Министерство образования Республики Беларусь

Учреждение образования
«Полоцкий государственный университет»

К. Я. Раханов, Н. А. Раханова

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Рекомендовано учебно-методическим объединением по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-40 80 04 «Информатика и технологии программирования»

Новополоцк
Полоцкий государственный университет
2021

УДК 004.738.5.056(075.8)
ББК 32.971.35-018.2я73
Р27

Одобрено и рекомендовано к изданию методической комиссией
факультета информационных технологий (протокол № 1 от 28.01.2020)

Кафедра вычислительных систем и сетей

РЕЦЕНЗЕНТЫ:
проф., д-р техн. наук, зав. каф. защиты информации
Белорусского государственного университета информатики и радиоэлектроники
Т. В. БОРБОТЬКО;
проф., д-р техн. наук, зав. каф. высшей математики
Военной академии Республики Беларусь
В. А. ЛИПНИЦКИЙ;
проф., д-р техн. наук, почетный профессор БГУИР
Л. М. ЛЫНЬКОВ

Раханов, К. Я.

Р27 Обеспечение конфиденциальности информации в сети Интернет : пособие / К. Я. Раханов, Н. А. Раханова. – Новополоцк : Полоц. гос. ун-т, 2021. – 192 с.

ISBN 978-985-531-723-5.

Пособие представляет собой системное изложение правовых, организационных и технических мер по защите конфиденциальной информации в сети Интернет. Изложена структура информации ограниченного доступа. Раскрываются основные принципы реализации технических мер защиты информации ограниченного распространения. Уделено пристальное внимание процедурам выстраивания системы защиты информации и ее аттестации. Содержится развернутый анализ актуальных методов социальной инженерии и проблем формирования информационной культуры организации. Материал основан на широком массиве нормативных правовых актов Республики Беларусь.

Предназначено для магистрантов специальности «Информатика и технологии программирования», студентов и преподавателей, а также руководителей организаций, специалистов по информационной безопасности и всех, кто интересуется вопросами защиты конфиденциальной информации в сети Интернет.

УДК 004.738.5.056(075.8)
ББК 32.971.35-018.2я73

ISBN 978-985-531-723-5

Содержание

ОТ АВТОРОВ

Благодарим многих людей, помогавших и поддерживавших нас при подготовке и издании пособия.

Рецензентов Борботько Тимофея Валентиновича, Липницкого Валерия Антоновича, Лынькова Леонида Михайловича за содержательные комментарии и рекомендации.

Заведующего кафедрой вычислительных систем и сетей Полоцкого государственного университета Богуша Рихарда Петровича за идею курса, а также за терпение и настойчивость.

Редактора Дарьянову Татьяну Александровну за тщательную и быструю техническую обработку текста.

Самую искреннюю признательность выражаем нашим наставникам в науке: Железняку Владимиру Кирилловичу, открывшему путь в ученый мир одному из авторов пособия, а также за поистине отеческую заботу и поддержку во всех начинаниях; Василевичу Григорию Алексеевичу за веру в творческий потенциал, готовность поддерживать в самых непростых условиях и доброе человеческое отношение.

ВВЕДЕНИЕ

В условиях постоянного роста количества пользователей сети Интернет (на ноябрь 2019 г. во всем мире их число достигло 4,1 млрд человек, что составляет 53% населения планеты [1]) глобальная сеть становится все более удобным и бюджетным средством передачи и распространения информации. Набирает обороты электронная торговля, организации все больше стремятся к предоставлению общедоступных услуг в реальном времени. Кроме того, новые технологии предоставляют работникам широкие возможности для удаленной трудовой деятельности, что требует использования средств дистанционного доступа к сетям организаций, а также к информации и услугам, связанным с поддержкой основной деятельности организаций.

Интенсивное развитие сети Интернет способствует тому, что информационные ресурсы становятся приоритетным объектом преступлений и киберинцидентов, подвергаются похищению, модификации, уничтожению, блокированию и другим воздействиям. Множественные угрозы и риски незаконного и необоснованного вмешательства в частную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и избыточное профилирование сужают личное пространство человека и нарушают его приватность. Формируется нелегальный рынок баз и банков данных, спрос на которые обусловливает похищение информационных массивов [2].

Интернет предоставляет злоумышленникам множество возможностей и для вторжения во внутренние сети организаций с целью похищения, искажения или уничтожения конфиденциальной информации.

Следовательно, основным требованием является обеспечение надлежащей технической защиты сетей и связанных с ними информационных систем и ресурсов. Физическим и юридическим лицам необходимо реализовывать правовые, организационно-распорядительные (административные), технические и криптографические меры, обеспечивающие минимизацию количества фактических или потенциальных угроз конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Изложенное предопределяет актуальность предлагаемого учебного курса.

Его задача состоит не только в том, чтобы предоставить студентам (магистрантам) теоретические знания, но и научить применять эти знания на практике, показать, каким образом тот или иной способ защиты информации, та или иная система нормативных требований реализуются в реальных условиях.

Для удобства работы с пособием считаем необходимым дать некоторые пояснения относительно его структуры и содержания.

Пособие содержит лекционную часть, вопросы для самопроверки и список литературы (включая нормативные правовые акты).

Первая глава пособия посвящена общим понятиям и определениям, поскольку ни один курс не может быть успешно освоен без понимания ключевой терминологии. Глава сформирована для того, чтобы всякий раз при употреблении специального термина в тексте не отвлекаться на пояснение его сути, а при необходимости вернуться к началу и прочесть соответствующие абзацы. Приведенные определения в подавляющем большинстве случаев являются официальными, т.е. закрепленными в нормативных правовых актах. Каждое определение обеспечено ссылкой на его источник, что позволит проверить его актуальность.

Изложенная в первой главе структура информации ограниченного доступа дает представление о том, конфиденциальность какого рода сведений необходимо обеспечивать в обязательном порядке, а также о типовых информационных системах, в которых обрабатывается такая информация.

Для обеспечения конфиденциальности информации важно создать целостный комплекс правовых, организационных и технических мер по защите сведений ограниченного доступа. Владения навыками «встраивания» в информационную систему исключительно программно-аппаратных средств защиты недостаточно. Утрата либо разглашение информации, распространение и (или) предоставление которой ограничено, признается одной из угроз национальной безопасности Республики Беларусь в информационной сфере [3], поэтому государственная политика в области информационной безопасности направлена на разработку и введение правовых режимов безопасности информации и информационных ресурсов, технических условий и политик безопасности [2]. Разделы 2 и 3 дают представление об основных принципах и процедурах выстраивания системы защиты информации в соответствии с предъявляемыми регуляторами нормативными требованиями, о правилах подготовки и внедрения локальных нормативных правовых актов, направленных на обеспечение конфиденциальности информации.

Система защиты информации не может оставаться статичной. По мере возникновения новых потребностей и совершенствования информационных технологий она неизбежно претерпевает изменения. Нередко это вызвано и изменениями в нормах права.

Так, уже в процессе подготовки пособия был пересмотрен один из основополагающих документов в области защиты информации – Положение о технической и криптографической защите информации, утвержденное Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации».

14 марта 2020 г. Положение начало действовать в новой редакции, утвержденной Указом Президента Республики Беларусь 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации» [4], и это повлекло за собой изменение целого пласта нормативных правовых актов.

Ожидаются изменения и в правовом регулировании защиты персональных данных. Пока соответствующие нормативные правовые акты не приняты, невозможно совершенно определенно прогнозировать, в каком направлении будет развиваться правовое регулирование этих отношений, поэтому при изложении материала некоторые вопросы оставлены открытыми или изложены предельно общим образом.

Авторы осознавали, что целевой аудиторией пособия будут лица, не имеющие специальной юридической подготовки, поэтому приняли решение не перегружать текст избыточными ссылками на статьи (части, пункты, абзацы) актов законодательства, а также избегать подробных наименований и длинных списков нормативных правовых актов, где это возможно. По этой же причине в пособии не освещались вопросы юридической ответственности за нарушение требований по защите информации.

При необходимости изучения официальных юридических текстов следует использовать списки нормативных правовых актов из приложений в конце пособия. Рекомендуется при этом проверять действие каждого документа, используя регулярно обновляемые информационные системы: например, ИПС «ЭТАЛОН» (в сети Интернет – ИПС «ЭТАЛОН-ONLINE»: http://etalonline.by/) – для актов законодательства, ИПС «Стандарт», ИПС «ЭТАЛОН-СТАНДАРТ» (в сети Интернет – каталог Национального фонда технических нормативных правовых актов: http://tnpa.by/) – для технических нормативных правовых актов.

Учитывая тематику курса, описание технических средств и способов защиты информации в главах 4–9 максимально ориентировано на обеспечение конфиденциальности информации в сети Интернет без отвлечения на общие правила, вероятно, уже известные из освоенных ранее учебных дисциплин.

Авторы посчитали необходимым выделить еще два особых блока, несколько «выбивающихся» из общей структуры пособия – о защите от средств социальной инженерии, направленной на использование слабостей человеческой психологии в целях получения конфиденциальной информации; а также о методах защиты от действий внутреннего нарушителя. С одной стороны, применяемые в этих сферах способы защиты информации являются общими, с другой – обладают серьезной спецификой, требующей отдельного анализа.

Одним из важнейших принципов защиты информации является правило, что стоимость создания системы защиты информации не должна превышать стоимость самой информации, которая обрабатывается в информационной системе. По этой причине в завершающей части курса размещена глава о методах экономической оценки затрат на обеспечение конфиденциальности информации в сети Интернет.

Текст пособия снабжен множеством перекрестных ссылок, позволяющих обеспечивать целостность восприятия информации и тесную связь между различными частями курса.

Содержание пособия соответствует образовательному стандарту по специальности второй ступени высшего образования ОСВО 1-40 80 04-2019 и учебной программе специальности высшего образования второй ступени (магистратура) 1-40 80 04 «Информатика и технологии программирования» для дневной (регистрационный № 27-19/до М–ФИТ от 28.03.2019) и заочной (регистрационный №28-19/зо М–ФИТ от 28.03.2019) форм получения образования.

Авторы пособия:

Раханов Константин Яковлевич – кандидат технических наук, доцент кафедры вычислительных систем и сетей Полоцкого государственного университета, технический директор ООО «ТриИнком» (главы 4–9, 11, 12, заключение); Раханова Надежда Александровна – исследователь в области юридических наук, юрисконсульт ООО «Юридическая компания Аксенов Групп» (главы 1–3, 10, введение).

Текст соответствует нормативным правовым актам Республики Беларусь на дату 01.10.2020.

1. ВВЕДЕНИЕ В ПРОБЛЕМУ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

1.1. Общие понятия и определения

1.1.1. Информационные отношения. Информационные системы и сети

Информационные отношения – это отношения, возникающие при (1) поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией[1]; (2) создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов; (3) организации и обеспечении защиты информации [5].

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [5].

Информация является нематериальным объектом, поэтому всегда неразрывно связана с ее носителем и совместно с ним образует **информационный объект** (**продукт**).

Носителями информации являются [6]:

– предметы с нанесенной на них символьной информацией в доступном для восприятия человеком виде (книги, рукописи, берестяные грамоты, глиняные таблички, свитки, списки и т.п.);

– предметы с нанесенной на них информацией в машинных кодах, т.е. в недоступном для непосредственного восприятия человеком виде (магнитные диски, дискеты, ленты, электронные и электронно-оптические носители информации и т.п.).

Носитель информации – это всегда материальный объект, хранящий информацию. Например, акустическая плоская волна, созданная голосовыми связками человека или техническим устройством и модулированная информативным сигналом, – это эффект, получаемый при воздействии на частицы воздуха, но воздух при этом – не носитель информации (он информацию не хранит), это среда передачи информации, аналогичная, скажем,

[1] Процесс **создания** информации в сферу информационных отношений не включается. Понятие «передача информации» используется в техническом смысле: как физический процесс пространственного переноса информации от источника к приемнику, а не как юридический процесс коммерческого оборота информации.

USB-кабелю. Среда передачи способна порождать **канал утечки информации**, через который информация потенциально может быть извлечена злоумышленником (подробнее – см. [7; 8]). Ноутбук (объект) с отображаемой на его экране текстовой информацией – не носитель информации, а средство ее обработки (носитель в этом случае – жесткий диск). В то же время человек со всей информацией, хранящейся в нейронах его мозга, – не носитель информации, потому что он – субъект, а не объект.

Чтобы передавать информацию по каналам связи с помощью средств вычислительной техники и сопрягаемых с ними устройств, ее необходимо преобразовать в цифровую (электронную) форму. В результате **цифровизации** (**дигитализации**) информация, как правило, оказывается включенной в различные информационные системы и информационные ресурсы.

Обработка информации в информационной системе включает в себя сбор, накопление, ввод, вывод, прием, передачу, запись, хранение, регистрацию, уничтожение, преобразование и отображение информации [9].

Информационная система – это совокупность баз данных, банков данных, информационных технологий и комплекса (комплексов) программно-технических средств [5], где:

– **база данных** – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях [5];

– **банк данных** – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими [5];

– **информационная технология** – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации [5];

– **комплекс программно-технических средств** – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий [5].

Примером информационной системы могут быть: Реестр принадлежности сетевых (IP) адресов, Национальный портал открытых данных Республики Беларусь (http://opendata.by/), АИС «Расчет» (автоматизированная информационная система единого расчетного и информационного пространства Республики Беларусь).

Информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи [5].

Интернет – глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов (Internet Protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP) и предоставляющая возможность реализации различных форм коммуникации, в т.ч. размещения информации для неограниченного круга лиц [9].

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах [5]. **Документированная информация** – это информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать [5]. К информационным ресурсам относятся, например, информационно-поисковые системы (ИПС «Стандарт», ИПС «Эталон», АПС «Бизнес-Инфо» и т.п.), веб-сайты, электронные учебно-методические комплексы и т.п.

Для определенных целей (например, для защиты критически важных объектов[2]) может использоваться понятие **объекта информатизации**, под которым понимаются средства электронной вычислительной техники вместе с программным обеспечением, в т.ч. системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или) технологическими процессами [4]. Объект информатизации может осуществлять функции информационной системы [10].

1.1.2. Доступ к информации. Общедоступная информация

Доступ к информации – ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение. Различают **санкционированный** (не нарушающий установленные правила разграничения доступа) и **несанкционированный** (нарушающий установленные правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами) **доступ** [11, с. 20–21].

С доступом к информации и ресурсам системы (сети) связана группа таких понятий, как **идентификация**, **аутентификация**, **авторизация** (см. в главе 6).

---

[2] О критически важных объектах информатизации см. в разделе 1.3.

В зависимости от категории доступа информация делится на общедоступную информацию и информацию, распространение и (или) предоставление которой ограничено.

Общедоступная информация – это информация, доступ к которой, распространение и (или) предоставление которой не ограничены [5]. К этой группе относится:

– информация, доступ к которой не может быть ограничен;

– прочая общедоступная информация.

Например, не могут ограничиваться предоставление и распространение информации о чрезвычайных ситуациях (скажем, об авариях на промышленных предприятиях), об экологической, санитарно-эпидемиологической обстановке (например, об эпидемиях, стихийных бедствиях, загрязнении пресных вод), о размерах золотого запаса, об уровне преступности, о состоянии здоровья Премьер-министра Республики Беларусь или Главы Администрации Президента Республики Беларусь (но не Президента Республики Беларусь) и т.д.[3] Отнесение информации к этой категории означает, что она в обязательном порядке должна быть предоставлена каждому заинтересованному лицу и не может быть скрыта, а лицо, распространяющее такую информацию, не подлежит юридической ответственности.

Можно сказать, что общедоступной является любая информация, кроме той, **распространение (предоставление) которой ограничено** (подробно об этом – в разделе 1.2).

От общедоступной информации следует отличать **массовую информацию**, которую составляют предназначенные для неопределенного круга лиц печатные, аудио-, аудиовизуальные и другие информационные сообщения и (или) материалы, опубликованные в печати, сообщенные посредством вещания теле- или радиопрограммы, интернет-ресурса или в иной форме распространения [12]. Общедоступная информация не обязательно является массовой, однако всякая массовая информация является общедоступной.

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней [5]. Требование конфиденциальности (см. раздел 1.1.3) к общедоступной информации неприменимо.

[3] Исчерпывающий перечень видов такой информации содержится в статье 16 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон об информации) [12].

1.1.3. Защита информации. Информационная безопасность

Защите подлежит информация (информационная система), неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу [5]. Под **вредом** здесь понимается ущерб жизни или здоровью, имущественный или моральный вред, подлежащий денежному измерению.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение (1) конфиденциальности, (2) целостности, (3) подлинности, (4) доступности и (5) сохранности информации [5].

Конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь [5].

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц [5].

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц [5].

Целостность информации – состояние защищенности информации от модификации, подмены, уничтожения неправомочным способом [11, с. 24].

Достоверность (подлинность, аутентичность) **информации** – свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником, либо тому субъекту, от которого она принята [11, с. 24].

Доступность – состояние информационной технологии, обеспечивающее своевременный и надежный доступ к информации и (или) функциональным возможностям информационной технологии правомочным образом [11, с. 24].

Если информация, распространение и (или) предоставление которой ограничено, не содержится в информационной системе, ее защита организуется обладателем информации [5].

Обладатель информации – это лицо, имеющее две разновидности правомочий: право использовать информацию и определять условия ее обработки, пользования ею в информационных системах и сетях и право распоряжаться имущественными правами на информацию (т.е. отчуждать или передавать такие права на условиях договора). Буквально: обладатель информации – это **правообладатель в отношении информации**.

Важно понимать, что понятия «собственник информации» и «владелец информации» являются юридически некорректными и использоваться

не могут, поскольку право собственности (а равно и владение как элемент права собственности) может устанавливаться только на материальную (телесную) вещь, а информация – объект нематериальный (подробнее об этом – М.А. Рожкова [13]). Отсюда следует, что в отношении информации недопустимы гражданско-правовые сделки (проще говоря, нельзя, например, «продать информацию»). Свойством оборотоспособности обладают только материальные носители информации, а также имущественные права на информацию, когда информация имеет экономическую (коммерческую) стоимость.

Обладателя информации следует отличать от **пользователя информации** – лица, обладающего правом получать, предоставлять (распространять) и использовать информацию, но не имеющего правомочий распоряжения правами в отношении такой информации.

Информация ограниченного доступа, содержащаяся в информационных системах, по общему правилу, защищается **собственником** или **оператором информационной системы** [5].

В информационные отношения, связанные с защитой информации, могут быть включены также и иные субъекты: владельцы программно-технических средств, информационных ресурсов, информационных систем и информационных сетей; собственники программно-технических средств, информационных ресурсов, информационных сетей.

Техническая защита информации – деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации [4].

Криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации [4].

