безопасность коммуникаций, А.14 Приемка, разработка и поддержка систем, А.15 Отношения с поставщиками услуг, А.16 Управление инцидентами информационной безопасности, А.17 Аспекты информационной безопасности в обеспечении непрерывности бизнеса, А.18 Соответствие требованиям.

[1] домены (domain) – это набор объектов, к которым могут обращаться субъекты. Доменом могут быть все ресурсы, к которым могут обращаться пользователи; все файлы, доступные программам; сегменты памяти, доступные процессам; службы и процессы, доступные приложению. Субъекту необходим доступ к объектам (ресурсов) для выполнения своих задач, и именно домен определяет, какие объекты доступны этому субъекту, а к каким доступ не предоставляется.

В случае внедрения СУИБ в соответствии с ISO 27001:2013 компания руководствуется Приложением А для выбора контролей, при этом, исключение контроля должно быть обоснованным, как и включение контроля, отсутствующего в стандарте.

Интересно, что контроли неравноценны. В целом контроли из Приложения А относятся к организационным мерам, например, встречаются контроли «Политика контроля доступа» (А.9.1.1), «Правила использования активов» (А.8.1.3), предусматривающие определение правил информационной безопасности в форме политик. Что же касается технически мер, то они формулируются исключительно общими словами, например, «Безопасность сетевых сервисов» (А.13.1.2). [36]

После решения задачи выбора контролей определяется: что конкретно должно быть сделано, какие ресурсы для этого необходимо задействовать, кто будет ответственным, и как будет проводиться оценка выполнения.

На данном этапе разрабатываются политики, процедуры, инструкции (подробнее о них ниже), внедряются технические средства защиты информации, проводится обучение специалистов, задействованных в процессах обеспечения ИБ, внедряется программа повышения осведомленности сотрудников компании в вопросах безопасности (security awareness program).

В результате внедрения контролей должны быть получены работающие процессы СУИБ, которые выполняются, измеряются и контролируются. Необходимо отметить следующие три важных составляющих контроля работы СУИБ: операционный контроль, внутренний аудит, анализ со стороны руководства. [35]

Операционный контроль подразумевает собой текущий контроль со стороны непосредственных руководителей. Например, принятая процедура предусматривает выполнение периодического сканирования на наличие уязвимостей сетевых сервисов, и отвечает за эту функцию конкретный специалист отдела ИБ. Соответственно руководитель отдела следит за тем, чтобы задача выполнялась подчиненным, и он вовремя получал отчет с результатами сканирования.

Внутренний аудит заключается в периодической проверке эффективности контролей..

Результатом подобных контрольных мероприятий будет информация о недостатках и необходимых улучшениях системы. Концепция постоянного улучшения СУИБ является одним из основных принципов стандарта.

Внедрение политики ИБ требует регламентации практически всех процессов обработки, хранения, передачи и обмена информации, разработки документированных процедур и инструкций. Как показывает практика, организационные меры играют очень важную роль во внедрении мероприятий

политики ИБ в организации, поэтому необходимо организовать непрерывное повышение осведомленности, повышения квалификации и обучения сотрудников организации в области ИБ.

ГЛАВА 3. СТАНДАРТЫ СЕРИИ ISO 2700X КАК ОСНОВА ПОСТРОЕНИЯ ЭФФЕКТИВНОЙ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Обзор международных стандартов ISO 2700x.

ISO/IEC 27000 – серия международных стандартов, которая включает стандарты по информационной безопасности, которые определяют требования к системам управления информационной безопасностью, к управлению рисками, а также руководство по внедрению.

По стандарту ISO 27001 2011 информационная безопасность – это обеспечение конфиденциальности, целостности и доступности информации; также возможно обеспечение и других свойств, таких как аутентичность, идентифицируемость, отказоустойчивость и надёжность. [50]

Стандарты можно разделить на четыре группы [32]:

1. Стандарты для обзора и введения в терминологию;
2. Стандарты, определяющие обязательные требования к СУИБ (система управления информационной безопасностью);
3. Стандарты, определяющие требования и рекомендации для аудита СУИБ;
4. Стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ.

К первой группе можно отнести стандарт семейства: ISO 27000. Он включает в себя: информационные технологии, средства обеспечения безопасности, системы менеджмента информационной безопасности, а также обзор и словарь. Другими словами, стандарт описывает основные определения, которые используются в стандартах информационной безопасности. [49]

Вторая группа включает в себя всего лишь один стандарт: ISO 27001. Суть этого стандарта заключается в описании информационных технологий, методов и средств обеспечения безопасности, менеджмента информационной безопасности и выявлении требований. Необходимо отметить, что это основной стандарт группы стандартов ISO 2700x. [50]

Стандарт ISO 27001 включает в себя описание общей модели внедрения и функционирования системы менеджмента информационной безопасности. Цель данного стандарта заключается в обеспечении согласованности менеджмента ИБ вместе с другими системами управления в компании. Другими словами, при внедрении других стандартов менеджмента, она может с легкостью применять единую систему аудита.

Система менеджмента информационной безопасности описана в данном стандарте с точки зрения создания, внедрения, эксплуатации, мониторинга и поддержки. При внедрении данной системы, компанию получает средства

мониторинга и управления безопасностью, которые помогают снизить различные типы рисков.

В приложениях стандарта ISO 27001 содержатся цели и средства управления информационной безопасностью. При внедрении системы менеджмента информационной безопасности, стандарт ISO 27001 использует цикл СУИБ.

В разделах четыре и восемь стандарта ISO 27001 содержатся основные требования создания СУИБ.

Стандарт ISO 27001 описывает системы управления ИБ на основе оценки рисков. Механизмы выработки контроля перечислены в приложении А, это перечень контролей, который являются обязательном списком для организации. Организация на основе этого списка может выбрать и внедрить те контроли, которые ей нужны при построении системы. Но каждое исключение из этого списка должно быть обосновано. Это показывает двойственность статуса этого списка. [50]

В третью группу можно включить три стандарта: ISO 27006, ISO 27007, ISO 27008, которые включают в себя указания и требования для аудита информационной безопасности.

ISO 27006 включает в себя: описание информационных технологий, средств обеспечения информационной безопасности и требования для организаций, которые выполняют аудит систем менеджмента информационной безопасности. Устанавливает требования к органам, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности, и способствует проведению аккредитации органов сертификации. Любой орган, осуществляющий сертификацию СУИБ, должен продемонстрировать в плане компетентности и надежности свое соответствие требованиям к органу, осуществляющему сертификацию СУИБ. Этот документ может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки или других процессов аудита. [46]

ISO 27007 описывает два первых пункта ISO 27006, а также указания для аудита систем менеджмента информационной безопасности. Данный стандарт очень полезен для аудиторов организаций. Стандарт применим для тех организаций, которые нуждаются в понимании или проведении внутренних, или внешних аудитов системы менеджмента информационной безопасности или осуществлении менеджмента программы аудита системы управления информационной безопасности. [6]

ISO 27008 включает в себя руководство для аудита по мерам обеспечения информационной безопасности. Данный стандарт специализирован на аудите информационной безопасности в организации.

В стандарт предлагает строгую организационную проверку защиты и программу анализа для средств управления информационной безопасностью, чтобы позволить организации быть уверенной, что их средства управления соответственно реализовывались и управлялись и что их информационная безопасность соответствует целевому назначению.

Стандарт дает представление о рассмотрении реализации и работы средств управления, включая техническую проверку соответствия. Это преимущественно нацелено на аудиторов информационной безопасности, которые должны проверить техническое соответствие средств управления информационной безопасностью организации против ISO 27002 и любых других стандартов управления, используемых организацией.

ISO/TR 27008 позволяет:

- идентифицировать и понять степень потенциальных проблем и недостатки средств управления информационной безопасностью
- идентифицировать и понять потенциальные организационные угрозы и уязвимости
- позволяет выработать стратегию действий для смягчения риска информационной безопасности. [12]

Последняя группа включает в себя оставшиеся стандарты семейства 2700x, а именно стандарты: ISO 27002; ISO 27003; ISO 27004; ISO 27005; ISO 27011; ISO 27031; ISO 27033; ISO 27034; ISO 27035; ISO 27799 (специализированной руководство СУИБ в здравоохранении).

ISO 27002 включает в себя свод практики менеджмента информационной безопасности, а также описание контролей и способов их реализации в организации в информационной безопасности. Их около ста. Эти контроли осуществляются преимущественно на уровне процессов, и разделены на так называемые домены: политика информационной безопасности, организационные вопросы ИБ, вопросы ИБ связи с персоналом, управление доступом, криптография, физическая безопасность и защита от угрозы окружающей среды, операционные вопросы ИБ, безопасность коммуникаций, приемка, разработка, поддержка информационных систем, взаимодействия с поставщиками, управление инцидентами ИБ, вопросы ИБ при непрерывности бизнеса, выполнения требований. [47]

Данный стандарт, ISO 27002, предоставляет указания для внедрения, разработки, поддержки и совершенства СУИБ. Его можно назвать основным стандартом для консультантов. Организация должна серьезно относиться к информационным активам, и внедрить СУИБ, основываясь на стандарте ISO 27002. Он включает в себя двенадцать разделов, которые описывают средства управления безопасностью (доменов) о которых говорилось выше.

Стандарт ISO 27002 имеет идентичную структуру приложения А в стандарте ISO 27001. Но помимо формулировок контролей есть подробные описания того, что скрывается за тем или иным контролем, и как этот контроль может быть реализован в организации.

В отличие от стандарта ISO 27002, ISO 27003 предоставляет руководство по осуществлению контроля информационной безопасности. В стандарт прописаны указания и методики для разработки и внедрения СУИБ. В нем описывается процесс определения и разработки СУИБ, от запуска до составления планов внедрения. В нем описывается процесс получения одобрения руководством внедрения СУИБ, определяется проект внедрения СУИБ (упоминается в данном международном стандарте, как проект СУИБ), и представлены рекомендации по планированию проекта СУИБ, в результате которого получается конечный план внедрения СУИБ.

Международный стандарт ISO 27002 предназначен для использования организациями, применяющими СУИБ. Он применяется ко всем типам организаций (например, коммерческим предприятиям, правительственным органам, некоммерческим организациям) любых размеров. Сложность структуры и риски каждой организации уникальны, и на внедрение СУИБ будут влиять ее особые требования. Небольшие организации могут посчитать, что действия, указанные в данном международном стандарте, применимы к ним и могут быть упрощены. Крупным организациям или организациям со сложной структурой для эффективного выполнения действий, указанных в данном международном стандарте, может потребоваться многоуровневая система организации или управления. Однако в обоих случаях соответствующие действия можно планировать, применяя данный международный стандарт. В данном международном стандарте приведены рекомендации и разъяснения; в нем не указано никаких требований.