Средства технической защиты информации – технические, программные, программно-аппаратные средства защиты информации, предназначенные для защиты информации от несанкционированного доступа и несанкционированных воздействий на нее, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности[4] [4].

[4] О методах и средствах оценки защищенности информации от утечки по техническим каналам – см. в публикациях В.К. Железняка, К.Я. Раханова [7; 14–17].

Средства криптографической защиты информации – технические, программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработку и проверку электронной цифровой подписи, хэширование, имитозащиту) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности [4].

Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ) – государственный орган, осуществляющий государственное регулирование, управление и контроль в сфере технической и криптографической защиты информации [5]. Создан Указом Президента Республики Беларусь от 21 апреля 2008 г. № 229-ДСП.

В компетенцию ОАЦ, в числе прочего, входит разработка проектов нормативных правовых актов, в т.ч. технических нормативных правовых актов, и принятие (издание) таких актов по вопросам технической и криптографической защиты информации, а также участие в разработке проектов нормативных правовых актов по вопросам информатизации.

Деятельность по технической и (или) криптографической защите информации подлежит **лицензированию**, если это информация:

– распространение и (или) представление которой ограничено (см. раздел 1.2);

– обрабатываемая на критически важных объектах информатизации (см. раздел 1.3);

– обрабатываемая в информационных системах в форме электронных документов.

Электронный документ – документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность, которые подтверждаются путем применения сертифицированных средств электронной цифровой подписи с использованием при проверке электронной цифровой подписи открытых ключей организации или физического лица (лиц), подписавших этот электронный документ [18].

Лицензирование осуществляется ОАЦ. Перечень видов подлежащей лицензированию деятельности по технической и (или) криптографической защите информации устанавливается пункте 13 Приложения 1 к Положению о лицензировании отдельных видов деятельности, утвержденному Указом Президента от 1 сентября 2010 г. № 450 «О лицензировании отдельных видов деятельности» [19].

Лицензирование предусмотрено для случаев, когда деятельность по защите информации ограниченного распространения осуществляется

внешними организациями. Если работы по технической и (или) криптографической защите информации выполняются для собственных нужд обладателем информации, распространение и (или) предоставление которой ограничено, собственником (владельцем) информационных систем и критически важных объектов информатизации, то получение лицензии на такую деятельность не требуется [19].

Отдельная лицензия предусмотрена для деятельности в отношении криптографических средств защиты государственных секретов. В этой области лицензирование осуществляется Комитетом государственной безопасности Республики Беларусь. Перечень видов деятельности, подлежащих лицензированию, установлен пунктом 107 Положения о порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами), утвержденного Указом Президента Республики Беларусь от 16.02.2012 № 71 «О порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)» [20].

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [3]. На рисунке 1.1 представлена модель информационной безопасности.

Угроза информационной безопасности – фактор (совокупность факторов), создающий (создающая) опасность для личности, общества, государства в информационном пространстве [21]. По сути, это потенциально возможное действие, событие или процесс, которые посредством воздействия на информацию и другие компоненты информационной системы могут нанести ущерб интересам субъектов [11, с. 24].

Рассмотрим детальную классификацию угроз информационной безопасности, предложенную Ю.А. Родичевым [11, с. 24] (рисунок 1.2).

В зависимости от результатов воздействия угрозы бывают пассивные и активные.

Информационная система подвергается **активной угрозе**, т.е. целенаправленному воздействию на ее компоненты с целью нарушения нормального функционирования (например, выведение из строя устройства, операционной системы, разрушение программного обеспечения, нарушение работы сети, уничтожение или искажение данных).

Пассивные угрозы направлены на несанкционированное использование информационной системы без нарушения ее функционирования и изменения информационного наполнения.

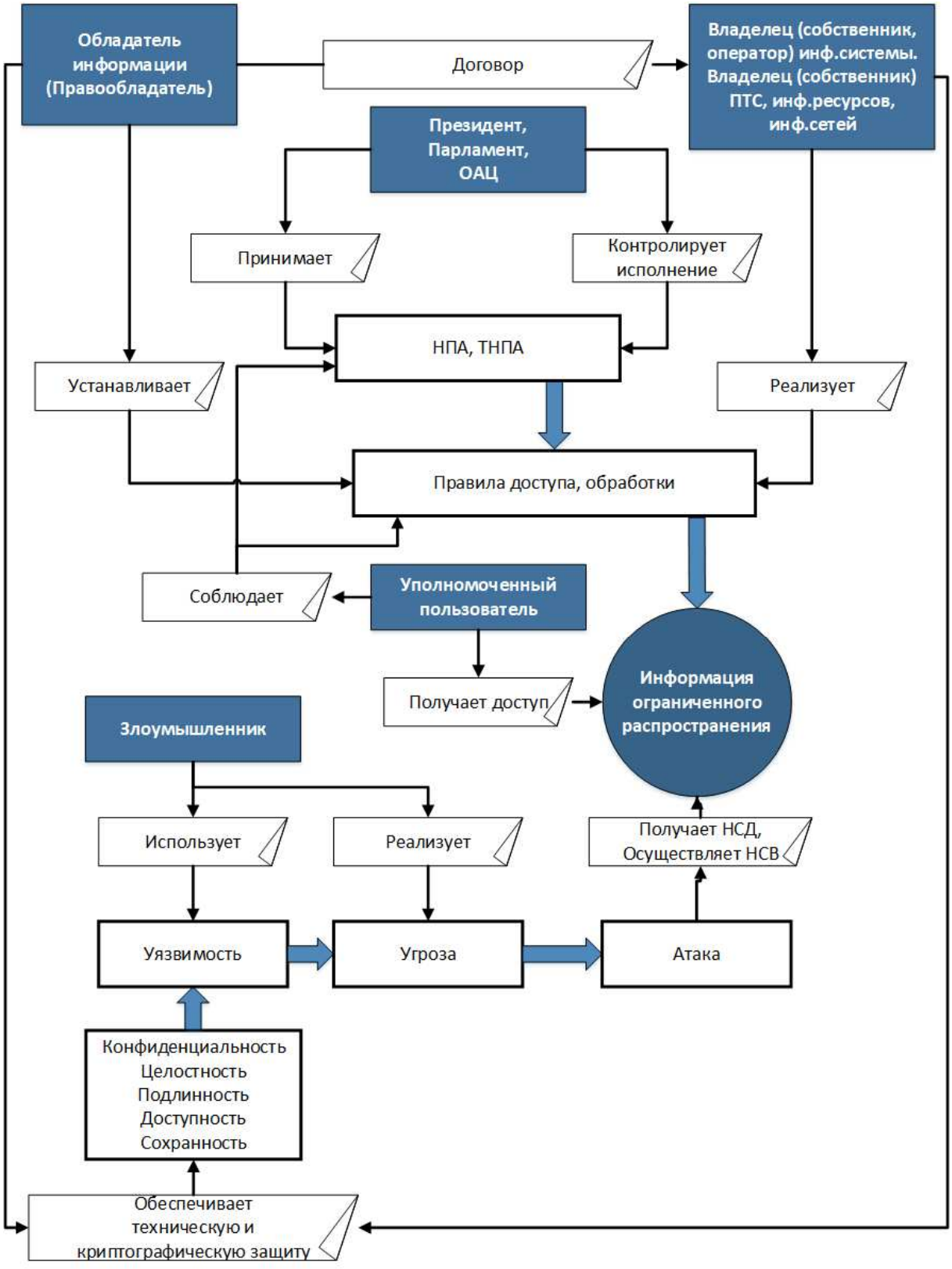


Рисунок 1.1. – Модель информационной безопасности

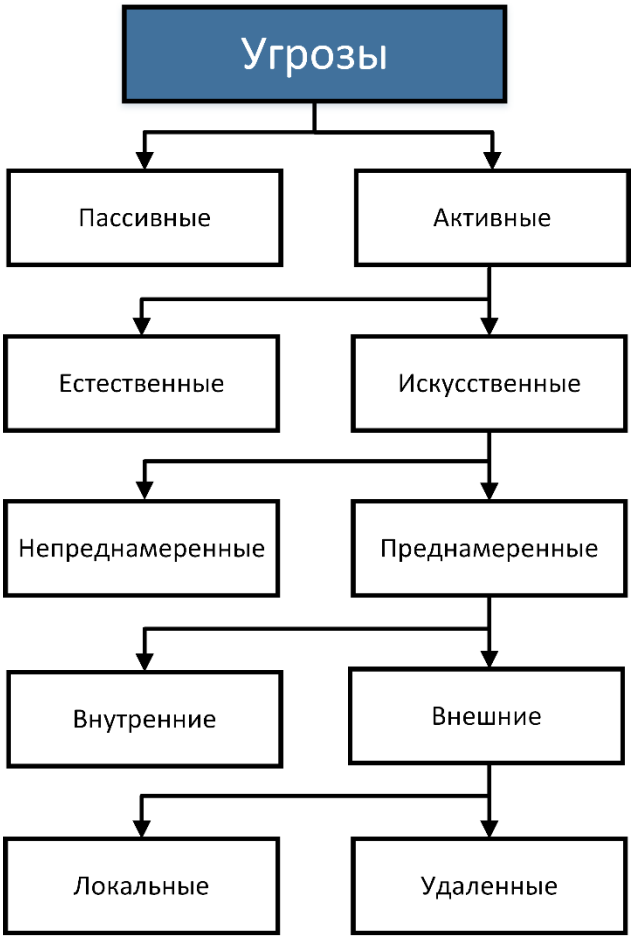


Рисунок 1.2. – Угрозы информационной безопасности

Активные угрозы безопасности могут быть естественными и искусственными. **Естественные** вызваны воздействием на информационные системы объективных физических процессов или стихийных природных явлений, не зависящих от человека (например, стихийные бедствия, аварии, внезапные отключения электропитания, поломки технических средств и т.п.). Эти угрозы невозможно прогнозировать, однако они могут привести к серьезным нарушениям, поэтому меры защиты от них должны применяться всегда.

Искусственные угрозы вызваны действиями человека (антропогенные) и подразделяются на непреднамеренные (случайные) и преднамеренные. Методы противодействия этим угрозам управляемы и, как правило, зависят от организации системы защиты информации, поскольку действия субъекта всегда можно оценить, спрогнозировать, после чего принять адекватные им меры.

Непреднамеренные угрозы связаны с людьми, непосредственно работающими с информационной системой. Как правило, это действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности,

но без прямого умысла. Часто такие угрозы являются следствием невыполнения персоналом организационно-технологических правил и требований внутренних нормативных документов.

Преднамеренные искусственные угрозы делятся на внутренние (со стороны персонала организации) и **внешние** (от посторонних лиц и организаций).

В свою очередь, внешние угрозы подразделяются на **локальные** (проникновение посторонних лиц в учреждение и доступ их к системе) и **удаленные** (незаконный доступ к системе через глобальные сети).

Примерами **источников угроз** могут быть хакеры, злонамеренные пользователи, незлонамеренные пользователи (которые иногда делают ошибки), компьютерные процессы и сбои [11, с. 18].

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации [11, с. 64].

Компьютерная атака – целенаправленное воздействие программно-техническими средствами на информационно-коммуникационные системы, сети, ресурсы, в т.ч. на автоматизированные системы управления критически важных структур, осуществляемое в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой ими информации [21].

Несанкционированное воздействие на информацию – изменение или уничтожение информации, осуществляемое с нарушением установленных прав или правил [4].

Несанкционированный доступ к информации – доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа [4].

Нарушителем (**злоумышленником**) принято считать лицо, непреднамеренно или с прямым умыслом предпринявшее попытку выполнения запрещенных операций в информационной системе и использующее для этого различные возможности, методы и средства [22, с. 95]. Терминология, применяемая в отношении нарушителей, может быть различной. Например, хакером (англ. hacker) чаще всего называют именно компьютерных злоумышленников, иногда – высококвалифицированных компьютерных специалистов. Последних иногда именуют «белыми шляпами» (англ. white-hats) в отличие от «черных шляп» (англ. black-hats), цель которых нанести вред системе. Встречаются и такие понятия, как кракер (англ. cracker), кид-хакер (англ. kid-hacker), шпион (англ. spy) [22, с. 96].

Модель нарушителя – предположения о возможностях (ограничениях возможностей) нарушителей, действия которых могут привести к потенциальному ущербу [23].

Формирование модели нарушителя обеспечивается следующим образом [23]:

1) определяются зоны, окружающие конфиденциальную информацию;

2) определяются все средства защиты между зонами и внутри них;

3) определяются возможные угрозы и вероятности их возникновения;

4) описывается состояние окружающей среды;

5) формируется классификация и описание вероятных нарушителей информационной безопасности.

Выделение классов нарушителей может выполняться по различным методикам (см., например, [23]). Каждая категория нарушителей привязывается к определенным угрозам и величине потенциального ущерба.

В пособии не будет уделяться внимание вопросам юридической ответственности за правонарушения, связанные с защитой конфиденциальности информации в сети Интернет. Рекомендуем обратиться к подготовленному Г.А. Василевичем и С.Г. Василевичем общему обзору законодательства об ответственности за правонарушения в информационной сфере в учебнике «Информационное право» (Минск, 2015) [24].

1.2. Структура информации ограниченного доступа

К информации, распространение и (или) предоставление которой ограничено, относится [5]:

– информация о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– служебная информация ограниченного распространения;

– информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

– информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

В теории информационной безопасности этот блок информации иногда именуется «предметной конфиденциальной информацией» [25] в противовес «служебной конфиденциальной информации», к которой относятся, например, имена и пароли пользователей, ID-идентификатор ключа (карты) доступа, код сейфа и т.п.

Правовые ограничения распространения могут устанавливаться и в отношении результатов интеллектуальной деятельности (произведений науки, литературы, искусства; исполнения, фонограммы, передачи организаций вещания и т.п.), однако в рамках настоящего пособия такая информация не рассматривается, поскольку, во-первых, она не является конфиденциальной, во-вторых, строго юридически и информацией не является.

1.2.1. Информация о частной жизни лица и персональные данные

В самом общем виде персональные данные – это любые данные, позволяющие прямо или косвенно идентифицировать конкретное физическое лицо (человека).

В Республике Беларусь основными персональными данными считаются [26]:

– идентификационный номер (буквенно-цифровая последовательность, которая указывается в документах, удостоверяющих личность: паспорт, вид на жительство и т.п.);

– фамилия, собственное имя, отчество (если таковое имеется);

– пол;

– число, месяц, год рождения;

– место рождения;

– цифровой фотопортрет;

– данные о гражданстве (подданстве);

– данные о регистрации по месту жительства и (или) месту пребывания;

– данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным.

Дополнительные персональные данные [26] – это данные:

– о родителях, опекунах, попечителях, семейном положении, супруге, ребенке (детях) физического лица;

– о высшем образовании, ученой степени, ученом звании;

– о роде занятий (место работы, дата трудоустройства и увольнения);

– о пенсии, ежемесячном денежном содержании по законодательству о государственной службе, ежемесячной страховой выплате по обязательному страхованию от несчастных случаев на производстве и профессиональных заболеваний;

– о налоговых обязательствах;

– об исполнении воинской обязанности;

– об инвалидности.

Основные и дополнительные персональные данные включаются в регистр населения – государственную централизованную автоматизированную информационную систему, основу которой составляет база персональных данных граждан Республики Беларусь, иностранных граждан и лиц без гражданства, постоянно проживающих в Республике Беларусь. Владелец регистра – Министерство внутренних дел Республики Беларусь.

Регистр населения отнесен к классу информационных систем 3-фл, 3-юл (о классификации информационных систем подробно – в разделе 1.3). Общедоступных персональных данных в регистре нет. Любые данные из регистра могут выдаваться только при авторизованном доступе и строго в объеме, определенном правами конкретной организации-получателя или физического лица.

Вместе с тем к персональным данным в самом широком смысле относятся также и иные данные (нередко именуются «чувствительными»):

– о расе, национальности и цвете кожи;

– о мировоззрении, политических или религиозных убеждениях;

– о состоянии здоровья (заболеваниях) физического лица;

– о сексуальной ориентации;

– об усыновлении;

– отпечатки пальцев, ладоней, радужная оболочка глаза (биометрические данные), код ДНК (генетические данные);

– сведения, составляющие тайну телефонных переговоров, почтовых и иных сообщений;

– иные сведения, составляющие личную и семейную тайну.

В конечном счете перечень данных, относимых к персональным, не может быть исчерпывающим, поскольку важен контекст: как только мы имеем возможность прямо или косвенно (в совокупности с иными данными) связать имеющуюся информацию с конкретным человеком, эта информация становится персональными данными.

Например, IP-адрес в общем виде определяет устройство, а не лицо, однако в некоторых случаях он может выступать онлайн-идентификатором человека.

Так, в Беларуси поставщик интернет-услуг (например, РУП «Белтелеком») обязан в течение года осуществлять хранение сведений об абонентских устройствах и оказанных интернет-услугах физическим лицам, что включает в себя, в числе прочего, фамилию, собственное имя и отчество пользователя, его адрес, внутренний и внешний IP-адреса и порты оконечного абонентского устройства (терминала), доменное имя, IP-адрес и порт посещаемого пользователем интернет-ресурса[5]. В данном случае IP-адрес – это персональные данные, поскольку потенциально (косвенным образом) он позволяет не только определить конкретное физическое лицо, но и отследить его активность в сети Интернет в течение года (само по себе это, конечно, не означает, что доступ к такой информации может получить любое лицо по запросу).

Другая ситуация – сбор и хранение IP-адресов посетителей сайта владельцем интернет-магазина, размещенного на этом сайте. Как таковое наличие IP-адреса в логах еще не говорит о том, что интернет-магазин собирает и обрабатывает персональные данные, но если помимо IP-адреса фиксируются иные сведения о пользователях (списки заказов, устройств, покупок, заметки, комментарии, адреса электронной почты, номера телефонов, время и периодичность посещения и т.п.), которые в совокупности сделают возможной идентификацию конкретного человека, то все, что хранит и обрабатывает интернет-магазин, в т.ч. IP-адрес, – это персональные данные.

Аналогичным образом, получив через форму для обратной связи номер телефона (обезличенный набор цифр) или адрес электронной почты (обезличенный набор символов), владелец интернет-ресурса не осуществил каких-либо действий с персональными данными, но как только потребовалось ввести полные фамилию, имя и отчество – имеет место сбор персональных данных.

Обработка и перемещение персональных данных во всем мире приобретает огромное экономическое значение. Базовый принцип работы с персональными данными – **получение письменного согласия** физического лица, к которому относятся персональные данные, **на любое действие** с ними (поиск, сбор, получение, передачу, обработку, накопление, хранение,

[5] Абзац второй пункта 6 Указа Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» [27], пункт 3.1.1 Инструкции о порядке формирования и хранения сведений о посещаемых пользователями интернет-услуг информационных ресурсах, утвержденной Постановлением Министерства связи и информатизации Республики Беларусь от 18 февраля 2015 г. № 6 «Об утверждении Инструкции о порядке формирования и хранения сведений о посещаемых пользователями интернет-услуг информационных ресурсах» [28].

распространение, предоставление), кроме случаев, когда получение такого согласия не требуется в соответствии с законодательными актами.

На практике при отсутствии детального правового регулирования могут возникать вопросы. Например, является ли письменным согласием проставление отметки («галочки») о согласии на обработку персональных данных на сайте интернет-магазина? В такой ситуации получить согласие пользователя на бумаге, если и возможно в принципе (например, отправив такой документ почтой), то технически и организационно – достаточно сложно. Конкретного решения проблемы белорусское законодательство пока не содержит, хотя специалисты нередко приравнивают электронную форму получения согласия к письменной, применяя аналогию с письменной формой сделки [29]. Проект Закона «О персональных данных»[6] предусматривает, что согласие на обработку персональных данных может быть получено и в электронной форме, в т.ч. путем указания кода, полученного в SMS, проставления отметки на сайте или другими способами.

Меры по защите персональных данных от разглашения должны приниматься с момента, когда такие данные были предоставлены, и до их уничтожения, обезличивания или получения согласия лица на их разглашение.

Если персональные данные были получены с нарушением требований законодательства, использовать их запрещается.

1.2.2. Сведения, составляющие государственные секреты

Сведения, составляющие государственные секреты, – это сведения в области политики, экономики, финансов, науки, техники, в военной области, области разведывательной, контрразведывательной, оперативно-розыскной деятельности, информационной и иных областях национальной безопасности Республики Беларусь, которые отнесены к государственным секретам уполномоченными государственными органами и иными организациями [31].

Установление ограничений на распространение и (или) предоставление сведений, а также применение иных мер защиты в отношении вышеперечисленных сведений называется засекречиванием (обратный процесс соответственно – рассекречиванием).

Общий перечень сведений, которые могут быть отнесены к государственным секретам, содержится в статье 14 Закона Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах» [31]. В частности,

[6] Ранее сообщалось [30], что может начать действовать не ранее середины 2020 г., однако на дату 01.07.2020 продолжает находиться на рассмотрении в Парламенте.

это сведения об экспорте и импорте вооружения и военной техники; об объемах финансирования из республиканского бюджета Вооруженных Сил Республики Беларусь; о гражданах, оказывающих (оказывавших) на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность.

Государственные секреты подразделяются на две категории [31]:

– **государственная тайна** – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь (срок засекречивания – до тридцати лет);

– **служебная тайна** – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь[7] (срок засекречивания – до десяти лет).

Для государственных секретов устанавливаются следующие степени секретности (и соответствующие грифы): для государственной тайны – «Особой важности», «Совершенно секретно»; для служебной тайны – «Секретно». Критериями разграничения служат тяжесть последствий и размер вреда вследствие разглашения сведений.

Любая деятельность с использованием государственных секретов может осуществляться только при наличии **допуска к государственным секретам**.

1.2.3. Служебная информация ограниченного распространения

Служебная информация ограниченного распространения – это сведения, касающиеся деятельности государственного органа, юридического лица, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в т.ч. их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц и которые не отнесены к государственным секретам [5] (соответствует гриф «Для служебного пользования»).

Сведения относятся к служебной информации ограниченного распространения в соответствии с перечнем, утвержденным Постановлением Совет

[7] Категории «тяжкие последствия для национальной безопасности» и «существенный вред национальной безопасности» являются оценочными и законодательством Республики Беларусь не определяются.

Министров Республики Беларусь от 12 августа 2014 г. № 783 «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну» [32]. К ним, к примеру, относятся сведения о дислокации постов и маршрутов патрулирования нарядами ДПС ГАИ МВД; сведения о количестве, точном местонахождении и емкости подземных хранилищ нефти, нефтепродуктов и газа; сведения о технических характеристиках метрополитена; схемы маршрутов по перевозке почты; государственные топографические карты масштабов 1:200 000 и 1:100 000; сведения о способах изготовления наркотических средств.

1.2.4. Охраняемая законом тайна

Охраняемая законом тайна – это сведения, составляющие:

- коммерческую тайну;
- профессиональную тайну;
- банковскую тайну;
- иную охраняемую законом тайну.

Коммерческой тайной могут являться сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в т.ч. секреты производства (ноу-хау) [33]. Чтобы защитить такую информацию, необходимо применить специальный способ ее охраны – установить режим коммерческой тайны.

Режим коммерческой тайны может устанавливаться в отношении сведений, которые одновременно соответствуют следующим требованиям [33]:

1) не являются общеизвестными (например, сведения с официальных сайтов) или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями (например, сведения о размере заработной платы работника, которые должны быть включены нанимателем в справку, выдаваемую по заявлению работника, и таким образом могут стать известны третьим лица[8]);

2) имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам, т.е. обладание такими сведениями позволяет лицу увеличить доходы, сократить расходы, сохранить положение на рынке товаров, работ или услуг либо получить иную коммерческую выгоду;

[8] В то же время наниматель вправе отнести к коммерческой тайне не размер заработной платы, а систему оплаты труда (прямая, премиальная, прогрессивная, аккордная, тарифная или бестарифная, либо их различные сочетания).

3) не являются объектами исключительных прав на результаты интеллектуальной деятельности (как, например, исходные коды программ, объекты дизайна, произведения науки, литературы);

4) не отнесены к государственным секретам.

В организациях в сфере информационных технологий коммерческую тайну могут составлять сведения о логинах и паролях к серверам и сервисам организации и контрагентов; сведения о клиентах (в т.ч. потенциальных), включая контактные данные их представителей; технические задания и спецификации по проектам; построение бизнес-процессов, включая особенности поиска сотрудников, проведения рекламных мероприятий и т.п. [34].

Режим коммерческой тайны может быть эффективен в отношении различных ноу-хау, а также тех технических решений, по которым патентная защита еще не получена либо которые непатентоспособны в принципе (например, методы ведения бизнеса, любые необъективированные идеи и т.п.) [35].

Существует перечень сведений, в отношении которых режим коммерческой тайны устанавливать запрещается (содержится в статье 6 Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» [33], далее – Закон о коммерческой тайне). К ним, например, относятся сведения, содержащиеся в учредительных документах юридического лица, сведения о численности и составе работников, наличии вакансий, недвижимом имуществе организации, а также сведения, которые являются врачебной, адвокатской, банковской, налоговой или иной охраняемой законом тайной.

Режим коммерческой тайны устанавливается следующим образом: определяется состав сведений, составляющих коммерческую тайну; принимаются меры, необходимые для обеспечения конфиденциальности таких сведений.

Конфиденциальность коммерческой тайны обеспечивается следующими обязательными мерами:

– ограничивается доступ к коммерческой тайне путем установления порядка обращения к носителям коммерческой тайны и контроля за соблюдением такого порядка (обычно путем разработки и утверждения локальных нормативных правовых актов);

– ведется учет лиц, получивших доступ к коммерческой тайне, и назначаются работники, ответственные за обеспечение конфиденциальности;

– с работниками, имеющими доступ к коммерческой тайне, заключается трудовой договор (контракт), содержащий обязательство о неразглашении коммерческой тайны, либо отдельное обязательство о неразглашении коммерческой тайны (иногда именуется NDA (non-disclosure agreement), подробнее – в разделе 2.1.2);

– с контрагентами, имеющими доступ к коммерческой тайне, заключаются соглашения о конфиденциальности (подробнее – в разделе 2.1.2).

Наряду с этими мерами владелец коммерческой тайны вправе применять не запрещенные законодательством технические средства и методы защиты информации, а также другие меры, не противоречащие законодательству.

На носителях коммерческой тайны может проставляться гриф «Коммерческая тайна» с указанием владельца.

Профессиональная тайна – это конфиденциальные сведения, полученные лицом в связи с осуществлением деятельности по определенной профессии. К профессиональной тайне, в частности, относится адвокатская тайна; нотариальная тайна; врачебная тайна; информация, полученная при оказании психологической помощи; аудиторская тайна; тайна страхования.

Банковской тайной являются следующие сведения [36]:

– о счетах и вкладах (депозитах), в т.ч. о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета;

– о размере средств, находящихся на счетах и во вкладах (депозитах);

– сведения о конкретных сделках, об операциях без открытия счета, операциях по счетам и вкладам (депозитам);

– об имуществе, находящемся на хранении в банке.

К **иной охраняемой законом тайне** относятся налоговая тайна, тайна почтовой связи, тайна усыновления, тайна исповеди и т.п.

1.3. Классификация информационных систем, в которых обрабатывается информация ограниченного распространения

Информацию, подлежащую защите от нарушений конфиденциальности в сети Интернет, чаще всего невозможно отделить от информационной системы, в которой она обрабатывается[9].

[9] Понятие информационной системы см. в разделе 1.1.

Для того чтобы обеспечить единые требования к защите информационных систем, в которых обрабатывается информация ограниченного распространения, государственным стандартом Республики Беларусь СТБ 34.101.30-2017 «Информационный технологии. Методы и средства безопасности. Информационные системы. Классификация» [37] (далее – СТБ 34.101.30-2017) с 01.10.2017 введена их классификация, предполагающая выделение двенадцати классов типовых информационных систем.

СТБ 34.101.30.2017 разработан Государственным предприятием «НИИ ТЗИ» и введен взамен действовавшего с 28.09.2007 по 11.04.2017 стандарта СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация» [38] (далее – СТБ 34.101.30-2007). По СТБ 34.101.30-2007 классификации подлежали не информационные системы, а объекты информатизации[10]. Предлагался достаточно сложный многокритериальный подход к отнесению того или иного объекта информатизации к определенному классу: следовало учитывать не только степень конфиденциальности информации, обрабатываемой объектом информатизации, но и организацию вычислительного процесса в объекте информатизации, в частности, размещены ли технические средства обработки информации в одной контролируемой зоне (территории, здании, части здания) или нескольких; имеются ли каналы обмена информацией за пределами контролируемой зоны и являются ли такие каналы открытыми или защищенными; разрабатывается ли комплекс средств безопасности объекта (профиль защиты).

Действующая классификация предлагает более понятные и четкие критерии разграничения информационных систем. Так, для целей классификации СТБ 34.101.30-2017 вводит понятие «типовые информационные системы», под которыми понимаются информационные системы, обрабатывающие один вид информации и функционирующие в одних условиях эксплуатации. Критериями классификации служат (1) вид обрабатываемой информации (категория доступа) и (2) наличие подключения к открытым каналам передачи данных.

Виды информации, на основе которых выделяются классы типовых информационных систем, в целом соответствуют тем, которые рассматривались в разделе 1.2: информация о частной жизни физического лица и персональные данные; охраняемая законом тайна; служебная информация ограниченного распространения; сведения, составляющие государственные секреты.

Открытый канал передачи данных по СТБ 34.101.30-2017 определяется как «комплекс технических средств и общедоступной среды

[10] Понятие объекта информатизации см. в разделе 1.1.

распространения, обеспечивающий передачу данных в виде сигнала электросвязи в определенной полосе частот или с определенной скоростью передачи между сетевыми станциями, сетевыми узлами или между сетевой станцией и сетевым узлом, а также между сетевой станцией или сетевым узлом и оконечным устройством первичной сети» [37].

С 20.02.2020 указанная классификация информационных систем содержится и в Положении о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденном Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 (далее – Положение о порядке технической и криптографической защиты информации).

Устанавливаются следующие классы информационных систем [37; 39]:

1. **Класс 6-частн** –негосударственные[11] информационные системы, в которых обрабатывается общедоступная информация и которые не имеют подключений к открытым каналам передачи данных.

2. **Класс 6-гос** – государственные информационные системы, в которых обрабатывается общедоступная информация и которые не имеют подключений к открытым каналам передачи данных.

3. **Класс 5-частн** – негосударственные информационные системы, в которых обрабатывается общедоступная информация и которые подключены к открытым каналам передачи данных.

4. **Класс 5-гос** – государственные информационные системы, в которых обрабатывается общедоступная информация и которые подключены к открытым каналам передачи данных.

5. **Класс 4-фл** – информационные системы, в которых обрабатывается информация о частной жизни физического лица и персональные данные, иная информация, составляющая охраняемую законом тайну физического лица, распространение и (или) предоставление которой ограничено (подробнее – в разделах 1.2.1, 1.2.4), и которые не имеют подключений к открытым каналам передачи данных.

В соответствии с СТБ 34.101.30-2017 к классу 4-фл относятся также информационные системы, в которых обрабатываются «сведения об исключительном праве (интеллектуальной собственности) физического лица на охраняемые результаты интеллектуальной деятельности».

[11] Государственная информационная система – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц [5].

6. **Класс 4-юл** – информационные системы, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено, за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые не имеют подключений к открытым каналам передачи данных.

В соответствии с СТБ 34.101.30-2017 к классу 4-юл относятся также информационные системы, в которых обрабатывается «информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу», а также «сведения об объектах, в отношении которых исключительные права на результаты интеллектуальной деятельности принадлежат Республике Беларусь».

7. **Класс 4-дсп** – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных. О служебной информации ограниченного распространения подробно – в разделе 1.2.3.

8. **Класс 3-фл** – информационные системы, в которых обрабатывается информация о частной жизни физического лица и персональные данные, иная информация, составляющая охраняемую законом тайну физического лица, распространение и (или) предоставление которой ограничено, и которые подключены к открытым каналам передачи данных.

9. **Класс 3-юл** – информационные системы, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено, за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения, и которые подключены к открытым каналам передачи дынных.

10. **Класс 3-дсп** – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных.

11. **Класс 2** – совокупность информационных систем, связанных с критически важными объектами информатизации.

Понятие объекта информатизации – в разделе 1.1.1.

Объекты информатизации подлежат отнесению к критически важным по установленным критериям значимости и показателями уровня вероятного ущерба в политической, экономической, социальной, информационной, экологической и иных сферах. Критерии значимости определяются Президентом Республики Беларусь, показатели уровня вероятного ущерба – ОАЦ по согласованию с заинтересованными государственными органами [4].

Государственный реестр критически важных объектов информатизации формирует и ведет Оперативно-аналитический центр при Президенте Республики Беларусь.

12. **Класс 1** – совокупность информационных систем, которые обрабатывают информацию, составляющую государственные секреты. Подробно о государственных секретах – в разделе 1.2.2.

Для информационных систем, которые могут быть отнесены к нескольким классам, присвоение класса осуществляется перечислением классов, к которым они могут быть отнесены. Например, регистр населения (см. раздел 1.2.1) отнесен к классу информационных систем 3-фл, 3-юл.

Вопросы для самопроверки

1. Дайте определения понятиям информационной системы и ее компонентов.
2. Какая информация относится к общедоступной?
3. Чем отличается распространение информации от предоставления информации?
4. Какие свойства информации обеспечиваются при организации ее защиты?
5. Какова взаимосвязь между угрозой информационной безопасности и уязвимостью информационной системы?
6. Определите структуру информации, распространение и (или) предоставление которой ограничено.
7. Какие сведения относятся к основным и дополнительным персональным данным в Республике Беларусь?
8. Какие категории информации выделяются в группе государственных секретов?
9. Чем отличается служебная тайна от служебной информации ограниченного распространения и профессиональной тайны?
10. Каким требованиям должны соответствовать сведения, в отношении которых устанавливается режим коммерческой тайны? В отношении каких сведений режим коммерческой тайны устанавливать запрещено?
11. Какими мерами обеспечивается конфиденциальность коммерческой тайны?
12. Какие критерии лежат в основе классификации информационных систем в соответствии с СТБ 34.101.30-2017 «Информационный технологии. Методы и средства безопасности. Информационные системы. Классификация»? Какие классы информационных систем при этом выделяются?

2. ОБЩАЯ ХАРАКТЕРИСТИКА МЕР ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Обеспечение конфиденциальности информации предполагает защиту от ознакомления с ней лиц, не имеющих прав доступа, что обеспечивается комплексом правовых, организационных и технических мер, реализованных в информационной системе.

Разумеется, ни одна система защиты информации не создается исключительно для обеспечения ее конфиденциальности. Основная цель создания систем защиты информации (и информационных систем, в которых информация обрабатывается) – предотвращение следующих действий в отношении информации:

- неправомерного доступа;
- уничтожения;
- модификации (изменения);
- копирования;
- распространения и (или) предоставления информации;
- блокирования правомерного доступа.

В последующем при изложении материала акцент по возможности будет сделан на мерах, направленных непосредственно на обеспечение конфиденциальности информации в сети Интернет. Конкретные меры по обеспечению конфиденциальности информации должны определяться на основании сформированной модели нарушителей (см. раздел 1.1.3).

2.1. Правовые меры обеспечения конфиденциальности информации в сети Интернет

Правовые меры защиты информации – это заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий [5].

Важно понимать, что не во всех случаях для обеспечения конфиденциальности информации требуется применение специальных правовых мер защиты.

Так, защита сведений, составляющих государственные секреты (см. раздел 1.2.2), не обеспечивается правовыми мерами в том смысле, что

не предполагает подписания каких-либо соглашений между обладателем информации (государством) и пользователем информации. Существует специальный юридический механизм – получение допуска.

Обеспечение конфиденциальности служебной информации ограниченного доступа (см. раздел 1.2.3) – должностная обязанность государственных служащих вне зависимости от того, предусмотрена ли она трудовым контрактом.

Защита информации, составляющей охраняемую законом тайну (см. раздел 1.2.4), кроме коммерческой тайны, от предоставления и (или) распространения также должна осуществляться «по умолчанию», в силу требований законодательства. Это значит, что лица, использующие такую информацию для исполнения своих профессиональных обязанностей, должны обеспечивать ее конфиденциальность как без подписания отдельных соглашений с обладателем информации, так и без включения специальных формулировок об этом в иные заключаемые договоры.

Таким образом, применение правовых мер защиты информации для целей обеспечения ее конфиденциальности обязательно только в отношении двух видов сведений: персональных данных (см. раздел 1.2.1) и коммерческой тайны (см. раздел 1.2.3).

Могут применяться два основных типа договоров между обладателем и пользователем информации:

– пользовательские соглашения (соглашения об использовании информационных систем и информационных ресурсов);

– соглашения о конфиденциальности (неразглашении).

Правовые меры обеспечения конфиденциальности информации в сети Интернет должны выполнять две основные задачи:

– не допустить распространения информации ограниченного доступа в сети Интернет лицами, которые имеют права доступа к такой информации. На решение такой задачи направлены различные соглашения о конфиденциальности (неразглашении);

– надлежащим образом оформить передачу информации ограниченного распространения по сети Интернет, что, как правило, обеспечивается пользовательскими соглашениями.

2.1.1. Пользовательские соглашения

Основная цель пользовательского соглашения – снизить риски юридической ответственности, возникающие в связи с использованием информационных ресурсов и информационных систем. Самый простой пример

пользовательского соглашения – это распространенные «политики конфиденциальности», которые, впрочем, затрагивают очень узкий аспект – правила сбора и обработки персональных данных пользователя.