Стандарт ISO 27003 предназначен для использования в сочетании с ISO/IEC 27001:2005 и ISO/IEC 27002:2005, но не предназначен для изменения или сокращения требований, указанных в ISO/IEC 27001:2005, или рекомендаций, приведенных в ISO/IEC 27002:2005. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности обеспечивает рекомендации для менеджмента рисков информационной безопасности, которые включают информацию и менеджмент рисков безопасности технологий телекоммуникации. Эти рекомендации предназначены, чтобы помочь реализовать достаточную информационную безопасность, основанную на подходе менеджмента рисками.

Этот международный стандарт является применимым ко всем типам организаций (например, коммерческие предприятия, правительственные агентства, некоммерческие организации), которые намереваются осуществлять

менеджмент рисками, ставящими под угрозу информационную безопасность организации. [4]

Измерения менеджмента информационной безопасности предоставлено в ISO 27004. Данный стандарт рассчитан для проектирования и выбора, лучших методов измерения эффективности системы.

Эффективно реализованная программа измерений позволит укрепить доверие заинтересованных сторон к результатам измерений, а также даст возможность заинтересованным сторонам применять меры измерений для непрерывного улучшения информационной безопасности и СУИБ.

Накопленные результаты измерений позволят следить за прогрессом в достижении целей информационной безопасности за некоторый период времени в интересах реализации процесса непрерывного совершенствования СУИБ организации. [5]

Стандарт ISO 27005 помогает рассмотреть различные методы защиты, а также управления рисками при информационной безопасности. Можно назвать этот стандарт самым важным в группе, так как рассмотрение рисков является основой при обеспечении информационной безопасности.

Этот международный стандарт является применимым ко всем типам организаций (например, коммерческие предприятия, правительственные агентства, некоммерческие организации), которые намереваются осуществлять менеджмент рисками, ставящими под угрозу информационную безопасность организации. [48]

Стандарт ISO 27011 специализируется на телекоммуникациях. Задача стандарта заключается в описании обеспечения информационной безопасности по СУИБ в телекоммуникационных организациях. [7]

Стандарт ISO 27031 создан для помощи в проведении анализ по обеспечению непрерывности бизнеса. В нем можно найти руководство по менеджменту информационной безопасности для телекоммуникаций. [8]

Информационную безопасность можно разделить на несколько типов. Сетевая безопасность является одним из типов информационной безопасности. Методы защиты информации и обеспечение сетевой безопасности подробно описаны в стандарте ISO 27033. Также здесь изложена информация о различных угрозах и методах проектирования сетевой инфраструктуры. [9]

ISO 27034 несет терминологический характер. Здесь можно узнать информацию о безопасности приложений, а также методах обеспечения безопасности данного программного обеспечения. Об управлении инцидентами по информационной безопасности можно узнать из ISO 27035. Данный стандарт является одним из ценных стандартов в группе развития и совершенствования СУИБ. [10, 11]

Проанализировав основную группу стандартов ISO 2700x, необходимо выделить взаимосвязь двух основных – ISO 27001 и ISO 27002.

Стандарт ISO 27001, представляя СУИБ, отвечает на вопрос «как это делать» и включает процедуры создания и поддержки СУИБ. Стандарт ISO 27002, представляет руководящие принципы по реализации средств управления, отвечая на вопрос «что нужно делать». Он включает перечень полезных средств управления.

Приложение А стандарта ISO 27001 в том же порядке перечисляет средства управления, приведенные в ISO 27002, но при этом дается только краткое описание этих средств управления. Оба стандарта позволяют подготовиться к прохождению сертификации на соответствие ISO 27001.

3.2 Обзор отечественных стандартов и их сравнение с зарубежными стандартами

На сегодняшний день насчитывается порядка 58 отечественных стандартов. В 1999 г. Международная Организация по Стандартизации (ISO) приняла международный стандарт ISO 15408 под названием Общие критерии оценки безопасности ИТ (Common Criteria for Information Technology Security Evaluation или сокращенно - Common Criteria), который в области обеспечения ИБ имел большое значение. В нем наиболее полно представлены критерии для оценки механизмов безопасности программно-технического уровня. Общие критерии определяют функциональные требования безопасности (security functional requirements) и требования к реализации функций безопасности (security assurance requirements). Стандарт стал своего рода гарантией качества и надежности сертифицированных по нему программных продуктов. [90, 93]

В отечественной версии ISO 15408 состоит из трех частей: СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3. Часть 1 СТБ 34.101.1-2014 «Введение и общая модель» устанавливает общий подход к формированию требований безопасности и оценке безопасности. На их основе происходит разработка основных конструкций, которые представляют требования безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Часть 2 СТБ 34.101.2-2014 «Функциональные требования безопасности» содержит различные функциональные требования безопасности и предоставляет возможность их детализации и расширения. Часть 3 СТБ 34.101.3-2014 «Требования доверия к безопасности» включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям [42, 43, 44].

СТБ 34.101.1,2,3 описывает способы защиты от несанкционированного доступа. Данный стандарт устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации; к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

СТБ ГОСТ Р 50922-2000 «Защита информации. Основные термины и определения». Он несет методологический характер и включает в себя основные термины и определения по информационной безопасности, а также описывает общие положения о защите информационной безопасности и некоторые факторы, которые на нее воздействуют. [41]

Защита от вирусов является первостепенной задачей при защите информационно безопасности. СТБ 34.101.15-2007 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Типовая программа и методика испытаний» содержит в себе типовое руководство по испытанию программного обеспечения на наличие вирусных программ. Этот стандарт распространяется на испытания программных средств и их компонентов, цели которых - обнаружить в этих ПС и устранить из них компьютерные вирусы силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний. [45]

С 2007 по 2014 гг. в Республике Беларусь введены в действие серия стандартов в области криптографической защиты информации. Были стандартизированы алгоритмы шифрования, имитозащиты, хэширования и управления ключами (СТБ 34.101.31), разделения секрета (СТБ 34.101.60), генерации псевдослучайных чисел (СТБ 34.101.47), электронной цифровой подписи и транспорта ключа (СТБ 34.101.45), протокол TLS (СТБ 34.101.65), протоколы формирования общего ключа на основе эллиптических кривых (СТБ 34.101.66). Стандартизированные алгоритмы и протоколы соответствуют лучшим зарубежным аналогам, а в некоторых случаях опережают эти аналоги или не имеют таковых. Разработанные стандарты начинают широко применяться при построении республиканских систем защиты информации. Известные примеры – запускаемая Государственная система управления открытыми ключами (далее – ГоСУОК) и проектируемая Единая система идентификации физических и юридических лиц (далее –ЕСИФЮЛ)

Разработка стандартов проводилась в Научно-исследовательском институте прикладных проблем математики и информатики (далее – НИИ). Следует подчеркнуть, что каждый из стандартов не является отдельной разработкой. В стандартах фиксируются результаты научных исследований в определенных областях криптологии. Базовые научные исследования проводились на протяжении последних 15-20лет.

Криптографические стандарты определяют национальную криптографическую инфраструктуру. Схожие инфраструктуры созданы в Российской Федерации и в Южной Корее. Особенностью страны является то, что стандарты разрабатываются не в федеральных агентствах ФСБ в РФ, KISA в Корее, а в независимой научно-исследовательской организации НИИ. [72]

Белорусские специалисты считают, что криптографическая инфраструктура не должна быть статической. Инфраструктура должна поддерживаться, по крайней мере, следующими мероприятиями:

1. Научные исследования должны быть направленны на уточнение оценок стойкости принятых криптографических алгоритмов и протоколов. По мере необходимости должны разрабатываться дополнительные алгоритмы и протоколы.
2. Поддержка интеграции, для встраивания отечественных криптографических алгоритмов в существующие информационные системы должны выпускаться расширения международных стандартов и спецификаций. В этих расширениях могут уточняться форматы криптографических данных, фиксироваться правила применения алгоритмов, вводиться согласованные наборы алгоритмов (криптоопределения) и др. Важным шагом в направлении интеграции является разработка компанией «АВЕСТ» стандартов на форматы данных (СТБ 34.101.17, 19, 23, 26).
3. Для упрощения разработки средств криптографической защиты информации (СКЗИ) должны выпускаться эталонные программные реализации алгоритмов и протоколов. Эталонные реализации могут быть сделаны общедоступными. Разработчики СКЗИ должны получать официальные комментарии и разъяснения относительно отдельных положений стандартов. Должен быть организован учет замечаний и предложений разработчиков по расширению и совершенствованию стандартов.
4. Для сокращения сроков и стоимости экспертизы и сертификации СКЗИ, для повышения качества испытаний должны выпускаться типовые методики испытаний, общедоступные наборы проверочных примеров. Должны разрабатываться программы автоматизации испытаний, например, программы проверки форматов криптографических данных.
5. Должны предприниматься шаги по популяризации и продвижению отечественных алгоритмов и протоколов. Ключевые стандарты должны быть зафиксированы в формате RFC (спецификаций Интернет). [56]

Анализируя принятые стандарты по информационной безопасности в Республике Беларусь, можно сказать, что они отвечают европейским требованиям. Также в Республике Беларусь самостоятельно разработаны и совершенствуется серия стандартов в области криптографической защиты информации. Но существует ряд проблем при переводе международных стандартов. Встречаются ошибки и двусмысленность терминологии, что приводит к несогласованности и разобщенности языка и понимания, а это– к разногласию в организации.

За период 1999-2017 гг. в Республике Беларусь вступило в силу около 60 отечественных стандартов, такое же количество стандартов насчитывает на данный момент и семейство стандартов ISO 2700x. [36]

Критериями сравнения международных и отечественных стандартов может служить терминология, требования к СУИБ, требования и рекомендации аудита СУИБ, предложение лучшей практики внедрения, развития и совершенствования СУИБ.

В отечественных и зарубежных стандартах есть по одному стандарту, в которых содержится терминология. В каждом из стандартов даны четкие определения информационной безопасности. Но есть и отличия. Отечественный стандарт больше специализируется на терминологии защиты информации и угроз ее потери. В данном стандарте преобладают такие определения как защита информации от утечки, защита информации от разглашения, система защиты информации, цель защиты информации. Европейский стандарт больше специализируется на правах доступа к информации отдельных лиц. В ISO 27000 можно увидеть информацию о таких определениях как аутентификация, доступность, конфиденциальность, событие, результативность.

Пользуясь отечественными стандартами, желательно использовать оригиналы, т.к. при переводах международных стандартов встречаются ошибки и двусмысленность терминологии. Это одна из проблем, при создании отечественных стандартов на основе международных.

Определение требований к СУИБ в отечественных и зарубежных стандартах есть по одному стандарту, стандарт ISO 27001 и стандарт СТБ 34.101 в трех частях. Европейский стандарт описывает четко и ясно алгоритм внедрения системы моделирования информационной безопасности. Она состоит из четырех этапов.

На первом этап обозначены цели и выгоды внедрения СУИБ, и отмечена поддержка руководства на внедрение и ввод в эксплуатацию СУИБ, распределена ответственность по СУИБ.

На втором этапе, организационном, создается группа по внедрению и поддержке СУИБ, организовывается Ее обучение внедрению и поддержке СУИБ и определяется область действия СУИБ

На третьем этапе проводится первоначальный анализ СУИБ, определяется перечень работ по доработке, существующей СУИБ.

На четвертом этапе определяются политики и цели СУИБ

Отечественные стандарт разделен на три части для описания полноты процесса. В первой части происходит описание некоторых определений и предоставляется алгоритм обеспечения информационной безопасности. Во второй – описание функциональных требований к информационной

безопасности, которые представлены в виде списка. Третья, как и вторая содержит правила в виде списка, однако, предоставляя требования для доверия к безопасности.

Зарубежные стандарты рассматривают все это в отдельных стандартах, не смешивая это так, как делается в Республике Беларуси.

Отечественный стандарт СТБ ISO/IEC 27006-2014 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента информационной безопасности» не отличается от европейского стандарта, в отличие от российских ГОСТ 51 -275 99, а также ГОСТ 7498. Он вводят базовую эталонную систему обеспечения безопасности открытых систем. Стандарт включает в себя подробное рассмотрение модели и описание того, как должна быть структурирована открытая система для проведения аудита и обеспечения качественной защиты ИБ данный. Так же, как и предыдущих стандартах, он разделен на две главы, однако, здесь, это упрощает понимание. Анализ факторов, которые могут быть использованы для защиты информации, вместе с эталонной моделью предоставляют хотя и неполные, однако достаточные сведения для аудита СУИБ.

Европейские и их аналоги – стандарты Республики Беларуси отличаются краткостью и лаконичностью своих изъяснений. Эти стандарт даже по критерию лучших практик внедрения, развития и совершенствования СУИБ, первенство занимают европейские стандарты. Они выигрывают и количественно в данной группе. Чёткое и ясное название стандартов, например, «свод практики менеджмента информационной безопасности», предоставляет проектирование, выбор, улучшение методов измерения эффективности системы. Более того, присутствие специализированных стандартов, являются огромным плюсом в европейских стандартах, т.е. заграницей информационная безопасность распространена везде на все слои информации индивидуума. Другими словами, защита происходит не только от краж, то и от разглашения фамилии или заболеваний, если того хочет человек. Специализация Белорусских стандартов направлена на сохранение материального статуса компаний и человека. Защита банковских карт, счетов в банке, номера кредитных карт: все это защищено. К этой группе можно отнести стандарты, относящиеся к криптографической защите, а также к стандартам, специализирующиеся на испытаниях ПО на наличие вирусов.

Использование стандартов безопасности ISO позволяет внедрять эффективные методы управления бизнес-рисками.

Таким образом, анализируя семейство стандартов ISO 2700x, необходимо выделить два основополагающих стандарта ISO 27001 и ISO 27002, которые

позволяют упорядоченно подойти к разработке, внедрению, управлению и поддержке программы по менеджменту информационной безопасности.

Разработка отечественных стандартов позволяет урегулировать несоответствие с законодательством, но есть проблемы при переводах международных стандартов, встречаются ошибки и двусмысленность терминологии.

На сегодняшний день европейские стандарты по информационной безопасности, количеством и качеством превышают отечественные. Следует отметить, что Республика Беларусь самостоятельно разрабатывает и совершенствует стандарты в области информационной безопасности, примером служит серия стандартов по криптографической защите информации, которая были разработана в НИИ.

ГЛАВА 4. ДОКУМЕНТАЦИОННОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В АРХИВЕ ОРГАНИЗАЦИИ

Современная СУИБ представляет собой процессно-ориентированную систему управления, включающую организационный, документальный и программно-аппаратный компоненты. Можно выделить следующие подходы к СУИБ: процессный, документальный и целостный.

Процессы СУИБ созданы в соответствии с требованиями стандарта ISO/IEC 27001:2005, в основе которого лежит цикл управления Plan-Do-Check-Act. В соответствии с ним, жизненный цикл СУИБ состоит из четырех типов деятельности: Создание - Внедрение и эксплуатация - Мониторинг и анализ - Сопровождение и совершенствование. Документированные процессы СУИБ обеспечивают выполнение всех требований стандарта 27001.

Документация СУИБ состоит из политик, документированных процедур, стандартов и записей и делится на две части: документация менеджмента СУИБ и эксплуатационная документация СУИБ.

Зрелостная модель СУИБ определяет детализацию разрабатываемой документации и степень автоматизации процессов менеджмента и эксплуатации СУИБ. При оценке и планировании используется модель зрелости CobiT (от англ. Control Objectives for Information and Related Technologies). В Программе повышения зрелости СУИБ приводятся состав и сроки мероприятий по совершенствованию процессов менеджмента ИБ и управления эксплуатацией средств ИБ.

В 2005 году в свет вышел международный стандарт в области информационной безопасности – BS ISO/IEC 27001. В документе сформулированы требования к системе управления информационной безопасностью (СУИБ), включая общую методологию создания, внедрения и оценки эффективности механизмов СУИБ. В настоящее время наблюдается повышенный интерес к этому стандарту со стороны компаний, работающих в различных отраслях. Соответствие ему становится важным фактором коммерческого успеха организации благодаря целому ряду преимуществ, которые она получает. [73]

Самым трудоемким и сложным этапом на пути к сертификации является собственно создание системы управления ИБ и внедрение ее механизмов в компании. Этот процесс можно разделить на 10 основных этапов [55]:

1. выборипроцесс(ы) (область деятельности), который(е) будут сертифицировать;
2. сбор команды, если необходимо, то привлечение специалистов;

3. проведение внутреннего аудита с целью определить текущее состояние СУИБ компании;
4. проведение идентификации ресурсов, которые входят в выбранную область деятельности;
5. определение ценности ресурсов;
6. подсчет рисков;
7. подготовка пакета документов: политики, стандарты, положения, процедуры и т. п.;
8. внедрение политик, стандартов, положений, процедур и т. п.;
9. проведение внутреннего аудита и оценка СУИБ с учетом проведенной работы по внедрению организационных и технических мер;
10. подача заявки на проведение сертификационного аудита.

В целом СУИБ распространяется на всю информационную систему (далее – ИС) компании. Однако внедрение системы управления – достаточно сложный процесс. Практика показывает, что сертификацию всех бизнес-процессов не всегда можно реализовать по разным причинам, например, финансовым. Поэтому, как правило, компании выбирают один из критичных бизнес-процессов (например, обработка и хранение данных клиентов, финансовые операции) или автоматизированных систем и внедряют процедуры системы управления, а потом распространяют их на остальные процессы компании.

Отметим, что в рамках области действия СУИБ требуется определить следующие активы: информационные ресурсы, средства хранения и обработки информации, программное обеспечение, пользователи ИС, вспомогательные сервисы и системы жизнеобеспечения.

Уровень требуемой защищенности зависит от степени критичности информации для компании. Оценку критичности информации проводят, как правило, по трем критериям: конфиденциальности, целостности и доступности. Для каждой информации требуется определить ущерб, который понесет компания при ее разглашении, модификации или невозможности получить к ней доступ. Сложность этого процесса заключается в том, что оценку критичности активов должны производить сотрудники, работающие с информацией, которые зачастую не знают, как это сделать. С целью упрощения данного процесса разрабатываются методики оценки критичности, различные формы для заполнения результатов. [61]

До момента утверждения сертифицируемой области действия имеет смысл составить список, или чек-лист, всех существующих бизнес-процессов в компании и выбрать из него наиболее критичные процессы с точки зрения информационной безопасности. Это может быть обработка и хранение данных клиентов, финансовые операции и др.

В качестве наиболее действенного способа определения области действия и бизнес-процессов, лучше использовать чек-лист. Он позволит систематизировать процессы. Уже на основании этого можно определить область действия и процессы, которые в нее попадают. (Приложение Б)

Чек-лист формируется на основе локальных нормативных актов организации и положениями стандартов (например, СТБ ISO/IEC). Например, в СТБ ISO/IEC 27002-2012 приведен перечень вопросов, при аудите ИБ:

- наличие политики информационной безопасности, обеспечивающей управление и поддержку в области информационной безопасности со стороны руководства организации в соответствии с требованиями бизнеса, соответствующими законами и нормативными актами;
- физическая безопасность и безопасность окружающей среды (предотвращение несанкционированного физического доступа и причинение ущерба для помещений и информации организации; предотвращение потери, повреждения, кражи или компрометации ресурсов и нарушение деятельности организации (например, в результате пожара);
- управление инцидентами информационной безопасности (информирование о событиях и слабостях информационной безопасности; управление инцидентами и усовершенствованиями информационной безопасности) и т.д. [47]

Для построения, внедрения и сертификации СУИБ нужно собрать квалифицированную группу. Для этого можно использовать чек-лист. Он определяет ключевые бизнес-процессы, а следовательно и ключевых работников, которые должны войти в группу, работающую над построением системы СУИБ и подготовкой к сертификации.

В качестве примера в состав группы могут входить: директор компании, директор по финансам и развитию, секретарь, как человек ответственный за работу с документами, менеджер по вопросам информационной безопасности, системный администратор.

Количество человек, входящих в состав рабочей группы по созданию и внедрению СУИБ, зависит от размера компании и технических процессов.

После создания рабочей группы по созданию и внедрению СУИБ проводится внутренний аудит с целью определить текущее состояние СУИБ компании.

Аудит информационной безопасности – процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности предприятия в соответствии с определенными критериями и показателями безопасности. [60]

Основные цели аудита информационной безопасности:

- получение оценки состояния защищенности информационной системы;
- расчет материальных средств, инвестируемых в создание системы менеджмента информационной безопасности;
- оценка возможного ущерба от реализации информационных угроз;
- разработка требований к построению политики безопасности;
- расчет необходимых ресурсов для создания системы менеджмента информационной безопасности;
- внедрение системы менеджмента информационной безопасности.

Самый распространенный вид аудита является активный аудит. Это исследование состояния защищенности информационной системы предприятия с помощью специального программного обеспечения. При таком анализе осуществляется сбор информации о состоянии системы информационной безопасности. Под специальным программным обеспечением понимают разнообразные сканеры сети, анализаторы сетевого трафика. Суть таких программ – сканирование и зондирования сетевых ресурсов с целью выявления их уязвимостей. [15] Такие атаки моделируют возможное воздействие на информационную систему, но не оказывают деструктивного воздействия. Результатом активного аудита является информация обо всех уязвимостях информационной сети, степени критичности уязвимости и способах устранения.