Чаще пользовательские соглашения относятся к смешанным договорам – соглашениям, в которых содержатся элементы различных договоров, предусмотренных законодательством. Таким образом, обеспечение конфиденциальности информации, обрабатываемой в информационной системе, – не единственная и не основная задача пользовательского соглашения.

Обычно пользовательские соглашения представляют собой договоры присоединения, т.е. договоры, условия которых определены одной стороной в стандартной форме и могут быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом (статья 398 ГК) [40] без внесения каких-либо изменений и дополнений.

Примером такого договора является пользовательское соглашение между владельцем интернет-ресурса[12], посредством которого распространяется массовая информация[13], и пользователем (далее в этом разделе – пользовательское соглашение). Такое пользовательское соглашение определяет условия использования интернет-ресурса, а также взаимные права и обязанности сторон.

Базовые условия пользовательского соглашения установлены Положением о порядке предварительной идентификации пользователей интернет-ресурса, сетевого издания, утвержденного Постановлением Совета Министров Республики Беларусь от 23.11.2018 № 850 [41] (далее в этом разделе – Положение), а также Законом о средствах массовой информации [12]. В результате анализа этих актов можно сделать несколько выводов, важных для области обеспечения конфиденциальности информации в сети Интернет.

1. В силу требований законодательства размещение пользователями на интернет-ресурсе информационных сообщений и материалов без их предварительной идентификации не допускается.

Активация учетной записи на интернет-ресурсе может осуществляться исключительно путем отправки кода активации в SMS-сообщении на указанный пользователем номер телефона. Использование иных идентификационных данных и технических средств возможно только в том случае,

[12] Под интернет-ресурсом здесь понимается интернет-сайт, страница интернет-сайта, форум, блог, приложение для мобильного устройства, иной информационный ресурс (его составная часть), размещенный в глобальной компьютерной сети Интернет, посредством которых распространяется массовая информация [12].

[13] Понятие массовой информации определено в разделе 1.1.

когда такие данные и средства позволяют идентифицировать личность пользователя (например, указания одного только обезличенного адреса электронной почты уже недостаточно). Кроме того, Положение не позволяет регистрировать на интернет-ресурсе более одной учетной записи с использованием одного номера телефона (одного комплекта иных идентификационных данных).

Должна также предусматриваться и невозможность размещения пользовательскую информацию анонимно.

Владелец интернет-ресурса вправе при проведении предварительной идентификации пользователя собирать, обрабатывать и хранить следующие персональные данные такого лица: фамилию, собственное имя, отчество (если имеется), пол, число, месяц, год рождения, место рождения, а также номер мобильного телефона и (или) адрес электронной почты.

Таким образом, учитывая характер получаемых данных, пользовательское соглашение обязательно должно обеспечивать получение активного письменного согласия физического лица на обработку персональных данных.

2. Владелец интернет-ресурса на время действия пользовательского соглашения, а также в течение года с даты его расторжения обязан обеспечить хранение на физически размещенных на территории Республики Беларусь серверах следующей информации:

– сведений, полученных при предварительной идентификации пользователя;

– сведений о размещении и изменении пользователем сообщений и материалов, дате и времени их размещения и изменения;

– сведений о сетевом (IP) адресе устройства пользователя, присвоенном при регистрации пользователя на интернет-ресурсе, внесении изменений в регистрационные данные пользователя;

– иных сведений, полученных владельцем интернет-ресурса при идентификации пользователя.

Таким образом, информационная система, элементом которой является описываемый интернет-ресурс, в связи с обработкой в ней значительного объема персональных данных (см. раздел 1.2.1) должна быть отнесена к классу 3-фл (см. раздел 1.3) и обеспечена специальной системой защиты информации (см. раздел 2.4).

3. Информация, предоставленная пользователем владельцу интернет-ресурса, может быть передана по законному требованию органов, осуществляющих оперативно-розыскную деятельность, органов прокуратуры

и предварительного следствия, органов Комитета государственного контроля, Министерства информации, налоговых органов, судов. Полагаем разумным включать предупреждение об этом в текст пользовательского соглашения.

4. Пользователь имеет право безо всяких ограничений расторгнуть в одностороннем порядке пользовательское соглашение в любое время.

В то же время владелец интернет-ресурса может расторгнуть пользовательское соглашение в одностороннем порядке (фактически – запретить пользователю размещать информацию на интернет-ресурсе) только в двух случаях:

– в случае получения от уполномоченных государственных органов сведений о том, что пользователь при регистрации учетной записи указал не соответствующую действительности информацию (исключение – допущенные грамматические ошибки);

– в случае использования при регистрации учетной записи информации, противоречащей требованиям законодательства Республики Беларусь, в т.ч. нарушающей права и законные интересы третьих лиц.

О факте расторжения пользовательского соглашения владельцем интернет-ресурса пользователю направляется уведомление в SMS-сообщении на номер телефона либо с использованием иных идентификационных данных и технических средств, позволяющих обеспечить информирование пользователя.

Такие действия владельца интернет-ресурса могут быть обжалованы пользователем в суде в месячный срок со дня получения такого уведомления.

5. Владелец интернет-ресурса обязан анализировать содержание интернет-ресурса, не допуская размещения:

– информации, распространение которой запрещено (например, сведения, пропагандирующие употребление наркотических средств; информация о способах изготовления взрывных устройств; информация, побуждающая к самоубийству; ненадлежащая реклама; информация о несовершеннолетних, пострадавших в результате противоправных действий и т.д. (полный перечень содержится в статье 38 Закона о средствах массовой информации [12]);

– недостоверной информации, которая может причинить вред государственным или общественным интересам (например, о посягательствах на независимость, территориальную целостность и суверенитет Республики Беларусь; о подготовке или осуществлении террористических актов [42]);

– сведений, не соответствующих действительности и порочащих честь, достоинство или деловую репутацию физических лиц либо деловую репутацию юридических лиц;

– материалов, содержащих нецензурные слова и выражения.

Пользовательское соглашение обязательно должно содержать предупреждение о недопустимости размещения пользователем вышеуказанной информации на интернет-ресурсе.

Здесь важно понимать, что информация, предоставление и (или) распространение которой ограничено, не относится к информации, распространение которой запрещено (это разные юридические категории), поэтому пользовательское соглашение не защищает обладателя информации ограниченного доступа от ее разглашения. Иными словами, собственник информационной системы в силу пользовательского соглашения не несет ответственности за размещение пользователями на интернет-ресурсе государственных секретов, служебной информации ограниченного распространения, охраняемой законом тайны, персональных данных иных лиц. Ответственность за такие действия несет пользователь.

2.1.2. Соглашения о конфиденциальности

Соглашения о конфиденциальности (в иной терминологии – соглашение о неразглашении (NDA), соглашение о раскрытии секретности (CDA), соглашение об имущественных правах на информацию (PIA)) могут охватывать самый широкий круг сведений – от коммерческой тайны нанимателя или третьих лиц до персональных данных [35].

Соглашения о конфиденциальности касаются только ограниченного перечня информации, указанного в самом соглашении, и не вводят какого-либо общего режима конфиденциальности в отношении всей информации, которая обрабатывается информационными системами той или иной организации.

Закон о коммерческой тайне соглашениями о конфиденциальности называет только гражданско-правовой договор между владельцем коммерческой тайны и контрагентом. Договоры с лицами, состоящими в трудовых отношениях с владельцем коммерческой тайны, или лицом, получившим к ней доступ, именуются обязательствами о неразглашении коммерческой тайны [33].

Соглашение о конфиденциальности заключается владельцем коммерческой тайны в письменной форме с третьими лицами (контрагентами) и могут сопровождать самые разнообразные гражданско-правовые

договоры: лицензионные договоры и прочие договоры, связанные с объектами интеллектуальной собственности; договоры подряда; договоры на выполнение научно-исследовательских и опытно-конструкторских работ; договоры о совместной деятельности; договоры купли-продажи предприятий, ценных бумаг и т.п. [35].

Соглашение о конфиденциальности может существовать как в виде отдельного документа, подписанного до заключения основного договора, так и быть включенным в текст самого договора с контрагентом.

Обязательными условиями соглашения о конфиденциальности является перечень информации, составляющей коммерческую тайну (или иной способ определения такой информации), пределы использования такой информации, а также срок, в течение которого контрагент обязан обеспечивать ее конфиденциальность.

Средством защиты от нарушения контрагентом соглашения о конфиденциальности является возмещение убытков и (или) установление штрафа за разглашение коммерческой тайны.

Обязательство о неразглашении коммерческой тайны может подписываться с работником только при наличии трудового договора с нанимателем (владельцем коммерческой тайны или лицом, получившим доступ к коммерческой тайне). Обязательство о неразглашении оформляется в виде отдельного документа. Включать его в текст трудового договора (контракта) не следует, поскольку обязательство может продолжать действовать и после прекращения действия трудового договора. Отказ работника от подписания обязательства о неразглашении является основанием для его увольнения на основании пункта 6 статьи 47 Трудового кодекса Республики Беларусь [43] (далее – ТК).

Обязательство о неразглашении коммерческой тайны не может быть подписано с лицом, не являющимся работником организации, т.е. при отсутствии заключенного трудового договора (контракта), как это имеет место в случае со стажерами и студентами, направленными в организацию для прохождения производственной или преддипломной практики. Предполагается, что доступ к конфиденциальной информации таким лицам должен быть закрыт.

Организация, заключившая соглашение о конфиденциальности, может, в свою очередь, взять со своих работников обязательства о неразглашении.

Обязательство о неразглашении коммерческой тайны может предполагать как позитивное (условие о выплате вознаграждения за его выполнение), так и негативное (условие об ответственности за его нарушение) стимулирование работника. В последнем случае рекомендуется [35] устанавливать

штраф. Взыскание штрафа при этом не лишает нанимателя права, во-первых, на основании ТК привлечь работника к материальной ответственности за разглашение коммерческой тайны, обязав возместить причиненный ущерб; во-вторых, применить к работнику меры дисциплинарной ответственности (в т.ч. увольнение по пункту 6 статьи 47 ТК [43]).

Как и соглашение о конфиденциальности, обязательство о неразглашении действует в течение определенного в нем срока либо до отмены режима коммерческой тайны в отношении составляющих ее сведений.

И работник организации, и контрагент обязаны незамедлительно сообщить владельцу коммерческой тайны о следующих допущенных ими либо ставших известными им фактах [33]:

– о факте незаконного ознакомления со сведениями, составляющими коммерческую тайну;

– о факте незаконного использования этих сведений;

– о факте разглашения коммерческой тайны или угрозы разглашения коммерческой тайны третьими лицами;

– о требованиях доступа к коммерческой тайне со стороны государственных органов и иных лиц.

Несмотря на то, что белорусское законодательство прямо упоминает соглашения о конфиденциальности только применительно к коммерческой тайне, это не означает запрета использовать такую юридическую конструкцию для защиты иных сведений ограниченного распространения (например, персональных данных).

2.2. Организационные меры обеспечения конфиденциальности информации в сети Интернет

Для обеспечения конфиденциальности информации могут применяться следующие организационные меры защиты:

1. Специальный режим допуска на территории, в помещения организации, где может быть доступна конфиденциальная информация или материальные носители конфиденциальной информации.

В качестве примеров таких мер приводятся [22, с. 34–35; 45; 46]:

– ограничение доступа в помещения, в которых происходит обработка конфиденциальной информации (организация проходной, пропускная система, карты доступа, регистрация фактов входа-выхода, контроль входящих и исходящих материальных ценностей и т.п.);

– установка систем обнаружения проникновений (например, сигнализаций, видеонаблюдения и т.п.);

– отсутствие очевидных идентификаторов (например, табличек, иных вывесок) на помещениях, в которых организовано хранение и обработка конфиденциальной информации;

– отделение средств обработки информации, используемых в организации, от средств обработки информации, управляемых третьими лицами (например, недопустимость создания общих помещений для копирования документов, общих архивных помещений и т.п.);

– выделение одного или нескольких средств обработки информации исключительно для работы с конфиденциальной информацией; регламентация порядка работы с такими средствами;

– хранение носителей информации в тщательно закрытых прочных шкафах или сейфах с авторизованным доступом;

– шифрование информации при резервном копировании;

– анонимизация носителей (сотрудники, имеющие доступ к носителям, не знают, какая информация на каком носителе записана, и управляют только анонимными номерами носителей; сотрудники, которые знают, какая информация находится на конкретном носителе, не имеют доступа к хранилищу носителей);

– установка дисплея, клавиатуры и принтера под ограниченным углом обзора, чтобы исключить просмотр информации лицами, не имеющими прав доступа;

– постоянное наблюдение за работой принтера и других устройств вывода конфиденциальной информации на материальные носители;

– уничтожение выведенных из эксплуатации дисков или иных материалов, содержащих фрагменты конфиденциальной информации;

– запрет ведения переговоров о непосредственном содержании конфиденциальной информации лицами, занятыми ее обработкой;

– ограничение доступа внутрь корпуса компьютера путем установления механических запорных устройств;

– уничтожение всей информации на дисках компьютера в случае необходимости ремонта техники (необходимо использовать средства низкоуровневого форматирования);

– отключение компьютера от локальной сети или сети удаленного доступа при обработке на нем конфиденциальной информации, кроме случаев передачи этой информации по сети;

– установка специального программного обеспечения, препятствующего запуску посторонних программ, кроме назначенных администратором

(принцип «любому лицу предоставляются привилегии, необходимые для выполнения конкретных задач, но не больше»);

– установка принтера и клавиатуры на мягкие прокладки с целью снижения утечки информации по акустическому каналу, а также включение устройств, создающих дополнительный шумовой фон (кондиционеры, вентиляторы) при обработке конфиденциальной информации на компьютере;

– разработка порядка действий с конфиденциальной информацией в случаях аварийных и чрезвычайных ситуаций.

2. Разграничение доступа к информации по кругу лиц и характеру информации.

Правила управления доступом и права доступа для каждого пользователя или группы пользователей следует определять в политике управления доступом [46]. Систему управления доступом следует основывать на предпосылке «все запрещено, если явно не разрешено», а не на более мягком правиле «все разрешено, если явно не запрещено».

Выделяются два основных подхода к разграничению доступа по кругу лиц и характеру информации: избирательный и полномочный.

Избирательный способ управления доступом характеризуется задаваемым администратором множеством разрешенных отношений доступа (например, в виде троек: объект, субъект, тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основании матрицы, в которой столбец соответствует объекту системы, а строка – субъекту. На пересечении столбца и строки указывается тип разрешенного доступа субъекта к объекту (например, «доступ на чтение», «доступ на запись», «доступ на исполнение» и т.п.) [11, с. 23].

Полномочный (мандатный) способ управления доступом заключается в совокупности правил предоставления доступа, базирующихся на множестве атрибутов безопасности субъектов и объектов (например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя). При таком способе управления доступом все субъекты и объекты системы однозначно идентифицированы; каждому объекту системы присвоена метка конфиденциальности, определяющая ценность содержащейся в ней информации; каждому субъекту системы присвоен некий уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ. Таким образом, полномочный способ управления доступом позволяет более гибко регулировать доступ к объектам с различными уровнями конфиденциальности,

предотвращать утечку информации с верхних уровней должностной иерархии на нижние и блокировать возможные проникновения с нижних уровней на верхние [11, с. 22–23].

В качестве примеров конкретных организационных мер по разграничению доступа могут быть приведены следующие [45; 22, с. 151–152]:

– разделение обязанностей в области управления доступом (например, запрос, авторизация и администрирование доступа);

– обязательное использование процедуры регистрации (учетной записи) пользователя при предоставлении доступа и отмене доступа ко всем информационным системам организации;

– лишение пользователей прав локального администратора на их рабочих местах;

– использование по общему правилу уникальных идентификаторов пользователей (использование групповых идентификаторов должно быть разрешено только там, где они необходимы);

– применение сложных паролей на уровне операционных систем и программного обеспечения (минимальная длина – 15 символов), периодическая смена паролей, надежное хранение паролей;

– официальная запись (фиксация) всех лиц, получавших доступ к информационной системе, в которой обрабатывается конфиденциальная информация;

– немедленное удаление (блокировка) прав доступа пользователей, которым изменили обязанности (должность) или покинувшим организацию;

– немедленное удаление (блокировка) прав доступа контрагентов к информационной системе после прекращения договоров с ними;

– определение санкций за попытки неавторизованного доступа;

– разработка правил использования сетей и сетевых услуг;

– осуществление проверки вводимой информации для доступа в систему только по окончании ввода всех входных данных (при ошибочном вводе система не должна указывать, какая часть данных является неверной);

– ограничение числа неудачных попыток входа в систему;

Дополнительно о разграничении доступа – в главе 4.

Реализация организационных мер защиты информации осуществляется в целях выполнения требований, изложенных в локальных нормативных правовых актах собственника (владельца) информационной системы, которые доводятся до сведения субъектов информационной системы под роспись [5].

2.3. Технические меры обеспечения конфиденциальности информации в сети Интернет

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации [5].

Дополнительные организационные и технические меры, соответствующие более конкретным задачам обеспечения конфиденциальности информации в сети Интернет, будут описаны в пособии далее – в разделах 4–11.

Вопросы для самопроверки

1. Дайте краткую характеристику правовым мерам защиты информации.
2. Чем отличается пользовательское соглашение от соглашения о конфиденциальности? Является ли соглашением политика конфиденциальности, размещенная на интернет-ресурсе?
3. Чем отличается соглашение о конфиденциальности от обязательства о неразглашении?
4. Допустимо ли увольнение работника в связи с его отказом от подписания обязательства о неразглашении?
5. Какие сведения о пользователе обязан хранить владелец интернет-ресурса, размещенного на серверах в Республике Беларусь? В течение какого срока должна храниться такая информация?
6. Приведите примеры организационных мер, направленных на обеспечение конфиденциальности информации в сети Интернет.
7. Какой способ управления доступом к информации по кругу лиц и характеру информации вы считаете более эффективным? Ответ обоснуйте.

3. ОРГАНИЗАЦИЯ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Принципы организации системы технической защиты информации

При создании системы защиты информации рекомендуется [47, с. 5–9; 11, с. 50] опираться на следующие принципы:

(1) системности;

(2) комплексности;

(3) непрерывности защиты;

(4) разумной достаточности;

(5) гибкости управления и применения;

(6) открытости;

(7) простоты применения защитных мер и средств;

(8) законности;

(9) персональной ответственности.

Принцип системности подразумевает создание и контроль функционирования системы защиты информации (информационной системы):

– при всех видах информационной деятельности (поиск, получение, передача, сбор, обработка, накопление, хранение, распространение (предоставление), пользование) и в отношении всех форм информации;

– для всех структурных элементов информационной системы;

– во всех режимах функционирования информационной системы;

– на всех этапах жизненного цикла информации (информационной системы);

– с учетом всех возможных объектов, угроз и направлений атак;

– с учетом взаимодействия объекта защиты с внешней средой.