Для представления алгоритма выполнения аудита в работе была разработана нотация [2] класса workflow в, которой отражены исполнители действий процесса. (Приложение В)

Аудит на соответствие требованиям информационной безопасности – это комплексный, циклический процесс, который состоит из следующих этапов:

- планирование аудита;
- планирование мероприятий по аудиту (разработка, согласование и утверждение планов мероприятий);
- сбор информации;
- проверка на соответствие группе требований (например, на соответствие стандарту СТБ ISO/IEC 27001);
- систематизация результатов обследования и формирование отчетности.
- Эти этапы составляют жизненный цикл аудита.

[2] Нотация – схема, в которой с помощью системы условных посменных обозначений, принятых в какой-либо области, раскрывается бизнес-процесс.

Непосредственно перед проведением аудита аудиторская группа должна иметь четко сформулированные задачи, область, критерии аудита, документы различных уровней (политики, процедуры, инструкции, стандарты организации и др.), перечень процессов и активов компании, подлежащих проверке, согласованную программу аудита от проверяемой организации, подтверждение проведения аудита.

Ключевым фактором при подборе экспертов для проведения аудита является то, что они должны быть независимыми от проверяемой организации. В крупных организациях это могут быть специальные сотрудники, занимающиеся аудитом, либо консалтинговые организации, основная деятельность которых, является проведение аудита систем управления информационной безопасностью. В группу аудиторов могут приглашаться технические эксперты, которые будут проверять правильность настройки и функционирования конкретного оборудования и программного обеспечения. [104]

При выборе аудиторов организация должна проверить, что они прошли соответствующую подготовку и имеют навыки, необходимые для проведения аудита. Основные темы, включенные в подготовку аудитора [91]:

- знание и понимание требований информационной безопасности;
- знание методов исследования, опроса, оценивания и отчетности;
- знание методов проведения аудита информационной безопасности;
- дополнительные навыки управления аудитом, такие как планирование, организация, общение с высшим руководством.

Аудиторы должны до проведения предварительной встречи провести анкетный опрос организации. Данная анкета должна выявить основную информацию об организации. На основании результатов, аудиторы оценивают продолжительность и стоимость аудита организации.

После составляется план аудита. Методика составления такого плана состоит из двух шагов: создание плана аудита, утверждение плана аудита. В план аудита включаются процессы и виды деятельности. Кроме того, определяются проверяемые отделы, персонал для проведения опроса.

План аудита должен быть составлен ответственным лицом и утвержден высшим руководством. На совещание с высшим руководством, должны быть обсуждены и утверждены следующие вопросы:

1. Административные, включающие обсуждение и утверждение контактного лица от организации для связи с аудитором до, вовремя и после проверки. Кроме этого должен быть определен комплект документов, который организация должна заранее направить аудиторской группе.

2. Аспекты, касающиеся непосредственно аудита: область аудита, временные рамки аудита, участие сотрудников, план аудита, отчетность, меры, принимаемые по итогам аудита, согласование плана аудита.

После определения с областью сертификации, подготовки всех необходимых документов, внедрения организационных и технических мер, самостоятельно проверили работоспособность СУИБ (провели внутренний аудит). [92]

Аудит документации является первым этапом проверки на соответствие требования. Вначале проверяются документы верхнего уровня: политика информационной безопасности или концепция информационной безопасности, частные политики, стандарты организации. Перечисленные документы должны отражать не только идеологию организации в целом в области информационной безопасности, но и отражать распределение ответственности между сотрудниками и руководством организации. [68]

Аудитор должен поочередно пройти каждое заявленное в программе подразделение и проверить выполнение необходимых требований. В ходе проверки может быть использовано интервьюирование, частичная проверка процесса, проверка с помощью выборки (проверка выполнение в определенные промежутки времени), либо полная проверка всех составляющих процесса.

В процессе аудита важным фактором является сбор фактов и свидетельств, для последующего анализа и отчета. Свидетельство может быть получено посредством наблюдения, измерения, испытания и другими способами. [16]

В ходе аудита должен быть проведен анализ рисков организации. Может быть применен аналитический и инструментальный анализ локальной вычислительной сети и информационных ресурсов организации, с целью выявления угроз и уязвимостей защищаемых активов Проведение консультаций со специалистами организации и оценка соответствия фактического уровня безопасности. Расчет рисков, определение текущего и допустимого уровня риска для каждого конкретного актива. Ранжирование рисков, выбор комплексов мероприятий (контролей) по их снижению и расчет теоретической эффективности внедрения. [114]

После проверки всех бизнес-процессов, заявленных в программе аудита, составляется отчет по выявленным несоответствиям. В нем отражаются все несоответствия. Он детализирован: все собранные факты по каждому процессу или пункту стандарта полностью отражены. Отчет по несоответствиям должен быть тщательно проверен на наличии ошибок и неточностью и по возможности не иметь больших объемов.

Далее составляется комплексный отчет по проведенному аудиту. Он может содержать рекомендации по устранению несоответствий и календарный план работ по улучшению СУИБ.

Завершить аудит рекомендуется заключительном совещанием, на котором подводятся итоги аудита, обсуждаются спорные вопросы, возникшие в ходе проведения проверки, согласовываются сроки устранения замечаний. Важно получить подтверждение понимания необходимости улучшения СУИБ и согласовать сроки начала и завершения работ по устранению несоответствий. [63]

Ниже перечислены варианты (примеры) описания области действия СУИБ:

1. Система управления информационной безопасностью в части обеспечения безопасности процессов разработки программного обеспечения;
2. Система управления информационной безопасностью в части обеспечения безопасности процессов взаимодействия с клиентами в части обработки клиентских данных;
3. Система управления информационной безопасностью в части обеспечения безопасности процессов предоставления услуг по управлению ИТ-инфраструктурой. [46]

После проведения внутреннего аудита, идентификацию ресурсов, определения ценности ресурсов и рисков, организация готовит пакет документов: политики, стандарты, положения, процедуры и т.п.

В процессе внедрения СУИБ требуется разработать объемный пакет документации. На внедрение эффективной СУИБ может уйти от 1-го до 2-х лет. В этом процессе на разработку документации СУИБ может потребоваться от 3 до 9 месяцев. Это огромный, но необходимый объем работы. Неправильно организованный процесс разработки документации может привести к серьезному перерасходу ресурсов и, более того, может снизить до минимума эффект от внедрения СУИБ.

Любой документ в рамках СУИБ является «живым» и должен пересматриваться по мере необходимости, но не менее 1 раза в год. Весь пакет документов, который должен существовать и создаваться в компании, в процессе построения СУИБ и подготовки к сертификации обширен. В каждом конкретном случае и для каждой компании этот перечень будет иметь свои особенности. [55]

Документация СУИБ может иметь любую удобную для организации структуру. Условно можно разделить документацию СУИБ на четыре группы: административные документы, документы верхнего уровня, документы среднего уровня и документы нижнего уровня.

Административные документы являются отправной точкой для внедрения СУИБ. Их разработку и издание осуществляет высшее руководство. С помощью административных документов будет установлена соответствующая организационная структура для управления информационной безопасностью на предприятии. Важнейшим результатом выпуска административных документов

является определение уполномоченное лицо по ИТ-безопасности и наделение его соответствующими полномочиями. С этого момента начинается работа над созданием основной документации самой СУИБ.

Документы верхнего уровня позволяют построить на предприятии основу СУИБ – систему управления рисками, а также реализовать основные управленческие процессы. Любые процессы управления базируются на документации. Управленческие процессы СУИБ не являются исключением. Документы верхнего уровня разрабатываются службой информационной безопасности и являются основой для ее работы.

Документы среднего (технического) уровня помогают реализовать конкретные действия по защите всех важных информационных активов от угроз различного происхождения. Это наиболее объемная часть документации. Именно в этом блоке происходит описание конкретных операций каждого участника СУИБ. В разработке технической документации принимают участие специалисты по ИБ, специалисты отдела кадров, управления ИТ, службы физической защиты, юридический отдел и др. На этом уровне документации решаются вопросы распределения ответственности по каждой операции, устанавливаются сроки, готовятся шаблоны договоров (соглашений) для работы с внутренними и внешними сторонами. Основными пользователями данной группы документов являются руководители подразделений, системные администраторы, ответственные за обеспечение информационной безопасности конкретных активов.

Документы нижнего уровня предназначены для конечных пользователей. Они являются эффективным инструментом для сокращения количества угроз, связанных с человеческим фактором. Как правило документы нижнего уровня являются выжимками из документов технического уровня. При их разработке следует четко понимать для кого они рассчитаны. Стоит отказаться от сложных формулировок и незнакомых терминов.

Таким образом, условное деление всей документации СУИБ на четыре группы позволит заниматься разработкой постепенно, переходя от верхнего уровня до нижнего.

Для определения перечня необходимой документации может использоваться один из трех подходов.

Первый подход – на основе требований стандарта ISO 27001. Алгоритм подготовки перечня базируется на проработке требований стандарта. В первом столбце таблицы перечисляются все требования стандарта. Каждое требование стандарта рассматривается с точки зрения необходимости разработки документов или записей. Во втором столбце таблицы записываются наименования документов и записей, необходимых предприятию для реализации этих требований. После заполнения всех строк во втором столбе

таблице будет сформирован перечень документации СУИБ. Этот подход можно использовать при любом алгоритме внедрения СУИБ.

Второй подход – на основе плана по обработке рисков. Для создания перечня предварительно нужно выполнить трудоемкую цепочку действий: идентифицировать активы, определить угрозы и уязвимости, оценить ущерб и вероятность каждого риска, просчитать риски, ранжировать риски. После этого напротив каждого риска необходимо прописать требуемые меры по обработке риска. Среди этих мер будут встречаться документы и записи. Таким образом сформируется перечень документов СУИБ с учетом уровня рисков. Т.е. для рисков с высоким значением возможно потребуется создать отдельные документы, для нескольких малых рисков можно применить единый краткий документ. Этот подход позволяет создать более точный перечень необходимой документации СУИБ.

Необходимо разработать документы: политика информационной безопасности, методология оценки и обработки рисков, положение о применимости, план устранения рисков, отчет об оценке рисков, процедура управления документами, процедура управления записями, порядок внутреннего аудита и др. [50]

В данной работе автор разработал перечень документов, который является ориентировочным, но в него включены обязательные документы, без которых внедрение СУИБ будет не возможным (Приложение Г)

Приведенный список не является окончательным и может дополняться, и изменяться. Стандарты серии ISO 27000 предполагают, определенную гибкость и позволяет использовать альтернативные документы. Добавления к текущему списку могут производиться с целью повышения уровня информационной безопасности и основываться на требованиях системы СУИБ.

Существуют документы, которые очень часто используются при подготовке и построении СУИБ, но не являются обязательными с точки зрения стандарта: политика использования собственных устройств, мобильное устройство и политика удаленного доступа, политика классификации информации, и др. Эти документы не являются обязательными с точки зрения стандарта, но они регламентируют ряд необходимых мер и действий, при внедрение которых необходимы для построения комплексной системы СУИБ.

Одним из ключевых назначений документов из дополнительного списка, это регламентация внедрения процессов и удобная форма донесения правил и норм до сотрудников компании и до внешних организаций.

Вторым фактором для создания дополнительных документов является необходимость письменного подтверждения проведения работ, требующихся в рамках построения и сопровождения системы СУИБ.

Важно, что основной раздел стандарта является обязательным, а следовательно, все требования должны быть выполнены и разработаны все упомянутые документы.

Типовая структура документов СУИБ, будь то политика или положение о применимости, процедура и т. п., должен содержать:

1. цель создания документа;
2. область действия документа, роли и обязанности задействованных лиц/сторон;
3. ссылки на перекрестные документы;
4. основная часть документа, где содержится суть политики и процедуры;
5. раздел о пересмотре документа, с указанием срока пересмотра;
6. история изменений.

Документ Политика информационной безопасности представляет собой документ, в котором определяются цели, задачи и пути их достижения, принципы. Политика ИБ как правило, является небольшим документом высшего уровня, который описывает основную цель СУИБ. Цели СУИБ обычно могут быть выделены в отдельный документ, но также они могут быть включены в политику информационной безопасности. [52]

Ключевые моменты из выдержки из политики ИБ:

Цель политики - защита информационных ресурсов компании от всех внутренних, внешних, преднамеренных или непреднамеренных угроз.

Основные положения политики ИБ:

1. Политика утверждается руководителем компании единолично или совместно с советом директоров компании;
2. Сотрудник, ответственный за обеспечение ИБ в компании, осуществляет управление процессами информационной безопасности, обеспечивая грамотное управление информационными ресурсами;
3. Для управления информационными ресурсами и СУИБ в компании может быть создан комитет по ИБ, обеспечивающий принятие регламентов и мер обеспечения ИБ коллегиальным способом;
4. Сотрудник, ответственный за ИБ, ежегодно и при появлении существенных изменений проводит анализ существующих политик ИБ с целью обеспечения их постоянной пригодности, адекватности и результативности;
5. Сотрудник, ответственный за ИБ, отвечает за определение детальных требований к системе информационной безопасности и контролирует выполнение этих требований;
6. Доступ к информации и информационным ресурсам компании предоставляется только лицам/сотрудникам, которым этот доступ

необходим для выполнения должностных или договорных обязательств. При этом уровень доступа минимально возможный;

7. Для каждого информационного ресурса компании определен владелец ресурса (сотрудник или подразделение), отвечающий за предоставление доступа к ресурсу и эффективное функционирование мер защиты информации, примененных для защиты ресурса и т.д.

Документированная политика ИБ должна быть утверждена руководством и доведена до сведения всех сотрудников организации и внешних сторон, к которым она относится.

Кроме высокоуровневой политики выделяют низкоуровневые политики (частные политики, подполитики), как правило, отражающие требования в определенной области (домене). В качестве примеров политик низкого уровня можно привести политику управления доступом, политику управления паролями, политику резервного копирования и т.п.

Точный состав частных политик зависит от особенностей организации: ее размера, структуры, корпоративной культуры и т.п.

Стандарт определяет обязательное требование, практику применения какого-либо решения. Примером корпоративного стандарта является, стандарт на конфигурацию серверов под управлением Linux. [2]

Руководства отличаются от стандартов тем, что носят рекомендательный характер. Руководства, в частности, могут определять, как именно следует реализовывать то или иное требование на практике с учётом локальной специфики. Так, например, специалист по информационной безопасности может разработать руководство, описывающее различные алгоритмы генерации надежных паролей, чтобы облегчить задачу выбора пароля пользователю.

Процедура представляют собой документ, определяющий последовательность действий по выполнению какой-либо задачи в соответствии с требованиями политик и стандартов. Из процедуры должно быть ясно, кто, что и когда делает. Хорошим примером процедуры является процедура регистрации пользователей в системе, описывающая этапы согласования заявки на доступ.

Необходимо отметить, что, в основном, упомянутые документы ориентированы на специалистов отделов ИТ/ИБ, руководителей подразделений. Для неподготовленных сотрудников содержание данных документов может быть непонятным. В таких случаях разрабатывается документ «Свод правил для сотрудников», в котором доступным языком без использования технических терминов формулируются требования, которые должны выполнять сотрудники. Также правила по обеспечению ИБ должен быть закреплен в положениях об отделах и должностных инструкциях.

К отдельным видам документов стоит отнести так называемые записи. Записи представляют собой те документы, которые создаются при выполнении процедуры, например, заявка на предоставление доступа к системе, журнал системы контроля доступа с информацией о том, кто входил в серверное помещение и т.п.

Реестр ресурсов – это таблица, содержащая основную информацию обо всех ресурсах, задействованных в бизнес-процессах, которые попадают в область действия СУИБ. Составление такой таблицы необходимо для дальнейшей обработки рисков: выбор методов устранения тех или иных угроз, понижения уровня риска. (Приложение Д)

Методология оценки и обработки рисков, как правило, представляет собой документ объемом от 4 до 5 страниц, который должен быть написан до выполнения процедур оценки и обработки рисков. Отчет об оценке степени риска пишут после того, как выполняются процедуры оценки степени риска и обработки риска. Этот отчет должен суммировать все результаты.

Положение о применимости пишется на основе результатов обработки риска. Это центральный документ в СУИБ, потому что он описывает не только средства, которые будут использоваться для Приложения А, но и то, как они будут реализованы, и их текущий статус. Также можно рассматривать положение о применимости в качестве документа, описывающего профиль безопасности организации.

После подготовки пакет документов и внедрения политики, стандартов, положений и т.п., проводится сертификационный аудит.

Существует два варианта: предварительный аудит и сертификационный и сертификационный.

Сертификационный аудит состоит из двух основных этапов: изучение документации, диалог с сотрудниками, входящими в область действия СУИБ.

Длительность каждого из этапов зависит от размера компании. Зная количество сотрудников компании, можно приблизительно оценить, сколько времени займет вся эта процедура [55]:

для организации с численностью меньше чем 10 сотрудников – до 4 месяцев;

- для организации с численностью 10–50 сотрудников – до 8 месяцев;
- для организации с численностью 50–500 сотрудников – до 12 месяцев;
- для организации с численностью 500 или больше сотрудников – до 18 месяцев.

Документы по обеспечению ИБ должны быть написаны максимально простым языком, чтобы их требования могли понимать и исполнять люди, не занятые в защиты информации. Чем проще и точнее будут описаны процессы защиты, тем проще будет пройти организации сертификационный аудит.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования была достигнута цель посредством решения поставленных задач.

1. Внедрение политики ИБ требует регламентации практически всех процессов при обработке, хранения, передачи информации в электронный архив, а также разработки документированных процедур и инструкций. В этой связи целесообразно использовать имеющиеся стандартные методологии для повышения качества подготавливаемых документов.

Как показывает практика, организационные меры играют важную роль во внедрении мероприятий политики ИБ в организации, поэтому необходимо организовать непрерывное, повышения квалификации и обучения сотрудников организации в области ИБ.

Для решения проблемы обеспечения информационной безопасности электронных архивов, необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Правовое обеспечение информационной безопасности в Республике Беларусь включает в себя комплекс норм, содержащихся в различных актах. Однако нельзя говорить о существующем совершенстве законодательства. Очевидно, что нормирование отдельных областей реализуется, как правило, не в единой системе и, как следствие, не взаимосвязано. Это приводит к несогласованности норм, и может привести к беспорядку и появлению новых рисков в сфере информационной безопасности.

Многими исследователями предлагаются различные меры по совершенствованию данного законодательства, в том числе выдвигаются идеи о выделении информационной безопасности в качестве подотрасли информационного права, и создания отраслевого стратегического документа, который регулировал основы государственной политики в сфере информационной безопасности.

На взгляд автора исследования, эти предложения являются оправданными. Такой документ комплексно урегулировал бы данную сферу отношений.

2. Анализируя принятые стандарты по информационной безопасности в Республике Беларусь, можно сказать, что они отвечают европейским требованиям. Но существует ряд проблем при переводе международных стандартов. Встречаются ошибки и двусмысленность терминологии, что приводит к несогласованности и разобщенности языка и понимания, что приводит к разногласию в организации.

Из серии стандартов ИСО 27000 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности» выделяются два взаимосвязанных и основных стандарта ISO 27001 и ISO 27002.

Стандарт ISO 27001 представляет СУИБ. Стандарт ISO 27002, представляет руководящие принципы по реализации средств управления.

Оба стандарта позволяют создать меры по обеспечению информационной безопасности электронных архивов

В Республике Беларусь проводится самостоятельная разработка и совершенствование стандартов по менеджменту информационной безопасности, примером может служить разработка серии стандартов в НИИ прикладных проблем математики и информатики БГУ в области криптографической защиты информации.

Разработка отечественных стандартов способствует более эффективному техническому регулированию на государственном уровне и позволяет регулировать расхождения с законодательством.

3. Современная СУИБ представляет собой процессно-ориентированную систему управления, включающую организационный, документальный и программно-аппаратный компоненты.

Самым трудоемким и сложным этапом на пути к сертификации является собственно создание системы управления ИБ и внедрение ее механизмов в организации.

Для получения объективных качественных и количественных оценок текущего состояния информационной безопасности предприятия в соответствии с определенными критериями и показателями безопасности проводится аудит.

Для представления алгоритма выполнения аудита в работе была разработана нотация класса workflow. Данная нотация используется для представления алгоритма выполнения процесса (аудита) (Приложение В)

В ней отображается: алгоритм выполнения бизнес-процесса, участники бизнес-процесса и их взаимодействие между, движение документов.

Преимуществом данного подхода является в простоте и наглядности. Использование этой схемы не требует специальных знаний, т.к. легко воспринимается сотрудниками с разным уровнем подготовки. Недостаток – это некоторая субъективность в детализации операций.

4. Немаловажной частью для создания СУИБ является создание документов. Документы по обеспечению ИБ должны быть написаны максимально простым языком, чтобы их требования могли понимать и исполнять люди, не занятые в защиты информации. Чем проще и точнее будут описаны процессы защиты, тем проще будет пройти организации сертификационный аудит.