Принцип комплексности требует согласования разнородных средств технической и криптографической защиты информации для построения единого целостного комплекса, не содержащего слабых мест на стыках его отдельных элементов.

Принцип непрерывности защиты предполагает не только проведение разовых мероприятий по организации комплекса защиты информации, но и поддержание непрерывного процесса его функционирования, включая постоянный мониторинг и контроль. Даже кратковременные перерывы

в работе системы защиты информации могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, а также внедрения программных и аппаратных средств преодоления системы защиты после восстановления ее функционирования.

Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

Принцип разумной достаточности основан на убеждении, что создать абсолютно непреодолимую систему защиты принципиально невозможно: при достаточном количестве времени и средств можно преодолеть любую защиту, поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности ресурсов, может создавать дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

В соответствии с **принципом гибкости** принятые меры и установленные средства защиты должны быть приспособлены к изменяющимся условиям функционирования информационной системы, а также к изменениям в самой информационной системе.

Принцип открытости предполагает, что защита не должна обеспечиваться только за счет секретности структуры информационной системы и алгоритмов обработки информации. Даже знание алгоритма работы системы защиты не должно давать возможности ее преодоления, в т.ч. разработчику. Однако это совсем не означает, что информация о конкретной системе должна быть общедоступна – необходимо обеспечивать защиту и от угрозы раскрытия параметров системы.

Принцип простоты применения средств защиты предполагает, что механизмы защиты должны быть интуитивно понятны и просты в использовании.

Принцип законности обеспечивается соблюдением всех требований нормативных правовых, в т.ч. технических, актов, а также, при необходимости, международных актов и стандартов построения системы защиты информации.

Принцип персональной ответственности требует распределения ответственности за обеспечение защиты информации между всеми участниками информационных отношений в соответствии с имеющимися у них правами и возложенными на них обязанностями.

3.2. Требования по организации системы технической защиты информации

Основы технической и криптографической защиты информации устанавливаются Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (с 14 марта 2020 г. действует в новой, существенно обновленной, редакции) [4].

На объектах информатизации, предназначенных для обработки информации, содержащей государственные секреты, создание системы защиты информации осуществляется в порядке, предусмотренном законодательством о государственных секретах. В рамках настоящего пособия эта сфера правового регулирования рассматриваться не будет.

Информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, должна обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь [5]. Наличие аттестата подтверждает, что система защиты информации соответствует требованиям законодательства об информации, информатизации и защите информации (о проектировании, создании и аттестации системы защиты информации – в разделе 3.3).

В отношении информации, распространение и (или) предоставление которой ограничено (см. раздел 1.2), ее защита организуется следующими субъектами:

– собственником или оператором информационной системы, содержащей такую информацию;

– обладателем информации, если такая информация не содержится в информационных системах.

В случае, если государственным органом или юридическим лицом осуществляется обработка информации, распространение и (или) предоставление которой ограничено, в организации должно быть определены подразделения или должностные лица, ответственные за обеспечение защиты информации [5]. С 14 марта 2020 г. работники такого подразделения (должностное лицо) должны иметь определенную квалификацию:

– иметь высшее образование в области защиты информации;

– иметь высшее или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством [4].

Для организации защиты информации также может быть привлечена сторонняя специализированная организация, имеющая специальное разрешение (лицензию) на деятельность по технической и (или) криптографической защите информации.

К слову, если работы по проектированию и созданию системы защиты информации будут выполняться специализированными организациями с использованием открытых каналов передачи данных (сетей электросвязи общего пользования), вводится требование о применении средств криптографической защиты информации, обеспечивающих линейное шифрование передаваемой информации [39].

Порядок создания системы технической и криптографической защиты информации, предоставление и (или) распространение которой ограничено, устанавливается Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [44] (далее – Приказ № 66), которым утверждены положения, касающиеся технической и криптографической защиты информации ограниченного распространения (кроме государственных секретов), в т.ч. на критически важных объектах информатизации, а также порядок аттестации систем защиты информации.

Для выполнения требований Приказа № 66 существует группа государственных стандартов серии СТБ 34.101 (в настоящее время действует 61 стандарт, перечень содержится в Приложении 1 к настоящему пособию).

Дополнительные обязанности по защите информации могут содержаться также и в иных актах законодательства. Например, Положением о порядке определения уполномоченных поставщиков интернет-услуг [48] устанавливается перечень более строгих требований к хостинг-провайдерам, интернет-провайдерам, оказывающим услуги государственным органам.

Помимо этого, действует серия международных стандартов ISO/IEC 27000, включающая стандарты по информационной безопасности, опубликованные совместно Международной организацией по стандартизации (International Organization for Standardization, ISO) и Международной электротехнической комиссии (International Electrotechnical Commission, IEC). Серия содержит лучшие практики и рекомендации для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ) и предназначена для содействия организациям при создании систем защиты финансовой информации, интеллектуальной собственности,

сведений о сотрудниках или информации, доверенной потребителями или контрагентами [49, с. IV]. В серии 27000 в настоящее время опубликовано 46 международных стандартов.

СМИБ – система политик, процедур и руководящих указаний, а также связанных с ними ресурсов, необходимых для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности организации. СМИБ использует подход, основанный на бизнес-рисках, где под риском информационной безопасности понимается потенциальная возможность того, что угроза использует уязвимость и тем самым станет причиной причинения ущерба организации.

В Республике Беларусь введено и действует 7 государственных стандартов серии СТБ ISO/IEC 27000 (Приложение 2), идентичных международным по техническому содержанию и структуре (за исключением минимальных редакционных изменений). Ключевыми стандартами для создания СМИБ в организации являются:

– СТБ ISO/IEC 27000-2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь» [49];

– СТБ ISO/IEC 27001-2016 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [50].

Соответствие созданной в организации системы защиты информации (системы менеджмента информационной безопасности) стандарту СТБ ISO/IEC 27001-2016 можно подтвердить в рамках Национальной системы подтверждения соответствия Республики Беларусь с выдачей соответствующего сертификата. В настоящее время такая сертификация носит добровольный характер и предполагает проведение аудита (при необходимости – в несколько этапов) [51].

На практике система защиты информации может соответствовать всем требованиям ISO, но это не означает, что она соответствует требованиям ОАЦ, и наоборот, хотя во многом эти требования дублируются.

Применение особых мер по защите информации ограниченного распространения может потребоваться также в силу норм международного права. Типичный и актуальный пример для Беларуси – требования Общего регламента защиты персональных данных Европейского союза (EU General Data Protection Regulation, Регламент GDPR), вступившего в силу 25 мая 2018 г. (см. раздел 3.3).

3.3. Выстраивание системы технической защиты информации, распространение и (или) предоставление которой ограничено

Для каждой информационной системы, предназначенной для обработки информации, распространение и (или) предоставление которой ограничено, необходимо создавать отдельную систему защиты. Исключение составляют два случая [52]:

– когда несколько информационных систем функционируют в общей программно-технической среде и принадлежат одному собственнику (владельцу);

– когда одному собственнику (владельцу) принадлежит несколько типовых информационных систем.

Для организации системы технической защиты информации необходимо пройти три этапа [39]:

– проектирование системы защиты информации;

– создание системы защиты информации;

– аттестацию системы защиты информации.

Однако прежде чем приступить к проектированию системы защиты информации, собственник (владелец) информационной системы должен определить виды обрабатываемой информации (категории доступа) и отнести информационную систему к определенному классу типовых информационных систем (см. раздел 1.2). Итоговый результат оформляется актом типовой формы [39].

3.3.1. Проектирование системы защиты информации

На этапе проектирования системы защиты информации необходимо [39] (рисунок 3.1):

1. Проанализировать структуру информационной системы и информационных потоков, определив:

– состав (количество) и места размещения элементов информационной системы (как аппаратных, так и программных);

– физические и логические границы информационной системы.

В последующем эти параметры найдут отражение в общей схеме системы защиты информации (см. ниже).

2. Разработать (или произвести корректировку) политики информационной безопасности организации.

Политика информационной безопасности организации – это общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, документально закрепленные собственником (владельцем) информационной системы [39].

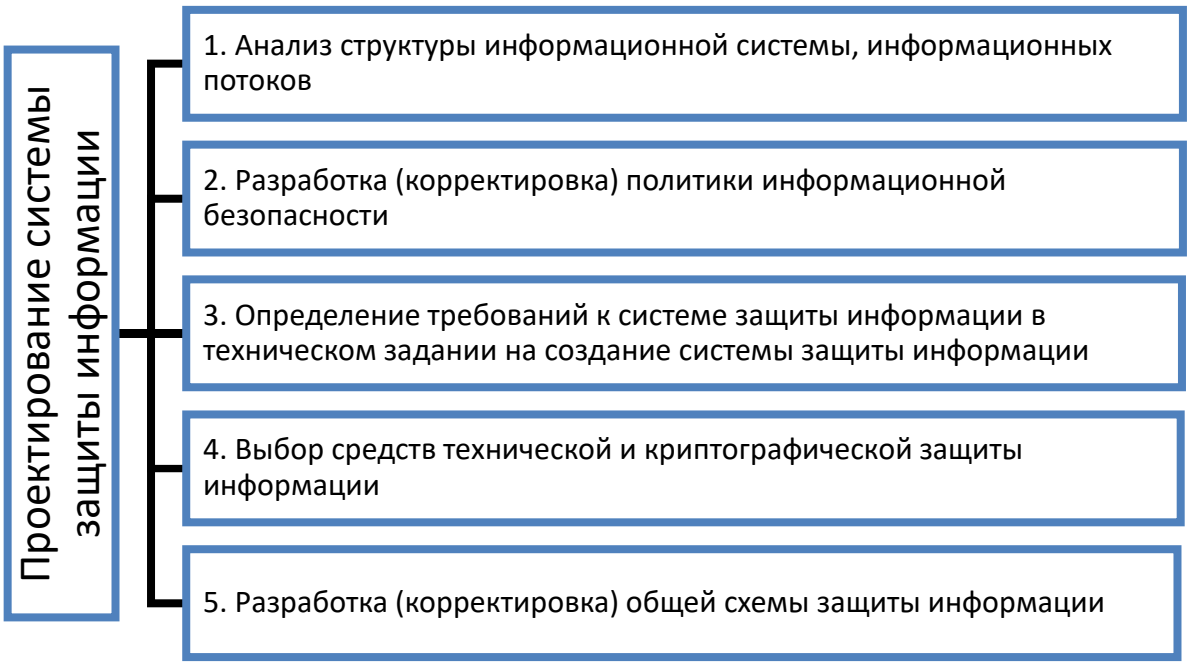


Рисунок 3.1. – Этапы проектирования системы защиты информации

Законодательные требования, предъявляемые к политике информационной безопасности организации, не слишком обширны [39].

Во-первых, политика информационной безопасности должна содержать цели и принципы создания системы защиты информации.

В части формулирования целей документ должен отвечать на вопрос «Для чего создается система защиты информации в организации?» или «Чего необходимо достичь?»: для соблюдения требований национального законодательства и международных договоров? для повышения конкурентоспособности бизнеса за счет дополнительных гарантий безопасности? для согласованности действий по обеспечению информационной безопасности и распределения ответственности внутри организации? для достижения адекватности, в том числе экономической целесообразности, мер защиты от угроз информационной безопасности? для снижения рисков юридической ответственности, возникающих в результате использования информационной системы? для повышения осведомленности в вопросах обеспечения защиты информации в организации?

Перечень таких вопросов (следовательно, и целей создания системы защиты информации) может быть гораздо шире.

Очевидно, что политика информационной безопасности не должна быть декларативной. Напротив, документ должен стать основой для построения эффективной стратегии обеспечения информационной безопасности.

Скажем, если организация в силу специфики своей деятельности ставит целью доступность посредством сети Интернет своих информационных систем, то в этом случае составляющими элементами стратегии безопасности должны стать уменьшение вероятности заражения информационной системы вирусами и ограничение взаимодействия открытых информационных систем с информационными системами, содержащими информацию ограниченного доступа.

Если в качестве цели создания системы безопасности выделяются конкурентные преимущества бизнеса (например, возможность продемонстрировать контрагентам защищенность информационной системы), то частью стратегии будет сертификация информационной системы.

Наконец, если организация выделяет в качестве цели намерение повысить осведомленность сотрудников в вопросах информационной безопасности и распределить ответственность, следует позаботиться о подготовке четких и понятных должностных инструкций, об описании ключевых процедур деятельности по всем основным направлениям.

О принципах защиты информации, на которых может базироваться политика информационной безопасности, – см. раздел 3.1.

Во-вторых, политика информационной безопасности должна содержать следующие данные:

– перечень информационных систем с отнесением их к тому или иному классу типовых информационных систем;

– перечень отдельно стоящих электронных вычислительных машин, используемых в организации и принадлежащих ей на праве собственности (ином законном основании);

– указание на подразделение защиты информации (иное подразделение, должностное лицо), ответственное за обеспечение защиты информации.

В-третьих, в политике информационной безопасности необходимо прописать обязанности пользователей информационной системы. Перечень пользователей следует определить заранее, при анализе структуры информационной системы и информационных потоков.

В-четвертых, если предполагается взаимодействие информационной системы организации с иными информационными системами (в т.ч. при осуществлении информационных отношений на правах операторов, посредников, пользователей информационных систем и обладателей информации), в политике необходимо прописать порядок такого взаимодействия.

Общий макет, по которому рекомендуется [53, с. 32] строить политику информационной безопасности, выглядит следующим образом:

– вводный раздел, подтверждающий заинтересованность высшего руководства проблемами информационной безопасности, а также содержащий цели и принципы защиты информации;

– организационный раздел с описанием структурных подразделений, комиссий, групп, ответственных за информационную безопасность;

– классификационный раздел, описывающий материальные и информационные ресурсы организации и необходимый уровень их защиты;

– штатный раздел, описывающий должности работников, ответственных за информационную безопасность, а также порядок реагирования работников на инциденты информационной безопасности и порядок организации обучения работников;

– раздел, освещающий вопросы физической защиты информации;

– раздел управления, описывающий подход к управлению компьютерами и сетями передачи данных;

– раздел, описывающий правила разграничения доступа к информации;

– раздел, описывающий порядок разработки и внедрения систем;

– раздел, описывающий меры, направленные на обеспечение непрерывной работы организации (доступности информации);

– юридический раздел, подтверждающий соответствие политики информационной безопасности текущему законодательству.

Развернутая структура политики информационной безопасности организации также предлагается СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности» [46, с. 12]. В частности, политика может предусматривать разъяснение конкретных положений и принципов обеспечения информационной безопасности (например, законности, системности, полноты (комплексности), непрерывности, равнопрочности, разумной достаточности, управляемости, персональной ответственности и т.п.); ссылки на «поддерживающую» политику документацию (например, процедуры защиты отдельных элементов информационной системы; правила безопасности, которым должны следовать пользователи и т.п.).

Вместе с тем в политике информационной безопасности следует избегать излишней детализации, поскольку по своей сути это все-таки общие намерения и направления деятельности, а не пошаговые инструкции.

3. Определить требования к системе защиты информации в **техническом задании** на создание системы защиты информации (далее – техническое задание).

Техническое задание должно содержать следующие информационные блоки:

(1) Данные об информационной системе: наименование и присвоенный класс типовых информационных систем.

(2) Перечень требований к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем.

Полный перечень таких требований содержится в Приложении 3 к Положению о порядке технической и криптографической защиты информации [39]. Часть из этих требований является обязательной, часть – носит характер рекомендации. Например, предусмотреть средства обеспечения конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи, обязательно только для информационных систем классов «дсп» – 4-дсп, 3-дсп (используемая технология здесь – криптографические токены). Обеспечивать централизованный сбор и хранение информации о событиях информационной безопасности в течение определенного срока хранения обязательно только в информационных системах класса 3-дсп, однако такие меры допустимо предусмотреть и в техническом задании на систему защиты информации в информационной системе любого класса. Некоторые требования логически вытекают из типа конкретной информационной системы: например, информационные системы классов 4-го типа не требуют обеспечивать конфиденциальность и контроль целостности информации при ее передаче посредством сетей электросвязи общего пользования по причине отсутствия в таких информационных системах подключений к открытым каналам передачи данных.

(3) Сведения об организации взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия).

Для взаимодействия информационных систем также существуют определенные правила, закрепленные в Приложении 4 к Положению о порядке технической и криптографической защиты информации [39; 44]. Например, не допускается какое-либо взаимодействие информационных систем 4-го и 5-го типов, 3-го и 6-го типов, 4-го и 3-го типов. Информационные системы 4-го и 6-го типов, а также 4-го типа между классами могут взаимодействовать только с использованием физически выделенного канала передачи данных.

(4) Требования к средствам криптографической защиты информации, включая требования:

– к криптографическим алгоритмам в зависимости от задач безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита);

– к криптографическим протоколам;

– к управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение);

– к функциональным возможностям безопасности;

– к форматам данных.

Профили требований, предъявляемых к средствам криптографической защиты информации, определяются ОАЦ.

(5) Перечень документации на систему защиты информации (перечень обязательных локальных нормативных правовых актов см. в разделе 3.2.2).

Разработанное техническое задание, за исключением указанного выше случая, до процедуры аттестации системы защиты информации в ОАЦ не предоставляется и не требует сторонней оценки в испытательных лабораториях.

При этом требования к системе защиты информации, которые указаны в качестве обязательных, могут не включаться в техническое задание только в двух случаях: если в информационной системе отсутствует соответствующий объект (технология); если предусматриваются обоснованные компенсирующие меры. В последнем случае нельзя избежать специального согласования технического задания с ОАЦ.

Собственник (владелец) информационной системы может разработать техническое задание самостоятельно, и если эта работа выполняется для собственных нужд, то наличие лицензии на осуществление деятельности по технической защите информации не требуется [19]. Второй вариант – обратиться в специализированную организацию, имеющую выданную ОАЦ лицензию на осуществление деятельности по технической защите информации [19][14].

4. Выбрать средства технической и криптографической защиты информации (понятия средств технической и криптографической защиты информации см. в разделе 1.1.3).

При необходимости может составляться задание на закупку сертифицированных (или прошедших экспертизу) средств защиты информации.

[14] Перечень специализированных организаций размещен на сайте ОАЦ по ссылке: https://oac.gov.by/activity/licensing/technical-and-cryptographic-information-protection/licensee.

Для создания системы защиты информации, распространение и (или) предоставление которой ограничено, разрешается [4] использовать только средства технической и криптографической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы ОАЦ[15].

5. Разработать общую схему системы защиты информации, которая должна содержать:

– наименование информационной системы и ее класс типовых информационных систем;

– места размещения объектов информационной системы (средств вычислительной техники, сетевого оборудования, системного и прикладного программного обеспечения, средств технической и криптографической защиты информации);

– физические границы информационной системы;

– внешние и внутренние информационные потоки, протоколы обмена защищаемой информацией.