Документация СУИБ может иметь любую удобную для организации структуру. Условно можно разделить документацию СУИБ на четыре группы: административные документы, документы верхнего уровня, документы среднего уровня и документы нижнего уровня. Условное деление всей документации СУИБ на четыре группы позволит заниматься разработкой постепенно, переходя от верхнего уровня до нижнего.

Документы по обеспечению ИБ должны быть написаны максимально простым языком, чтобы их требования могли понимать и исполнять люди, не занятые в защиты информации. Чем проще и точнее будут описаны процессы защиты, тем проще будет пройти организации сертификационный аудит

В работе был разработан перечень основных документов, которые нужно для проектирования, реализации и сопровождения СУИБ (Приложение Г).

Приведенный список не является окончательным и может дополняться и изменяться. Стандарты серии ISO 27000 предполагают, определенную гибкость и позволяет использовать альтернативные документы. Добавления к текущему списку могут производиться с целью повышения уровня информационной безопасности и основываться на требованиях системы СУИБ.

В заключение следует подчеркнуть: правильно распланированный процесс построения СУИБ пройдет намного легче и быстрее. Главное – чтобы все участники процесса понимали важность своих задач и несли ответственность за их выполнение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Bjorn, A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems – Model-based Risk Analysis Targeting Security / A.G. Bjorn // [Электронный ресурс]. – Режим доступа: www.nr.no/coras. – Дата доступа: 10.03. 2019.
2. CIS Security Benchmarks. Center for Internet Security, 2014., 2005.// [Электронный ресурс]. – Режим доступа: https://benchmarks.cisecurity.org/downloads/. – Дата доступа: 10.03. 2019.
3. Dirk, P. Catalogue of Risks / P. Dirk. – Natural, Technical, Social and Health Risks. – Springer, 2007. – 314 p.
4. ISO/IEC 27003:2017 Information technology – Security techniques – Information security management system – Guidance [Электронный ресурс]. – 2017. – Режим доступа: http://www.iso27001security.com/html/27003.html – Дата доступа: 02.04.2019.
5. ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27004.html – Дата доступа: 02.04.2019.
6. ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27007.html – Дата доступа: 02.04.2019.
7. ISO/IEC 27011:2016 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27011.html – Дата доступа: 02.04.2019.
8. ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communications technology readiness for business continuity [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27031.html – Дата доступа: 02.04.2019.
9. ISO/IEC 27033:2010 Information technology – Security techniques – Network security [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27033.html – Дата доступа: 02.04.2019.
10. ISO/IEC 27034:2011 Information technology – Security techniques – Application security [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27034.html – Дата доступа: 02.04.2019.
11. ISO/IEC 27035:2016 Information technology – Security techniques – Information security incident management [Электронный ресурс]. – Режим

доступа: http://www.iso27001security.com/html/27035.html – Дата доступа: 02.04.2019.

12. ISO/IEC TR 27008:2011 Information technology – Security techniques – Guidelines for auditors on information security controls [Электронный ресурс]. – Режим доступа: http://www.iso27001security.com/html/27008.html – Дата доступа: 02.04.2019.

13. IT-Grundschutz Catalogues. Bundesamt für Sicherheit in der Informationstechnik, 2005 // [Электронный ресурс]. – Режим доступа: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html. – Дата доступа: 10.03. 2019.

14. Robertson D.S. The information revolution // Communication research. – N.Y., 1990. – vol. 17. – № 2

15. Абламейко, М.С. Правовое обеспечение информационной безопасности при формировании информационного общества в Республике Беларусь / М.С. Абламейко, Д.А. Марушко // Весці Нацыянальнай Акадэміі Навук Беларусі. Серыя гуманітарных навук. – 2011. - № 4. – С. 39-45.

16. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). С. 37-41.

17. Барабин, В.В. Военно-политическая деятельность государства в системе национальной безопасности / В. В. Барабин. – М.: Изд-во МО РФ, 1998. – 124 с.

18. Бачило, И.Л., Лопатин В.Н., Федотов М.А. Информационное право / Под ред. акад. РАНБ.Н. 2-е изд., с изм. и доп. – СПб.: Юридический центр Пресс, 2005. – 725 с.

19. Безопасность. Информационный сборник фонда национальной и международной безопасности. / ИСТИНА.: М, 1994. – № 3 (19). – С. 91.

20. Блинов, А.М. Информационная безопасност / А.М. Блинов – СПб.: СПбГУЭФ, 2010. – 96 с.

21. Ващекин, Н.П. Безопасность и устойчивое развитие России / Н. П. Ващекин, М. И. Дэлиев, А. Д. Урсул. – М.: ИНФРА-М, 1998. – 112 с.

22. Веруш, А.И. Национальная безопасность Республики Беларусь / А.И. Веруш. – Минск: Амалфея, 2012. – 204 с.

23. Гайкович, В.Ю., Ершов, Д.В. Основы безопасности информационных технологий. / В.Ю. Гайкович, Д.В. Ершов // Сайт Киевского государственного университета информационно-коммуникационных технологий. [Электронный ресурс]. – 2007. – Режим доступа: http://kiskiev.narod.ru/M_Ref2.htm. – Дата доступа: 10.03.2019.

24. Гальперина, М.С., Анализ некоторых методов оценки рисков информационной безопасности / М.С. Гальперина // Молодежный научно-

технический вестник [Электронный ресурс]. – 2004. – Режим доступа: www.sntbul.bmstu.ru/file/out/627960. – Дата доступа: 10.03.2019.

25. Гармаш, В.Н. Американский архивный журнал "The Record" / В.Н. Гармаш // Отеч. архивы. – 1998. – № 1.– С. 99-103.

26. Глобальное исследование утечек конфиденциальной информации в I полугодии 2017 года. // [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016_half_year.pdf. – Дата доступа: 01.04.2019.

27. Глущенко, В. В. Введение в кризисологию. Финансовая кризисология. Антикризисное управление / В. В. Глущенко. – М.: ИП, 2008. – 88 с.

28. Городов, О.А. Информационное право / О.А. Городов. – М.: Проспект, 2009. – 256 с.

29. Государственная Программа «Электронная Беларусь», 27 декабря 2002 г., № 1819 // [Электронный ресурс]. – Режим доступа: https://nces.by/wp-content/uploads/progr-elektr-belarus.pdf. – Дата доступа: 01.04.2019.

30. Гражданский кодекс Республики Беларусь, 7 декабря 1998 г., № 218-З // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019

31. Гришанова Е.М., Артамонова Я.С., Чиликин И.А. Информационная безопасность и информационные коммуникации / Е.М. Гришанова, Я.С. Артамонова, И.А. Чиликин // T-Comm - Телекоммуникации и Транспорт. – 2012. – №2. – С. 14-16.

32. Джаматова Д., Агзамова С. Обзор и сравнение семейства стандартов информационной безопасности ISO 27000 / Д.Джаматова, С.Агзамова // Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения [Электронный ресурс]. – Режим доступа: http://www.unicon.uz/www/2015/sbornik.pdf. – Дата доступа: 02.04.2019.

33. Доктрина информационной безопасности Российской Федерации: утв. Президентом Российской Федерации, 9 сентября 2005 г., № Пр-1895 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

34. Доля, А. Внутренние ИТ-угрозы в России 2006 / А. Доля // Компьютер-пресс. – 2007. – Май. – С. 180-184.

35. Дорофеев, А.В. Марков А.С. Менеджмент информационной безопасности: основные концепции / А.В. Дорофеев, А.С. Марков // Вопросы кибербезопасности. – 2014. – № 1(2). – С.67-73.

36. Дорофеев, А.В., Шахалов, И.Ю. Основы управления информационной безопасностью современной организации / А.В. Дорофеев, И.Ю. Шахалов // Правовая информатика. – 2013. – № 3. – С.35-43.

37. Ермошкин, Г.Н. Анализ существующих моделей оценки рисков ИБ для частных облачных сред / Г.Н. Ермошкин // Методы и системы защиты информации, информационная безопасность. Сер.: Естественные и технические науки. – 2012. - № 6/7. – С. 22-30.

38. Жук О.Ю. Нормативно-правовое обеспечение информационной безопасности в системах электронного документооборота // Управление в социальных и экономических системах: материалы междунар. науч.-практ. конф., Минск, 30-31 мая 2009 г. / Минский институт управления; редкол.: Н.В.Суша [и др.]. – Минск, 2009. – С. 337-380.

39. Жук О.Ю. Обеспечение защиты электронных документов при архивном хранении // Мінулае і сучаснасць: архівы ў сістэме гуманітарных ведаў: матэрыялы Міжнар. навук. канф., прысвеч. 100-годдзю Віцебскай вучонай архіўнай камісіі (Мінск, 20 мая 2009 года) / рэдкал.: Н.М. Дзятчык, С.У. Жумар, В.С. Пазднякоў. – Мінск : БелНДІДАС, 2010. – С. 276-280.

40. Жук, О.Ю. Аудит информационной безопасности в системах электронного документооборота / О. Жук // Архивы и делопроизводство. 2008. № 3. С. 123–127

41. Защита информации. Основные термины и определения: СТБ ГОСТ Р 50922-2000 – Введ. 01.01.01. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2000. – 6 с.

42. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель: СТБ 34.101.1-2014 – Введ. 01.09.14. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2014. – 53 с.

43. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности: СТБ 34.101.2-2014 – Введ. 01.09.14. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2014. – 178 с.

44. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 3. Гарантийные требования безопасности: СТБ 34.101.3-2014 – Введ. 01.09.14. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2014. – 131 с.

45. Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Типовая программа и методика испытаний: СТБ 34.101.15-2007 – Введ. 01.11.07. – Минск: Межгос. совет по

стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2007. – 36 с.

46. Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности: СТБ ISO/IEC 27006-2014 – Введ. 01.02.15. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2014. – 44 с.

47. Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности: СТБ ISO/IEC 27002-2012 – Введ. 01.01.13. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2012. – 85 с.

48. Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности: СТБ ISO/IEC 27005-2012 – Введ. 01.01.13. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2013. – 68 с.

49. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь: СТБ ISO/IEC 27000-2012. – Введ. 01.01.13. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2012. – 17 с.

50. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: СТБ ISO/IEC 27001-2011 – Введ. 01.01.12. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус, гос. ин-т стандартизации и сертификации, 2011. – 27 с.

51. Кабочкина Т.С. Федеральные центры документации США. История, современный опыт // Отеч. архивы. – 1997. – № 6. – С. 92-100.

52. Как написать концепцию информационной безопасности предприятия // Сетевые решения [Электронный ресурс]. – Режим доступа: http://www.nestor.minsk.by/sr/2006/07/sr60713.html. – Дата доступа: 10.03.2019.

53. Кастельс, М. Информационная эпоха, общество и культура / М. Кастельс – М.: ГУ ВЩЭ, 2000. – 608 с.