До 14 марта 2020 г. требование о составлении общей схемы системы защиты информации не было обязательным, однако собственники (владельцы) информационных систем нередко использовали такой способ представления данных при оформлении структуры информационной системы. Если схема была подготовлена ранее, на стадии проектирования системы защиты информации ее следует пересмотреть и при необходимости произвести корректировку в соответствии с требованиями законодательства.

3.3.2. Создание системы защиты информации

На этапе создания системы защиты информации необходимо (рисунок 3.2):

1. Внедрить средства технической и криптографической защиты информации, которые были выбраны на первом этапе.

---

[15] Технические требования к средствам защиты информации, выпускаемым в обращение на территории Республики Беларусь, а также порядок подтверждения их соответствия требованиям информационной безопасности и маркировки знаком соответствия установлены Техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) [54]. Перечень технических нормативных правовых актов, взаимосвязанных с ТР 2013/027/BY, содержится в Приказе ОАЦ от 12.03.2020 № 77 [55]. Описание общего порядка проведения экспертизы и сертификации можно изучить по следующим ссылкам: https://oac.gov.by/activity/expertise/technical-and-cryptographic-information-protection/examination-procedure; https://oac.gov.by/activity/certification/technical-and-cryptographic-information-protection/certification-of-information-security-tools.

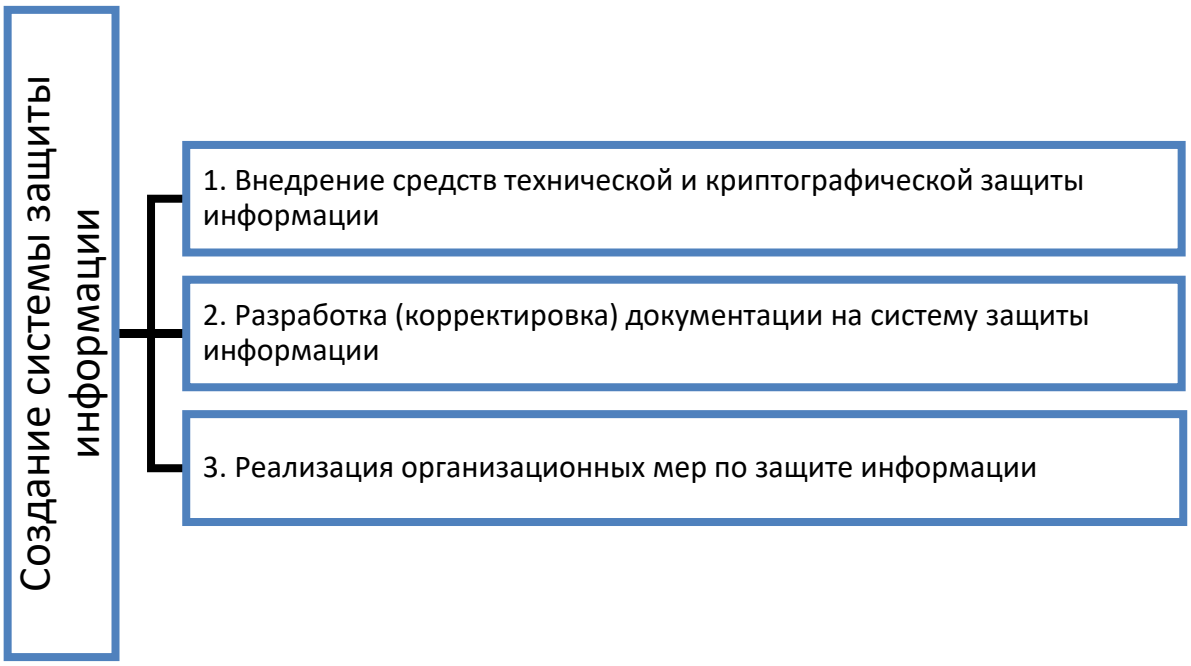


Рисунок 3.2. – Этапы создания системы защиты информации

В ходе внедрения средств технической и криптографической защиты информации осуществляется их монтаж и наладка в соответствии с эксплуатационной документацией, а также смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию, либо блокировка учетных записей, не предусматривающих смену указанных реквизитов.

Этап внедрения завершается проверкой работоспособности средств технической и криптографической информации, а также их совместимости между собой и с другими объектами информационной системы. На данном этапе проверяется корректность выполнения такими средствами требований безопасности в реальных условиях эксплуатации и во взаимодействии с элементами информационной системы [53]. Результаты рекомендуется оформить актом проверки.

2. Разработать документацию на систему защиты информации по перечню, определенному в техническом задании.

В соответствии с Положением о порядке технической и криптографической защиты информации должны быть подготовлены локальные нормативные правовые акты по следующим вопросам [39]:

– о способах разграничения доступа пользователей к объектам информационной системы;

– порядок резервирования и уничтожения информации;

– порядок защиты от вредоносного программного обеспечения;

– порядок использования съемных носителей информации;

– порядок использования электронной почты;

– порядок обновления средств защиты информации;

– порядок осуществления контроля (мониторинга) за функционированием информационной системы и системы защиты информации;

– порядок реагирования на события информационной безопасности и ликвидации их последствий;

– порядок управления криптографическими ключами, в т.ч. требования по их генерации, распределению, хранению, доступу к ним и их уничтожению.

Блок информации **о способах разграничения доступа пользователей** к объектам информационной системы может содержаться как в едином локальном нормативном правом акте, оформленном в виде общих правил, так и быть разделенным на несколько документов, например:

– правила управления физическим доступом на территорию (в помещения) организации;

– положение о видеонаблюдении;

– правила управления доступом пользователей информационной системы (могут быть выделены правила для сотрудников организации и правила для третьих лиц);

– инструкция о порядке обращения с техническими средствами обработки информации;

– правила управления обменом информацией с помощью всех типов средств коммуникации внутри организации;

– правила обмена информацией между организациями;

– правила использования сетей и сетевых услуг;

– инструкция по безопасности оборудования;

– правила использования мобильных средств связи;

– перечень разрешенного программного обеспечения;

– правила дистанционной (удаленной) работы.

Некоторые локальные нормативные правовые акты могут быть изданы в виде приказов (например, приказ об утверждении мест хранения носителей информации, приказ об утверждении перечня документов по защите информации и т.п.).

Возможно, на этой стадии станет очевидной необходимость изменения и дополнения существующих локальных нормативных правовых актов (например, коллективного договора, инструкции по делопроизводству, правил найма сотрудников, инструкции по работе с обращениями граждан

и юридических лиц, графика работ (сменности) и т.п.), а также должностных инструкций сотрудников организации.

Подготовка документов **о порядке реагирования на события информационной безопасности** и ликвидации их последствий предполагает создание четкого алгоритма действий при возникновении угрозы информационной безопасности (в т.ч. в результате чрезвычайных обстоятельств или обстоятельств непреодолимой силы), нарушении или прекращении функционирования информационной системы, нарушении конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Интересно, что по СТБ ISO/IEC 27002-2012 [46] такой порядок действий должен быть организован вплоть до процедур взаимодействия с государственными органами и организациями. В частности, рекомендуется определить, когда и каким образом следует контактировать с правоохранительными и надзорными органами, провайдерами интернет-услуг и операторами телекоммуникаций.

Алгоритм действий должен быть понятен не только должностным лицам, ответственным за обеспечение защиты информации, но и обычным пользователям информационной системы.

При разработке документации по этому вопросу часто прибегают к созданию так называемой **модели угроз безопасности информации** (в белорусском законодательстве термин не используется, однако нередко применяется на практике). Модель угроз является методическим документом, который предназначен для должностных лиц, обеспечивающих безопасность информационной системы. В модели угроз, как правило, описываются основные типы и виды предполагаемых угроз, объекты воздействия, конкретные способы реализации угроз и меры реагирования. Важной частью модели угроз является модель нарушителя, где детально характеризуются основные типы (виды) внешних и внутренних нарушителей и средства, которые могут быть ими использованы (о модели нарушителя см. в разделе 1.1).

В целом при разработке локальных нормативных правовых актов, связанных с системой защиты информации, следует помнить о принципе разумной достаточности и не стремиться создать отдельные детализированные инструкции абсолютно для всех процессов в организации, особенно если речь идет о микроорганизациях[16]. либо о простых информационных системах Иногда достаточно двух базовых документов: развернутой инструкции

[16] Микроорганизации – зарегистрированные в Республике Беларусь коммерческие организации со средней численностью работников за календарный год до 15 человек включительно [59].

пользователя информационной системы, в которой будут прописаны все ключевые правила и алгоритмы деятельности основных сотрудников – от правил обращения с техническими средствами обработки информации и до порядка действий в случаях возникновения угроз безопасности информации; инструкции для сотрудников, ответственных за обеспечение информационной безопасности, где будет приведен порядок выявления угроз и осуществления контроля (мониторинга) за функционированием информационной системы.

В конечном счете стоимость создания системы защиты информации, в т.ч. разработки пакета локальных нормативных правовых актов, не должна превысить стоимость той информации, которая обрабатывается в информационной системе.

4. Реализовать организационные меры по защите информации (см. раздел 2.2).

Реализация организационных мер защиты информации осуществляется в целях выполнения требований, изложенных в локальных нормативных правовых актах, которые должны быть доведены до сведения пользователей информационной системы под роспись. Важным этапом внедрения организационных мер по защите информации является издание руководителем приказов о назначении ответственных лиц по каждому направлению деятельности, о создании комиссий и групп реагирования.

До внесения изменений в действующее законодательство создание системы защиты информации необходимо было завершить проведением опытной эксплуатации системы защиты информации, чтобы проверить ее работоспособность в различных режимах функционирования информационной системы, в т.ч. при необходимости – в условиях нештатной ситуации. Результаты проверки оформлялись протоколами и итоговым актом. С 14 марта 2020 г. опытная эксплуатация созданной системы защиты информации формально проводиться не должна.

3.3.3. Аттестация системы защиты информации

Документальное подтверждение соответствия системы защиты информации требованиям законодательства об информации, информатизации и защите информации производится в результате ее аттестации.

С 14 марта 2020 г. действует новое Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено [56], утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

Изменение законодательства не повлекло тотальной переаттестации эксплуатируемых в Беларуси систем защиты информации, поскольку был создан так называемый «переходный период»: информационные системы, которые были введены в эксплуатацию до 14 марта 2020 г., могут эксплуатироваться в течение срока действия уже выданного аттестата соответствия.

Этапы аттестации защиты информации представлены на рисунке 3.3.

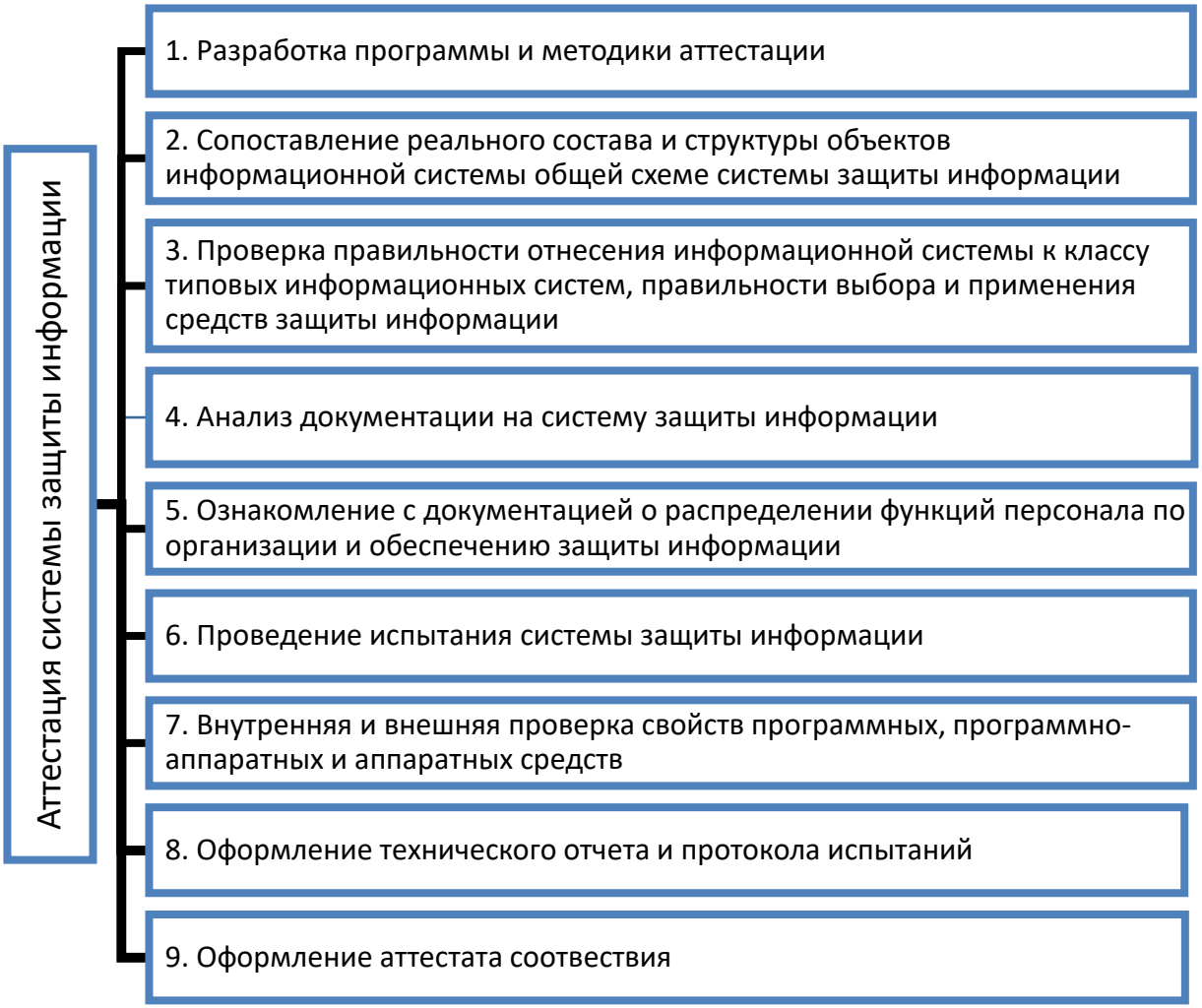


Рисунок 3.3. – Этапы аттестации системы защиты информации

В настоящее время проведение аттестации обязательно в следующих случаях:

– при создании системы защиты информации (до ввода информационной системы в эксплуатацию);

– по истечении срока действия аттестата соответствия (оформляется сроком на пять лет);

– при изменении технологии обработки защищаемой информации;

– при изменении технических мер, реализованных при создании системы защиты информации.

Аттестация может быть проведена специализированной организацией на основании заключенного договора. Специализированная организация должна иметь лицензию с указанием составляющего вида деятельности «аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам» [56].

Специализированная организация проводит аттестацию по заявке владельца (собственника) информационной системы на основании исходных данных о системе защиты информации. Срок такой аттестации не может превышать 180 календарных дней, включая 30 календарных дней для устранения заявителем выявленных недостатков.

Важным нововведением является то, что при проведении аттестации специализированной организацией должны быть привлечены представители собственника (владельца) информационной системы из состава подразделения защиты информации (иного подразделения, должностного лица, ответственного за обеспечение защиты информации).

Для аттестации специализированной организацией заявитель обязан предоставить следующие исходные данные по аттестуемой системе защиты информации:

– политику информационной безопасности организации;

– акт отнесения к классу типовых информационных систем;

– техническое задание на создание информационной системы (если в нем закреплены требования по защите информации) или системы защиты информации;

– общую схему системы защиты информации;

– документацию на систему защиты информации;

– копии сертификатов соответствия либо экспертных заключений на средства защиты информации.

Второй вариант проведения аттестации – самостоятельно собственником (владельцем) информационной системы без получения специального разрешения (лицензии) на соответствующий вид деятельности (стало возможным с 4 сентября 2019 г.). В этом случае в составе организации должно быть создано подразделение (назначено должностное лицо), выполняющее функции по технической и (или) криптографической защите информации. Создание подразделения или возложение функций по защите информации на существу-

ющее подразделение (должностное лицо) следует оформлять приказом руководителя организации[17].

Собственник (владелец) информационной системы должен назначить аттестационную комиссию (оформляется приказом или иным решением) и определить (произвольно) срок проведения аттестации.

При аттестации проводится комплексная оценка системы защиты информации в реальных условиях эксплуатации информационной системы. В ходе аттестации необходимо [56] выполнить следующие мероприятия (допустимо – на выделенном наборе сегментов информационной системы, реализующих полную технологию обработки защищаемой информации):

1. Разработать программу и методику аттестации.

Указанные документы разрабатываются аттестационной комиссией или специализированной организацией (в последнем случае должны быть согласованы с заказчиком аттестации).

Программа и методика аттестации должны содержать следующие сведения:

– перечень выполняемых работ и продолжительность их выполнения;

– перечень методов проверки требований безопасности, реализованных в системе защиты информации;

– перечень используемой контрольной аппаратуры и тестовых средств.

2. Установить соответствие реального состава и структуры объектов информационной системы общей схеме системы защиты информации.

3. Проверить правильность отнесения информационной системы к классу типовых информационных систем, правильность выбора и применения средств защиты информации.

4. Проанализировать разработанную документацию на систему защиты информации на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации.

---

[17] В связи с отменой лицензирования деятельности, связанной с выполнением работ по технической и (или) криптографической защите информации, если эти работы выполняются для собственных нужд обладателем информации, распространение и (или) предоставление которой ограничено, собственником (владельцем) информационных систем и критически важных объектов информатизации, с 04.09.2019 снято требование о наличии в штате организации не менее 3 работников, имеющих высшее образование в области защиты информации либо высшее или профессионально-техническое образование и прошедших переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации. В то же время с 14 марта 2020 г. работы по технической и криптографической защите информации в организации могут проводиться подразделением защиты информации или иным подразделением (должностным лицом), работники которого имеют высшее образование в области защиты информации либо высшее или профессионально-техническое образование и прошли переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации.

5. Ознакомиться с документацией о распределении функций персонала по организации и обеспечению защиты информации.

6. Провести испытание системы защиты информации на предмет выполнения установленных законодательством требований по защите информации.

7. Провести внутреннюю и внешнюю проверку программных, программно-аппаратных и аппаратных средств защиты информации.

Многие средства защиты информации имеют известные свойства (уязвимости), которые могут быть использованы случайно или умышленно для нарушения информационной безопасности системы. Сведения о таких свойствах подтверждаются изготовителями (разработчиками) средства защиты информации.

Таким образом, на этом этапе проверяется наличие у средства защиты известных уязвимостей и возможность их использования нарушителем. Проверка считается успешной, если уязвимостей не обнаружено или они не могут быть использованы (компенсированы) для нарушения информационной безопасности.

При наличии подключения информационной системы к сетям электросвязи общего пользования, в т.ч. Интернет, мероприятия, указанные в пунктах 6 и 7, обязательно должны быть проведены с использованием генератора сетевого трафика и средства контроля эффективности защищенности информации [56].

8. Оформить технический отчет и протоколы испытаний.

Технический отчет должен содержать:

– сроки проведения испытаний;

– вывод о соответствии (несоответствии) реального состава объектов информационной системы общей схеме системы защиты информации;

– вывод о выполнении (невыполнении) установленных законодательством требований по защите информации;

– отчет о проведенной внутренней и внешней проверках.

9. Оформить аттестат соответствия.

Итоговый аттестат соответствия имеет утвержденную форму [56] и должен быть подписан руководителем собственника (владельца) информационной системы (при проведении аттестации самостоятельно) или руководителем специализированной организации.

Копии аттестата соответствия, технического отчета и протоколов испытаний по итогам аттестации не позднее 10 календарных дней со дня оформления (получения) аттестата предоставляются в ОАЦ вместе со сведениями об информационной системе по утвержденной форме [57].

3.4. Порядок эксплуатации информационной системы с применением аттестованной системы защиты информации

Важно понимать, что после создания системы технической защиты информации необходимо постоянно поддерживать ее в действующем состоянии в процессе эксплуатации, а также позаботиться о защите информации в том случае, если эксплуатация информационной системы будет прекращена.

В процессе эксплуатации информационной системы с применением аттестованной системы защиты информации осуществляются [39]:

– контроль за соблюдением требований, установленных в нормативных правовых актах, в т.ч. в технических, документации на систему защиты информации собственника (владельца) информационной системы;

– контроль за порядком использования объектов информационной системы;

– мониторинг функционирования системы защиты информации.

В случае выявления нарушений требований по защите информации их необходимо зафиксировать (например, в специальном журнале) и принять меры к своевременному устранению.

О событиях информационной безопасности, в т.ч. фактах нарушения функционирования информационной системы, конфиденциальности, целостности, подлинности, доступности либо сохранности информации, необходимо уведомить ОАЦ в течение суток с момента выявления этих событий [57].

Если в течение пяти рабочих дней устранить нарушения не удалось, необходимо действовать по следующему алгоритму:

(1) прекратить обработку информации, распространение и (или) предоставление которой ограничено;

(2) письменно информировать ОАЦ о нарушениях;

(3) осуществить доработку системы защиты информации и провести оценку на предмет необходимости ее повторной аттестации;

– выявление угроз, которые могут привести к сбоям, нарушению функционирования информационной системы;

– резервное копирование информации, содержащейся в информационной системе;

– обучение (повышение квалификации) пользователей информационной системы;

– уничтожение (удаление) данных и криптографических ключей с машинных носителей информации, равно как и уничтожение самих носителей информации в случае, если эксплуатация информационной системы будет прекращена (например, при ликвидации организации).

О прекращении функционирования информационной системы необходимо в произвольной форме уведомить ОАЦ в течение суток [57].

3.5. Требования по защите информации в соответствии с Общим регламентом защиты персональных данных Европейского союза

Белорусские организации попадают в сферу действия Общего регламента защиты персональных данных Европейского союза (EU General Data Protection Regulation, Регламент GDPR), вступившего в силу 25 мая 2018 г.[18], во всех случаях, когда ими обрабатываются персональные данные (см. раздел 1.2.1) лиц из Европейского союза (принципиально здесь не гражданство, а фактическое местонахождение хотя бы в одной из стран ЕС):

– если запрашивается контактная информация (например, при бронировании гостиниц, пассажирских перевозках, продажах через интернет-магазин, если соответствующий сайт использует язык или валюту стран ЕС);

– если анализируется пользовательское поведение (в социальных сетях, маркетплейсах и т.п.);

– если разрабатывается программное обеспечение (мобильные приложения, облачные решения, онлайн-игры и т.п.), которое работает с персональными данными.

Соблюдение требований Регламента GDPR крайне важно, поскольку, если в результате нарушения установленных правил обработки персональных данных лицу будет причинен ущерб, может быть предъявлен иск о его возмещении к компании, допустившей нарушение. Кроме того, Регламент GDPR предусматривает огромные штрафы за нарушение его требований: до 20 млн евро или до 4% годового мирового оборота компании (в зависимости от того, какая сумма окажется больше).

Например, штраф в размере 50 000 000 евро был применен за нарушение требований Регламента GDPR к разработчику известного интернет-

[18] Полный официальный текст Общего регламента защиты персональных данных Европейского союза: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. Неофициальный перевод на русский язык: https://internetinstitute.ru/wp-content/uploads/2017/10/GDPR.pdf.

поисковика – компании Google LLC. Соответствующее решение было принято Национальной комиссией по информатизации и свободе Франции (далее – CNIL) в январе 2019 г.

По данным CNIL, компания Google LLC не смогла надлежащим образом проинформировать пользователей о том, как их персональные данные собираются и используются для показа рекламных и маркетинговых сообщений. Также Google LLC не удалось должным образом получить согласие пользователей в целях использования их данных для показа им персонализированной рекламы – отсутствовало так называемое прямо выраженное согласие, которое реализуется, например, посредством клика (щелчка) по соответствующей галочке договора в электронной форме. Кроме того, CNIL обнаружила, что согласие пользователей Google LLC на использование их персональных данных недействительно, т.к. информация о сборе и использовании данных неоднозначна и неконкретна (разбита по нескольким документам, затрудняет четкое представление пользователя о том, какие именно персональные данные собираются и как они используются компанией), а также не указан срок хранения таких данных [60].

Для того чтобы снизить риск ответственности за нарушение требований Регламента GDPR, специалисты рекомендуют внедрять [60–62] следующие правила сбора и обработки персональных данных:

1. Максимально просто излагать цели, методы и объемы обработки персональных данных в политиках (соглашениях) конфиденциальности, предлагаемых пользователям, а сами политики (соглашения) размещать в легко доступном для ознакомления месте.

2. Получать осведомленное согласие пользователя на сбор и обработку персональных данных. Молчание или бездействие не означает согласия – оно должно быть выражено утверждением или четкими активными действиями (например, «галочки» о согласии не могут быть заранее проставлены на сайте). Согласие будет недействительным, если у пользователя не было выбора или не было возможности отозвать свое согласие.

Согласие не требуется только в том случае, если запрашиваются данные, которые объективно необходимы для исполнения договора. Например, для продажи товара через интернет-магазин объективно необходимо получить банковские реквизиты для дистанционной оплаты, а также почтовый адрес и имя покупателя для доставки товара. Тем не менее, даже полученные таким образом данные нельзя использовать в иных целях без дополнительного согласия.

В случае, если персональные данные получены от третьих лиц, а не от самого пользователя напрямую, Регламент GDPR требует представить

субъекту персональных данных развернутое уведомление об обработке персональных данных (так называемое «право быть информированным»).

Например, в отношении шведской компании Bisnode Органом по надзору за соблюдением законодательства о защите персональных данных Республики Польша на основании Регламента GDPR был применен штраф в размере 200 000 евро за несоблюдение компанией указанного обязательства.

Компания Bisnode получила персональные данные из публичных реестров деловой активности и использовала такую информацию в коммерческих целях (для маркетинга). По словам представителя Bisnode, компания информировала отдельных лиц об обработке их персональных данных только в том случае, если у нее были адреса их электронной почты. В остальных случаях такого информирования не происходило. Компания заявила, что не выполняла свое обязательство по информированию субъектов персональных данных из-за высоких затрат, которые для этого потребуются. Вместо этого она опубликовала обобщенное уведомление об обработке персональных данных на своем веб-сайте. В результате помимо штрафа на компанию Bisnode обязана в течение трех месяцев связаться с 6 млн лиц, чтобы выполнить требования Регламента GDPR, что по расчетам компании будет дополнительно стоить около 8–9 млн евро [60].

3. Собирать и использовать персональные данные исключительно в тех целях, которые заявлены компанией (онлайн-сервисом). При этом количество собираемых персональных данных должно быть минимально необходимым, пользователь должен понимать, с какой целью они будут использоваться, а компания должна быть готова подтвердить, что такая цель обоснована и необходима.

Для соблюдения требования Регламента GDPR в существующую систему защиты информации необходимо «встроить» следующие элементы:

1. Подготовить пакет документов о выполнении Регламента GDPR, поскольку только фактического соблюдения всех требований недостаточно.

Необходимо подготовить как минимум следующие документы [61; 62]:

– политику обработки персональных данных (в более привычном наименовании – политику конфиденциальности);

– внутренние правила и процедуры работы с персональными данными;

– реестр персональных данных и реестр процессов обработки персональных данных;

– учетные записи обработки персональных данных.

Реестр персональных данных – это инструмент учета персональных данных с указанием их местоположения, ответственного владельца файла или процесса, чувствительности информации, уровня доступа к ней, периода хранения, рисков и значимости, доступности данных. Приказом руководителя следует назначить лицо, ответственное за ведение реестра и подготовить соответствующую инструкцию [61].

Реестр процессов обработки персональных данных – это инструмент учета процессов обработки персональных данных, где помимо характеристик процесса должны отражаться виды обработки данных (сбор, хранение, изменение, передача, удаление и т.д.), контакты инспектора (инженера) по защите информации, основание для обработки данных (согласие, законный интерес и т.д.), местоположение сервера и его оператора, юридическое основание для размещения данных на сервере, данные процессора (обработчика) персональных данных, а также сведения о том, производилась ли оценка воздействия защиты данных [61].

Полный комплект документации может включать в себя несколько десятков политик и реестров.

2. Внедрять настройки приватности в программное обеспечение еще на этапе обработки (принцип privacy by design) и изначально (по умолчанию) предлагать пользователю максимальные настройки приватности (принцип privacy by default).

3. Использовать псевдонимизацию (обезличивание), что предполагает отдельное хранение информации, позволяющей установить личность человека, и дополнительных сведений, которые к нему относятся (например, имя пользователя хранится отдельно от истории его действий в аккаунте) [61; 62].

4. Обеспечить пользователю «право быть забытым» (возможность по требованию пользователя полностью удалить персональную информацию отовсюду, включая резервные копии) и «право на портативность» (возможность передать пользователю весь массив собранных провайдером персональных данных для передачи иному провайдеру, т.е. произвести экспорт данных) [61].

Назначить инспектора по защите персональных данных (Data protection officer, DPO) [62], если деятельность организации связана:

– с обработкой персональных данных, которая требует регулярного и систематического мониторинга физических лиц в больших масштабах (например, крупные социальные сети, компании, работающие с Big Data, крупные маркетплейсы);

– с масштабной обработкой чувствительных персональных данных (см. раздел 1.2.1).

Проводить специальную оценку влияния мер для защиты персональных данных (Data Protection Impact Assessments, DPIA) во всех случаях, когда:

– проводится автоматизированная обработка персональных данных или осуществляется профайлинг;

– обрабатываются чувствительные персональные данные или же персональные данные, принадлежащие лицам, на которых контроллер имеет влияние (например, это может касаться студентов, пациентов, работников компании);

– обрабатываются персональные данные в больших масштабах, или они собраны в местах, к которым имеет доступ широкая общественность; например, это открытые площадки (камеры видеонаблюдения в публичных местах являются лишь наиболее известным примером) [62].

6. При обработке персональных данных обеспечить надлежащую их защиту от несанкционированной или незаконной обработки, уничтожения и повреждения.

Например, на текущий момент самый большой штраф по Регламенту GDPR применен именно в связи с ненадлежащим осуществлением технических и организационных мер для обеспечения необходимого уровня безопасности. В июле 2019 г. Управление комиссара по информации (ICO) Великобритании сообщило о наложении штрафа в размере около 230 млн долл. на авиакомпанию British Airways за крупную утечку данных, когда злоумышленники путем перенаправления посетителей интернет-страницы авиакомпании с официального сайта на «зеркало» сумели украсть персональные данные порядка 380 000 клиентов авиакомпании (имена, номера банковских карт и их CVV-коды, адреса электронной почты) [63].

7. Обеспечить соблюдение требований Регламента GDPR контрагентами (например, организациями-подрядчиками, которые либо разработали информационную систему, либо обслуживают информационную систему).

8. Обучать работников базовым правилам работы с персональными данными, лимитировать доступ к персональным данным для разных категорий работников, подписывать соответствующие обязательства о неразглашении [60].

Назначить представителя компании в ЕС.

9. Исключение – для компаний, которые:

– обрабатывают персональные данные нерегулярно;

– не имеют дела с чувствительными персональными данными;

– едва ли представляют риск для прав физических лиц в связи с использованием их персональных данных [62].

Вопросы для самопроверки

1. Перечислите основные принципы создания системы защиты информации.

2. Каковы основные этапы организации системы технической защиты информации?

3. Какие основные действия необходимо совершить на этапе проектирования системы защиты информации?

4. Для чего разрабатывается политика информационной безопасности организации? Какие сведения включаются в политику информационной безопасности?

5. Какие сведения должны быть обязательно отражены в локальных нормативных правовых актах, направленных на реализацию политики информационной безопасности организации?

6. Опишите процедуру аттестации системы защиты информации в соответствии с требованиями ОАЦ.

7. Чем процедура аттестации системы защиты информации отличается от сертификации системы защиты информации в рамках Национальной системы подтверждения соответствия Республики Беларусь?

8. Какие обязательные процедуры необходимо выполнять в процессе эксплуатации информационной системы с применением аттестованной системы защиты информации?

9. В каких случаях белорусские организации обязаны соблюдать требования Общего регламента защиты персональных данных Европейского союза?

10. Какие элементы следует «встроить» в систему защиты информации для соблюдения требований Общего регламента защиты персональных данных Европейского союза?

4. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

4.1. Вредоносные программы

Вредоносное программное обеспечение является инструментом большинства нарушений информационной безопасности. Вредоносной программой считается любая специальная программа, которая приносит вред пользователю, компьютеру или сети [64, с. 20].

Вредоносное программное обеспечение предоставляет возможность совершать следующие действия на устройствах:

– перехват конфиденциальных данных пользователей;

– шифрование или уничтожение данных;

– блокирование доступа пользователя к компьютеру для вымогательства;

– выполнение распределенных вычислений, например, для выработки криптовалют;

– нарушение работы программ и операционной системы;

– уничтожение данных BIOS и др.

Не всякие вредоносные программы одинаково опасны. На противоположных точках находятся безвредные, которые не способны повлиять на производительность и функционирование операционной системы и лишь уменьшают дисковое пространство, и очень опасные, которые могут передавать конфиденциальную информацию, уничтожать или изменять данные. На шкале между ними могут быть помещены неопасные, которые уменьшают свободную оперативную память, дисковое пространство и в дополнение к этому воспроизводят графические или звуковые эффекты, а также опасные, которые способны привести к сбоям и ошибкам в работе компьютера [47, с. 31].

Ниже представлены классификации, позволяющие понять основное назначение и суть вредоносного программного обеспечения.

4.1.1. Классификация вредоносных программ по типу операционной системы

По типу операционных систем выделяют пять семейств системных платформ: Microsoft Windows, Google Android, Apple macOS, Linux и другие системные платформы [65, с. 26].

Классификация вредоносных программ по типу операционной системы наиболее очевидна и имеет значение для эффективного противодействия:

каждому семейству системных платформ соответствует своя программа антивирусной защиты.

Наибольшее число вредоносных программы создается для операционных систем семейства Microsoft Windows (около 95% всех существующих в мире вредоносных программ [65, с. 26]).

Далее следует мобильная платформа Google Android, которая является самой популярной операционной системой для мобильных устройств (смартфонов, планшетов), рассчитана на среднестатистического пользователя и потому достаточно интуитивна. Используя эту платформу, злоумышленники могут рассылать платные SMS-сообщения и совершать втайне от пользователя телефонные звонки на различные коммерческие номера; подписывать жертву на те или иные виртуальные услуги и списывать денежные средства за их использование; показывать на телефоне рекламу и даже похищать деньги с карт-счета, перехватывая входящие SMS с одноразовыми паролями и кодами авторизации из мобильного банкинга. Существуют даже блокировщики и троянцы-шифровальщики для Android, которые могут встречаться и в официальном каталоге Google Play, несмотря на все принимаемые корпорацией Google меры [65, с. 27].

Уверенное третье место по количеству известных угроз занимает операционная система Apple macOS, которая с точки зрения архитектуры и разграничения прав доступа существенно безопаснее Windows, но в Apple macOS подавляющее большинство вредоносных программ составляют так называемые рекламные троянцы (как правило, реализованы в виде надстроек (плагинов) для наиболее популярных браузеров: Safari, Chrome, Firefox). Именно они демонстрируют жертве назойливую рекламу при открытии им в окне браузера различных веб-страниц. Существуют также троянцы-майнеры, использующие вычислительные мощности компьютеров Apple для выработки электронных криптовалют путем сложных математических вычислений [65, с. 27].

Четвертое место – у вредоносных программ для операционных систем семейства Linux, которые активно используются на различных «умных» устройствах (например, бытовые и промышленные wi-fi роутеры, точки доступа, сетевые хранилища, кабельные модемы, телевизионные приставки, камеры с веб-интерфейсом управления, и т.д.). Для операционных систем Linux существуют и троянцы для заражения веб-серверов, FTP- и почтовых серверов в Интернете (заражение хоста открывает злоумышленникам, например, доступ к SMTP-серверу для организации массовых рекламных рассылок, к веб-серверу – для реализации автоматических перенаправлений

посетителей сайта на интернет-ресурсы, распространяющие другое вредоносное программное обеспечение для организации DDoS-атак или хищения пользовательских данных) [65, с. 30].

Учитывая малую распространенность других системных платформ количество вредоносных программ для них в общей массе не слишком значительно. Например, по данным ESET на 2019 г., число вредоносных программ мобильной платформы Apple iOS составляет менее 1% от количества вредоносных программ для мобильной платформы Google Android [66].

4.1.2. Классификация вредоносных программ по вредоносным признакам

Классификация по вредоносным признакам на типы и подклассы осуществляется в соответствии с формальными признаками, определяющими их функционирование.

Компьютерные вирусы. К компьютерным (файловым) вирусам относят вредоносные программы, которые обладают возможностью саморепликации (автоматического распространения) и способностью заражения файловых объектов. Под заражением понимается технология, с использованием которой вирус внедряется непосредственно в файл исполняемого приложения (программы). При запуске зараженной программы на исполнение пользователь одновременно запускает и встроенный в нее вирус, который загрузившись в память компьютера, выполняет заложенные в него деструктивные функции [65, с. 32].

Компьютерные вирусы делятся на следующие подклассы.