54. Кодекс Республики Беларусь об административных правонарушениях, 21 апреля 2003 г., № 194-З // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

55. Колобова, А. ISO 27001: какой путь лучше? / А. Колобова // IT-Manager №2 2015 г. [Электронный ресурс]. – Режим доступа: http://allcio.ru/download/pdf/itmanager/135/70-74.pdf. – Дата доступа: 10.03.2019.

56. Компания «ИнфоОборона» и ОСАО «Ингосстрах» представляют новый продукт: страхование информационных рисков // [Электронный ресурс]. – Режим доступа: http: //www.infooborona.ru/folder55.html. – Дата доступа: 01.04.2019.

57. Конституция Республики Беларусь 1994 года: с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 года и 17 октября 2004 года. – 4-е изд., стер. – Минск: Нац. Центр правовой информ. Респ. Беларусь, 2010 г. – 64 с.

58. Костомаров, М.Н. Управление информационными ресурсами за рубежом / М.Н. Костомаров, РГГУ. – М., 1997. – 87 с.

59. Кубарев, А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков / А.В. Кубарев // [Электронный ресурс] – Режим доступа: http://cyberleninka.ru/article/n/podhod-k-formalizatsii-uyazvimostey-informatsionnyh-sistem-na-osnove-ih-klassifikatsionnyh-priznakov.pdf. – Дата доступа: 01.03. 2019.

60. Курило, А.П. Аудит информационной безопасности / А.П. Курило – М.: БДЦ-пресс, 2006. – 304 с.

61. Лазовский, С.В. Понятие информационной безопасности государства и ее место в правовой системе Республики Беларусь / Лазовский С.В. // Юридический журнал. - 2008. – № 3. – С. 70-73.

62. Левченко Л.Л. Обеспечение сохранности электронных документов в Национальном архиве Соединенных Штатов Америки // Вестник архивиста, 2013 [Электронный ресурс]. – Режим доступа: http://www.vestarchive.ru/elektronnye-dokymenty/2218-obespechenie-sohrannosti-elektronnyh-dokymentov-v-nacionalnom-arhive-soedinennyh-shtatov-ameriki.html – Дата доступа: 10.03. 2019.

63. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet / А.С. Марков, А.А. Фадин // Вопросы кибербезопасности. 2013. – № 1(1). – С. 28-36.

64. Марков, А. А. Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе / А. А. Марков // Вестник Волгоградского государственного университета. 2010. – № 1. – С.123-129.

65. Марков, А.С., Цирлов, В.Л. Управление рисками – нормативный вакуум информационной безопасности / А.С. Марков, В.Л. Цирлов // Открытые системы. СУБД. – 2007. – № 8. – С. 63-67.

66. Медведовский И.Д. Современные методы и средства анализа и контроля рисков информационных систем компаний / И. Д. Медведовский //

[Электронный ресурс]. – Режим доступа: http://www.bugtraq.ru/library/security/itrisk.html. – Дата доступа: 10.03.2017.

67. Михайлов, О.А. Электронные документы в архивах. Проблемы приема. Обеспечение сохранности и использование. Аналитический обзор зарубежного и отечественного опыта / О.А. Михайлов. – 2-е изд., доп. – М.: Диалог МГУ (ФАС России, РОИА, РГАНТД), 2000. – 325 с.

68. Найханова, И.В. Аудит систем менеджмента качества и информационной безопасности / И.В. Найханова // Вестник Московского государственного технического университета им. Н.Э. Баумана. – 2011. № SPEC. – С. 152-156.

69. Налоговый кодекс Республики Беларусь (общая часть), 19 декабря 2002 г., № 166-З // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

70. Национальная безопасность Республики Беларусь / С. В. Зась [и др.]; под ред. М.В. Мясниковича и Л.С. Мальцева. – Минск: Беларус. навука, 2011. – 557 с.

71. Нестеркина, Е. Методы реализации стандартной стратегии рисков облачных вычислений / Е. Нестеркина // ЦОД, датацентры, облачные вычисления, Saas, 2013 [Электронный ресурс]. – Режим доступа: http://dcnt.ru/?p=10700. – Дата доступа: 10.03. 2019.

72. НИИ прикладных проблем математики и информатики БГУ Что дальше [Электронный ресурс]. – 2017. – Режим доступа: http://apmi.bsu.by/blog/cryptology/todo.html – Дата доступа: 02.04.2019.

73. Носаков, В. Подходы компании "Инфосистемы Джет" к информационной безопасности / В. Носаков // Jet Info №7. 2006 г [Электронный ресурс]. – Режим доступа: http://www.jetinfo.ru/jetinfo_arhiv/podkhody-kompanii-infosistemy-dzhet-k-informatsionnoj-bezopasnosti/sozdanie-kompleksnoj-sistemy-upravleniya-informatsionnoj-bezopasnostyu/2006. – Дата доступа: 10.03. 2019.

74. Носевич, В.Л. Доказательная сила архивного электронного документа / В.Л. Носевич // Архівы і справаводства. – 2018. – №3 (117). – С. 68–73.

75. Носевич, В.Л. Информационные технологии в архивной службе / В.Л. Носевич // [Электронный ресурс]. – Режим доступа: http://inf.grid.by/jour/article/download/43/45. – Дата доступа: 10.03.2017.

76. Носевич, В.Л. Как будет происходить комплектование государственных архивов электронными документами / В.Л. Носевич // Архівы і справаводства. – 2018. – №2 (116). – С. 47–56.

77. Носевич, В.Л. Как обеспечить хранение электронных документов организации / В.Л. Носевич // Архівы і справаводства. – 2018. – №4 (118). – С. 73–78.

78. О внедрении ГОСТ ИСО/МЭК 17799 и 27001 / А.С.Марков, С.А.Леденко и др. // Information Security – 2006 – №3/4.

79. О гармонизации законодательства государств-участников СНГ в области информатизации и связи: Постановление межпарламентской Ассамблеи государств-участников Содружества Незасисимых государств в области информатизации и связи, 18 ноября 2005 г., № 26-7 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

80. О мерах по совершенствованию использования национального сегмента сети Интернет: Указ Президента Республики Беларусь, 1 февраля 2010 г., № 60 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

81. О модельном законе «О безопасности»: Постановление Межпарламентского Комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан, 15 октября 67 1999 г., № 9-9 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

82. О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192: Постановление Совета Министров Республики Беларусь, 29 апреля 2010 г., № 645 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

83. О некоторых вопросах развития информационного общества в Республике Беларусь: Указ Президента Республики Беларусь, 8 ноября 2011 г., № 515 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

84. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации: Указ Президента Республики Беларусь, 25 октября 2011 г., № 486 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

85. О некоторых мерах по совершенствованию защиты информации: Указ Президента Республики Беларусь, 16 апреля 2013 г., № 196 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

86. Об информации, информатизации и защите информации: Закон Республики Беларусь, 10 ноября 2008 г., № 455-З // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

87. Об утверждении Инструкции об организации системы внутреннего контроля в банках, небанковских кредитно-финансовых организациях, банковских группах и банковских холдингах: Постановление Правления Национального банка Республики Беларусь, 30 ноября 2012 г., № 625 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

88. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Республики Беларусь, 9 ноября 2010 г., № 575 // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

89. Об электронном документе и электронной цифровой подписи: Закон Республики Беларусь, 28 декабря 2009 г., № 113-З // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

90. Общие сведения о международном стандарте ISO 15408 [Электронный ресурс]. – 2017. – Режим доступа: http://iso27000.ru/standarty/iso-15408-obschie-kriterii-ocenki-bezopasnosti-informacionnyh-tehnologii/obschie-kriterii-ocenki-bezopasnosti-informacionnyh-tehnologii – Дата доступа: 02.04.2017.

91. Остапова, В. В. Международные стандарты аудита / В. В. Остапова, З.В. Богинская. – Ростов н/Д.: Феникс, 2006. – 191 с.

92. Пастоев, А. Методологии управления ИТ-рисками / А. Пастоев. // [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/metodologii-upravleniya-it-riskami. – Дата доступа: 10.03.2019.

93. Перечень нормативной документации в области информационной безопасности [Электронный ресурс]. – 2017. – Режим доступа: http://itsec.by/perechen-normativnoj-dokumentacii-v-oblasti-informacionnoj-bezopasnosti-po-sostoyaniyu-na-01-10-2014 – Дата доступа: 02.04.2019.

94. Петренко, С.А., Курбатов, В.А. Политики информационной безопасности / С.А. Петренко, В.А. Курбатов. – М: ДМК Пресс, 2011. – 396 с.

95. Разумников С.В. Анализ возможности применения методов octave, riskwatch, cramm для оценки рисков ИТ для облачных сервисов / С.В. Разумников // Современные проблемы науки и образования. [Электронный ресурс]. – 2014. – № 1. – Режим доступа: http://www.science-education.ru/ru/article/view?id=12197. – Дата доступа: 02.04.2019.

96. Романец, Ю.В., Тимофеев, П.А. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев. – М.: Радио и связь, 2001. – С. 13-16.

97. Рыбаков, А.Е. «Принять предложение трудового коллектива…» / А.Е. Рыбаков // [Электронный ресурс]. – Режим доступа:

http://belniidad.by/sites/default/files/rybakou_-_belniidad_20.pdf. – Дата доступа: 10.03.2017.

98. Рысков, О.И. Об основных направлениях деятельности зарубежных архивных органов в области исследования и нормативного регулирования работы с электронными документами / О. И. Рысков // Секретарское дело. – 2005. - № 3. – С. 75-85.

99. Советский энциклопедический словарь / Гл. Ред. А.М. Прохоров. – 4-изд. – М.: СЭ, 1988. – 1600 с.

100. Соглашение между Правительством Республики Беларусь и Правительством Республики Казахстан о сотрудничестве в области защиты информации // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

101. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности, 20 ноября 2013 г. // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

102. Соколов, М.С. Информационная безопасность. К вопросу о содержании понятия «информационная безопасность» / М.С. Соколов // Закон и право. – 2011. – № 5. – С. 9-14.

103. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2013 г. / Матвеев В.А., Медведев Н.В., Троицкий И.И., Цирлов В.Л. // Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. – 2013. – Спец. вып. – С. 3-6.

104. Статистика управление по раскрытию преступлений в сфере высоких технологий. // [Электронный ресурс]. – Режим доступа: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/stastistika-urpsvt. – Дата доступа: 01.04.2019.

105. Теоретические и прикладные проблемы информационной безопасности: тез. докл. Междунар. науч.-практ. конф. (Минск, 21 июня 2012 г.) / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск: Акад. МВД, 2012. – 331 с.

106. Тепляков, А.А., Гваева, И.В., Орлов, А.В. Обеспечение безопасности и надежности информационных систем / А.А. Тепляков, И.В. Гваева, А.В. Орлов. – Минск: Акад. упр. При Президенте Респ. Бел., 2007. – С.20.

107. Типовой закон ЮНСИТРАЛ о международной коммерческой согласительной процедуре. // [Электронный ресурс]. – Режим доступа: https://www.uncitral.org/pdf/russian/texts/arbitration/ml-conc/03-90955_Ebook.pdf. – Дата доступа: 01.04.2019.

108. Тихонов, В.И. Обеспечение сохранности электронных документов / В.И. Тихонов //Вестник архивиста. – 2005. – №. 5-6. С 211-212, 225-226

109. Трудовой кодекс Республики Беларусь, 26 июля 1999 г., № 296-З // Эталон-Беларусь [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. – Минск, 2019.

110. Уголовный кодекс Российской Федерации, 13 июня 1996 г., № 63-ФЗ // Консультант Плюс: Версия Проф. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр». – М., 2019.

111. Уолрэнд, Дж. Телекоммуникационные и компьютерные сети. / Дж. Уолренд. – М.: Постмаркет, 2001. – С. 358.

112. Управление рисками. Метод CRAMM // [Электронный ресурс]. – 2015. – Режим доступа: http://www.itexpert.ru/rus/ITEMS/77-33/. – Дата доступа: 10.03.2019.

113. Утвержден новый государственный стандарт на управление документами // [Электронный ресурс]. – Режим доступа: http://belniidad.by/content/utverzhden-novyi-gosudarstvennyi-standart-na-upravlenie-dokumentami. – Дата доступа: 01.04.2019.

114. Хорев А.А. Магистерская программа подготовки «Аудит информационной безопасности автоматизированных систем» // [Электронный ресурс]. – Режим доступа: http://bit.mephi.ru/wp-content/uploads/bit_3_2011_13.pdf. – Дата доступа: 01.04.2019.

115. Чурко, О.В. Некоторые вопросы информационной безопасности в Беларуси в современных экономических условиях / О.В. Чурко // Управление защитой информации. – 2007. - № 2, Том 11. – С. 219-227.

116. Ларин, М.В., Рысков, О.И. Электронные документы в управлении. Методическое пособие. ВНИИДАД. М., - 2008. - 206 с.

ПРИЛОЖЕНИЕ А

Статистические данные МВД за 2019 год

ПРИЛОЖЕНИЕ Б

Чек-лист для определения области деятельности СУИБ компании[3]

№ п/п	Название бизнес-процесса	Краткое описание	Участники бизнес-процесса	Какие информационные системы	Какого рода информация обрабатывается в	На основе какой нормативной и законодательной базы работает	Критичность с точки зрения ИБ	Важность процесса с точки зрения

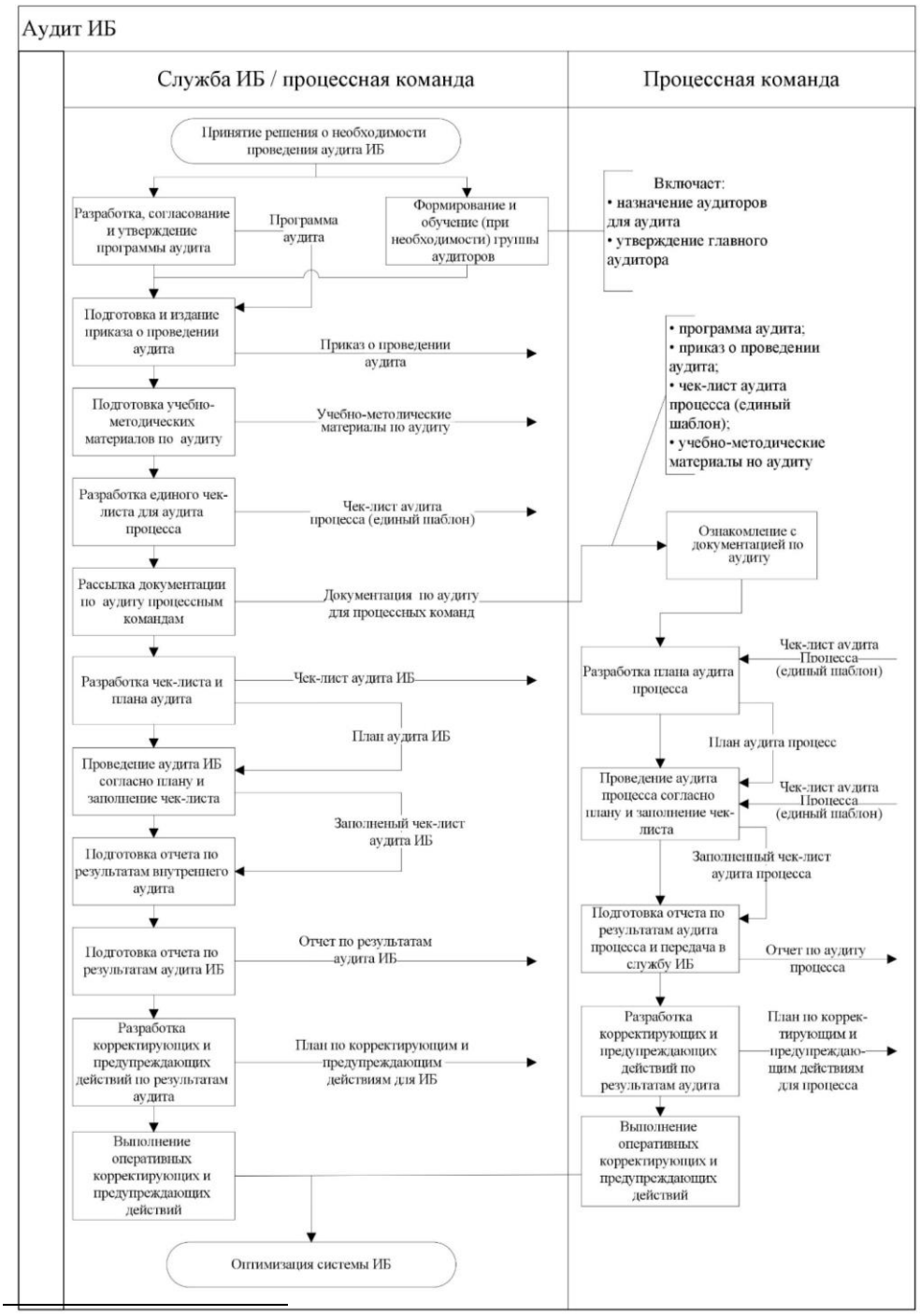
* где:
1 – высокая
2 – средняя
3 – низкая
4 – не влияет на процесс

** где:
1 – важен
2 – маловажен
3 – не важен

[3] разработка автора

ПРИЛОЖЕНИЕ В

Нотация для представления алгоритма выполнения аудита СУИБ[4]



[4] разработка автора

ПРИЛОЖЕНИЕ Г

Рекомендации по перечню документов [5]

Этот перечень является ориентировочным, но в нем включены обязательные документы без которых внедрение СУИБ будет не возможным.

№	Документ	Ссылка	Примечание
Управление документацией			
1.	Процедура управления документацией	7.5.2, 7.5.3, A.5.1.2, A.8.2.2, A.18.1.3	Если в организации уже разработаны требования по управлению документацией (определены места хранения, ответственные, правила по пересмотру, разработке, наименованию, содержанию, оформлению и д.р.). В таком случае разрабатывать и документировать отдельную процедуру по разработке документов СУИБ не требуется. Следует проверить существующие документы на соответствии стандартам ISO (например, по ответственным), если часть из них отсутствует, то можно их задокументировать в «Политике управления ИБ» (см. п. 5). Рекомендуется создать краткую памятку, по управлению документацией СУИБ.
2.	Памятка по разработке и пересмотру документов СУИБ	7.5.2, 7.5.3, A.5.1.2	
3.	Комплект шаблонов типовых документов СУИБ	см.27003	Политики/положения, процедуры/регламенты, инструкции, отчеты, журналы учета и пр.
4.	Перечень документов СУИБ	7.5.3	Рабочий (регулярно обновляемый) документ в виде таблицы. В нем помимо наименования документов указывается дату утверждения документа, ответственного за пересмотр, дату последнего пересмотра. Отдельной таблицей рекомендуется вести перечень «записей» (приказов, протоколов, актов, отчетов и д.р.)

[5] разработка автора

Управление ИБ			
5.	Область действия СУИБ	4.3	В данном документе нельзя забывать указать основные бизнес процессы (вспомогательные процессы, информационные активы, информационные системы и д.р.). Желательно написать обоснование выбора данной области действия СУИБ. Уровень детализации документа определяется самостоятельно. Обычно 5-10 страниц текста. Основные процессы удобно описывать в нотации.
6.	Декларация ИБ	5.1, 5.2, A.5.1.1	Декларация – это документ, показывающий приверженность руководства. Обычно короткий (1 страница текста) и публичный (общедоступный) документ. Политика является сборником положений по управлению ИБ, обычно 20--- 30 страниц текста.
7.	Политика управления ИБ	5.1, 5.2, 6.2, A.5.1.1, A.6.1.5, A.18.1.2	
Управление рисками			
8.	Процедура управления рисками ИБ	6.1.2, 8.2	
9.	Методика оценки Рисков ИБ	6.1.2, A.8.2.1, A.11.1.4	Желательно дополнить методикой инвентаризации активов и положениями о критериях принятия рисков.
10.	Реестр активов (информационных)	A.8.1.1, A.8.1.2	
11.	Отчет об оценке рисков ИБ	6.1.3 f, 8.2, A.8.1.1, A.8.2.1,	Помимо формальной оценки рисков необходимо провести совещание/согласование допустимого уровня риска (остаточных рисков). Итоговый отчет должен содержать упоминание владельцев рисков.

12.	Положение о применимости мер контроля	6.1.3 d	
13.	План обработки рисков	6.1.1, 6.1.3 e, 8.3	
Внутренний аудит			
14.	Отчет (ы) о проведении внутреннего аудита	9.2	

ПРИЛОЖЕНИЕ Д

Реестр ресурсов[6]

№ п/п	Тип ресурса	Владелец ресурса	Пользователь ресурса	К	Ц	Д
	Информация					
	Оборудование (компьютерное, прикладное, сетевое)					
	Программное обеспечение					
	Сервисы (внутренние, внешние)					
	Персонал					
	Помещения					

где:

К - конфиденциальность;

Ц - целостность;

Д - доступность.

К, Ц, Д - свойства информации, которые важны для каждого типа ресурса с точки зрения информационной безопасности. Проставляются знаками «+» и «-» (как вариант можно ставить 1 или 0).

[6] разработка автора