Стелс-вирусы (вирусы-невидимки) – вирусы, полностью или частично скрывающие свое присутствие в памяти компьютера, для чего выполняют перехват обращений антивирусных программ к пораженным объектам (загрузочным секторам, элементам файловой системы, памяти и т.д.) и подставляют вместо себя незараженные участки информации;

Полиморфные вирусы, **полиморфик-вирусы** (вирусы-призраки) – вирусы, которые скрывают свое присутствие на компьютере путем шифрования тела вируса. Для шифрования тела вирус использует случайные ключи и алгоритмы шифрования, из-за чего тело вируса не содержат ни одного постоянного участка кода, что исключает возможность опознания вируса по сигнатурам.

Макровирусы – вирусы, разработанные на макроязыках, которые встроены в прикладные пакеты (текстовые и графические редакторы, электронные таблицы и т.д.). Заражение от одного файла к другому происходит

при открытии документа с включенной опции, разрешающей исполнение макрокоманд.

Скрипт-вирусы – вирусы, которые написаны на различных скриптовых языках (VBS, JavaScript, BAT, PHP и т.д.). Скрипт-вирусы либо заражают другие скрипт-программы, либо являются частями многокомпонентных вирусов.

Вирусы-ссылки (link-вирусы) – вирусы, которые при запуске зараженного файла «заставляют» операционную систему выполнить свой код (перейти по ссылке). Переход по ссылке выполняется без изменения физического содержимого файлов, а путем модификации необходимых полей файловой системы, например, записывают свое тело в последний кластер логического диска.

Перезаписывающие вирусы используют наиболее простой способ заражения: полностью заменяют код заражаемого файла своим кодом, не изменяя названия исполняемого файла. Такие вирусы еще и просто обнаруживаются, поскольку исходная программа перестает функционировать и не может быть восстановлена.

Компаньон-вирусы не изменяют заражаемые файлы, а создают файл-двойник, который получает управление при запуске заражаемого файла. Компаньон-вирусы при заражении могут переименовывать файл, запоминать новое имя файла для последующего запуска, а вместо переименованного файла записывают свой код.

Паразитические вирусы изменяют содержимое дисковых секторов или файлов при распространении своих копий (необязательно совпадающих с оригиналом). Сами зараженные файлы полностью или частично остаются работоспособными.

OBJ-, **LIB-вирусы, вирусы в исходных кодах** – вирусы, заражающие библиотеки компиляторов, объектные модули и исходные коды программ, достаточно экзотичны и практически не распространены. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, следовательно, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же «живого» вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ/LIB-файлы, на втором (линковка) получается работоспособный вирус.

Компьютерные черви. Компьютерные черви – разновидность вредоносных компьютерных программ, обладающих способностью к саморепликации по локальной сети, каналам электронной почты, с использованием сменных носителей информации или иными методами [65, с. 34].

Компьютерные черви делятся на следующие подклассы.

Сетевые черви используют для распространения сетевые протоколы и уязвимости в сетевом программном обеспечении.

Файловые черви копируют свой код в системные каталоги с присвоением распространенных названий файлов (например, install.exe или game.exe), которые привлекают пользователя к их запуску. Файловые черви можно встретить также в корневой папке съемного накопителя (флэш-карты или карты памяти) в формате autorun.inf (в устаревших версиях операционных систем такой файл автоматически запускает червя при каждом обращении к накопителю).

Почтовые черви – вредоносные программы, которые после запуска отыскивают все хранящиеся на компьютере адреса электронной почты и рассылают свою копию по этим адресам в виде вложения в электронное письмо [65, с. 34]. Почтовый червь способен извлекать адреса электронной почты из любых файлов, включая текстовые документы, а адрес отправителя могут копировать из списка контактов на зараженном компьютере, обеспечивая «узнаваемость» письма потенциальным получателем. Таким образом, получатель, открывая вложение, становится очередным звеном массовой рассылки.

Троянские программы (троянские кони, троянцы, трояны) – вредоносные программы, которые проникают на компьютер под видом легитимных программ. Состоят из двух частей: серверной, которая запускает программного агента на зараженном компьютере, и клиентской, которая устанавливается на компьютере злоумышленника, подключается к серверной части и передает ей команды для исполнения на компьютере жертвы. Соединение обычно устанавливаются по протоколам TCP и UDP. IP-адрес и порт для подключения к зараженному хосту сервер троянской программы передает через встроенные средства оповещения, например, отсылкой на электронный адрес, в мессенджер, веб-запросом, сетевым запросом.

Серверная часть троянской программы способна блокировать антивирусные программы и межсетевые экраны и обеспечить последующий автоматический запуск при загрузке операционной системы. С внедрением межсетевого экранирования и NAT-технологий подключение клиента троянской программы к зараженному хосту менее вероятно, однако для их

преодоления может использоваться технология реверсного сервера (backconnect-сервера), который на зараженном компьютере сам выполняет подключение к серверу злоумышленника [67].

Троянцев принято делить на следующие подклассы [65, с. 47–70]:

- троянцы-блокировщики (винлокеры);
- троянцы-шифровальщики (энкодеры);
- банковские троянцы;
- веб-инжекты;
- троянцы-загрузчики;
- майнеры;
- рекламные троянцы;
- узкоспециализированные троянцы.

Основная опасность троянских программ состоит в том, что злоумышленник может получить практически неограниченный доступ к зараженному компьютеру, однако в отличие от компьютерных вирусов и сетевых червей троянцы не способы к самовоспроизведению.

Бэкдоры – дефекты алгоритма (программы), намеренно встроенные разработчиком для получения несанкционированного доступа к данным или удалённому управлению компьютером.

Буткиты – загрузочные вирусы или троянцы, которые в отличие от программных поражают определенные системные области носителей данных (дисков, устройств) и запускаются либо раньше операционной системы, либо одновременно с ней, но в любом случае перед загрузкой основных средств антивирусной защиты. Это позволяет им перехватывать некоторые функции управления операционной системой и, как следствие, парализовать запуск и нормальную работу антивирусных программ, а также блокировать попытки «вылечить» инфицированное устройство. Неудачное удаление буткита может привести к повреждению логической структуры диска, вследствие чего система перестанет загружаться [65, с. 38].

Руткиты способны скрывать различные объекты в операционной системе (файлы, папки, запущенные приложения и/или загруженные драйвера), а также происходящие в системе процессы (запуск и выгрузку приложений, загрузку динамических библиотек, встраивание в запущенные процессы, заражение файловых объектов и т.п.). Кроме того, такие вредоносные программы могут осуществлять перехват системных функций, модифицировать системные объекты и объекты ядра операционной системы [65, с. 39].

Биоскиты – вредоносные программы, способные модифицировать содержимое микросхем BIOS инфицированного компьютера. На практике встречаются крайне редко (последняя такая программа – Trojan.Bioskit.l –

была обнаружена специалистами «Доктор Веб» в сентябре 2011 г., и по всем признакам она походила скорее на экспериментальную и незавершенную разработку академического характера, чем на реальную угрозу [65, с. 40]).

Ботнет (бот-сеть) – сеть зараженных устройств, которые способны обмениваться информацией и позволяют управлять ими дистанционно при помощи одного или нескольких командных серверов [65, с. 40]. Ботнеты могут создаваться для централизованной DDoS атаки на различные серверы Интернета или выполнения массовых рассылок.

Шпионы предназначены для слежения за пользователем и передачи информации с его устройств злоумышленникам (чаще всего реализуются в виде классических троянцев). Наиболее популярные среди них – кейлоггеры, которые считывают, сохраняют в специальный журнал и передают злоумышленникам коды нажимаемых пользователем клавиш. Существуют также троянцы-шпионы, способные создавать и отправлять киберпреступникам снимки содержимого экрана, GPS-координаты положения зараженного устройства, журнал звонков, изображения; выполнять несанкционированную фото- и видеосъемку, записывать телефонные разговоры и даже использовать встроенный микрофон мобильного устройства для скрытой диктофонной записи [65, с. 42].

Нежелательный и нерекомендуемые приложения. Помимо вредоносных программ существует широкий ассортимент потенциально опасных и нежелательных приложений, которые сами по себе вредоносного потенциала не несут, но способны доставить пользователю сложности. Например, приложения класса Adware – утилиты, которые, возможно, и имеют какую-то полезную функциональность, но при этом помещают во все просматриваемые пользователем веб-страницы назойливую рекламу. Другой пример – приложения семейства Fakealert, к которым относятся всевозможные поддельные антивирусы, утилиты для оптимизации системного реестра, «ускорения» Интернета и «лечения» компьютера от несуществующих неисправностей [65, с. 43].

4.1.3. Классификация вредоносных программ по способу загрузки в операционной системе

В зависимости от способа загрузки в операционную систему вредоносные программы делят на резидентные, полурезидентные, нерезидентные (транзитные).

Резидентные вредоносные программы при запуске операционной системы загружают в оперативную память свою скрытую часть, позволяющую отслеживать и перехватывать обращение операционной системы

к объектам для заражения. Такие программы остаются активными до выключения компьютера [47].

Полурезидентные вредоносные программы запускают отдельный поток в зараженной программе, в котором отслеживаются и перехватываются обращения операционной системы к объектам для заражения. Работает зловредный поток столько, сколько работает зараженная программа.

Нерезидентные (транзитные) вредоносные программы активны только во время передачи управления зараженной (вредоносной) программе.

4.2. Способы проникновения вредоносного программного обеспечения на устройства пользователей

Вредоносное программное обеспечение может проникать на устройства пользователей следующими способами.

1. **Через съемные накопители информации** (карты памяти, мобильные телефоны и планшеты, подключаемые к компьютеру). Выбор устройства для заражения вредоносная программа обычно осуществляет путем перечисления имен дисков, содержащих значение «USB», а также смонтированных в системе разделов и логических дисков в поисках съемных накопителей [65, с. 92].

2. **Посредством вредоносных рассылок**: по электронной почте, в социальных сетях, в мессенджерах, реже – через короткие сообщения (SMS) на номер мобильного телефона. Считается самым распространенным способом заражения [65, с. 93]. Злоумышленники маскируют вложенные вредоносные программы привлекательными наименованиями, сопровождают мотивирующими к просмотру сообщениями, используют сервисы сокращения ссылок, подмену номеров телефонов.

3. **Через уязвимости (скрытые ошибки в коде приложений или операционной системы)**. Уязвимости могут быть связаны с недостатками архитектуры операционной системы или приложения либо являться следствием ошибок разработчиков программного обеспечения. При этом особо выделяются критические уязвимости, позволяющие полностью нарушить работоспособность операционной системы или приложения, и уязвимости нулевого дня, которые уже известны злоумышленникам и для которых еще не выпущено обновление («заплатка», «патч») [65, с. 95]. Особенность проникновения через уязвимости состоит в том, что оно может происходить без всякого участия пользователя, автоматически.

4. **Посредством загрузчиков**, самостоятельно скачивающих из сети Интернет и запускающих на устройстве новые вредоносные программы. Изначальное заражение устройство может происходить иным способом, а затем происходит дальнейшее массовое распространение вредоносных программ. Загрузчики могут быть объединены в ботнеты (см. раздел 4.1.2), которые покупают создатели вредоносного программного обеспечения, оплачивая успешные загрузки на устройства пользователей [65, с. 99].

5. **Через поддельные и взломанные сайты.**

Подделываются чаще всего сайты файлового обмена (торренты, библиотеки и т.п.) и сайты с вопросами (например, форумы), поскольку они изначально предназначены для скачивания различных файлов и вредоносный файл проще замаскировать.

Взламываются сайты, которые используют популярные системы управления контентом с открытым исходным кодом (например, Wordpress или Joomla), поскольку в них проще отыскать уязвимости. Взломав сайт, киберпреступники обычно загружают на него шелл-скрипт, который открывает доступ к файловой системе атакованного интернет-ресурса. Второй вариант – размещение в различных файлах, являющихся компонентами CMS, сценариев для перенаправления посетителей сайта на вредоносные ресурсы (элементы TDS) или для непосредственной загрузки вредоносных программ [65, с. 109].

6. **Посредством бесплатных и взломанных приложений.**

Вредоносное программное обеспечение может быть «встроено» во взломанные версии платных коммерческих приложений, а также замаскировано под «пиратские» копии музыкальных произведений и книг. Бесплатные приложения могут дополняться нежелательными утилитами или рекламными троянцами.

В целом необходимо понимать, что любой из перечисленных способов так или иначе использует информационную неграмотность пользователя.

4.3. Признаки заражения устройства

О заражении компьютерным вирусом могут свидетельствовать следующие признаки [64]:

– программы выполняются медленнее, чем обычно;

– компьютер перестает реагировать на клавиатуру или периодически блокирует ее работу;

– компьютер самопроизвольно периодически перезагружается;

– появляются необычные сообщения об ошибках;

– меню и диалоговые окна отображаются в искаженном виде;

– антивирусную программу невозможно запустить или невозможно получить обновление для нее;

– на рабочем столе появились новые ярлыки;

– некоторые приложения исчезли;

– самопроизвольно открываются программы или показывается реклама;

– изменился размер файлов;

– уменьшился объем доступной оперативной памяти или процессора.

Такие признаки при правильно функционирующем антивирусном программном обеспечении свидетельствуют о том, что компьютер инфицирован еще неизвестным вирусом. Интервал заражения компьютера новым видом вредоносной программы может составлять до нескольких дней и даже недель.

4.4. Средства антивирусной защиты

Средства антивирусной защиты могут быть программными, программно-аппаратными либо иметь организационный характер.

Программные средства могут работать, используя следующие методы защиты:

– регулярное сканирование;

– обнаружение изменений файлов;

– эвристический анализ;

– резидентную защиту операционной системы;

– «вакцинирование» программ.

Антивирусные программы-сканеры, осуществляя регулярное сканирование (сигнатурный анализ), последовательно просматривают проверяемые файлы в поиске сигнатур[19] известных вредоносных программ. Антивирусные программы-сканеры способны найти только уже известные вирусы, для которых была определена сигнатура, поэтому их наибольшая эффективность достигается постоянным обновлением баз данных сигнатур. Сканеры-полифаги способны сразу удалять обнаруженные вредоносные программы. Самые известные среди них – Panda, Dr. Web, Kaspersky, Avast.

[19] **Сигнатура** – уникальная последовательность байтов, принадлежащих конкретно известному вирусу и не встречающаяся в других программах.

Антивирусные программы-ревизоры направлены на обнаружение изменений файлов (метод контроля целостности): они сохраняют исходное состояние главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов, информацию о структуре каталогов и номера плохих кластеров дисков, а иногда и дополнительные параметры – объем оперативной памяти, количество подключенных дисков и т.п. При обнаружении подозрительных изменений ревизор сообщает об угрозе пользователю. Основное преимущество ревизоров в том, что они способны обнаруживать любые компьютерные вирусы, в т.ч. неизвестные ранее, а также могут восстанавливать инфицированные файлы и загрузочные секторы, используя сохраненную ранее информацию. Ревизоры наиболее эффективны в комплексе со сканерами. В русскоязычной среде наиболее известны ADinf и ревизор, встроенный в антивирус Kaspersky.

Метод эвристического анализа предполагает проверку программ операционной системы, прикладных программ и загрузочных секторов дисков с целью найти в них код, характерный для компьютерного вируса, что позволяет обнаруживать ранее не изученные вирусы. Все современные антивирусные программы реализуют собственные методы эвристического анализа. Учитывая, что эвристики действуют на основании предположений, они могут как пропускать неизвестные угрозы, так и признавать безопасные программы вредоносными.

Резидентная защита («невидимый сторож») – антивирусная программа, которая загружается в оперативную память компьютера раньше других программ. После загрузки операционной системы антивирусная программа отслеживает и перехватывает действия, выполняемые другими программами, которые считаются подозрительными и свидетельствуют о наличии компьютерного вируса. При обнаружении таких действий резидентный сторож, как правило, сообщает пользователю о наличии подозрительных действий, ожидая его ответа (разрешение или запрещение данных действий). Обычно резидентные сторожа автоматически проверяют все запускаемые программы на наличие сигнатур известных вирусов. Выгружается из оперативной памяти резидентный сторож только при выключении компьютера после остальных программ.

Вакцинирование устанавливает способ защиты конкретной программы от вируса, при котором к этой программе присоединяется специальный модуль контроля, следящий за ее целостностью. При этом проверяются контрольная сумма программы или какие-либо другие ее характеристики. Если вирус заражает вакцинированный файл, то модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

Аппаратно-программные средства основаны на применении любого программного метода с помощью специальных технических устройств. Как правило, они реализуются с помощью специализированного устройства (контроллера), которое вставляется в компьютер в виде расширения, и специального программного обеспечения, управляющего работой этого устройства и приводящего в исполнение один или несколько программных методов. Наличие такого устройства дает возможность защитить главную загрузочную запись, загрузочные секторы, выполняемые файлы, файлы конфигурации и т.п. Аппаратно-программные средства также позволяют защитить компьютер от неквалифицированного пользователя, не давая ему удалить важную информацию, переформатировать диск, изменить файлы конфигурации.

Организационные средства защиты от вредоносных программ обеспечивают выработку и соблюдение пользователями определенных политик (правил) работы с информацией. Выделяют две категории правил обработки информации: правила использования программ и правила обработки информации.

В правила обработки информации включают следующие пункты:

– запрещается открывать вложения в почтовых сообщениях от незнакомых отправителей;

– после подключения сменного накопителя (дискет, компакт-дисков, flash-накопителей) выполняется сканирование накопителя антивирусом на наличие вредоносных программ;

– все загружаемые файлы из сети Интернет требуют тщательной проверки на наличие вредоносных программ;

– не допускается загружать неожидаемые файлы или установщики программ из сети Интернет;

– разрешается использовать только те программы (файлы), происхождение которых известно.

В правила использования программ включают следующие пункты:

– допускается использование только лицензионных программ, полученных из надежных источников;

– регулярно устанавливать обновления безопасности операционной системы и используемых программ;

– использовать наиболее актуальные (совершенные) версии защитных программ;

– следить, чтобы программы, обеспечивающие защиту компьютера, были запущены, а функции защиты активированы;

– не приостанавливать работу защитных программ для увеличения производительности или снятия ограничений при работе с компьютером;

– следить, чтобы антивирусные базы регулярно обновлялись;

– без необходимости и полного понимания сути изменений не изменять настройки программ, обеспечивающих защиту.

Все средства защиты от компьютерных вирусов можно сгруппировать по времени их использования:

– до обнаружения зловредного программного обеспечения: усиление системы – установка всех последних патчей и изменений, удаление ненужных или неиспользуемых модулей, отслеживание появления новых угроз на основных сайтах по безопасности, периодическое резервное копирование основных программ и данных;

– при обнаружении: использование антивирусных средств для контроля всей входящей информации, применение специальных средств обнаружения, сканирование компьютера с использованием операционной системы, загружаемой с внешнего диска, которая может быть отличной от сканируемой;

– в ходе устранения результатов атаки: сохранение следов атаки для предоставления правоохранительным органам, восстановление поврежденных программ и данных.

4.5. Методы антивирусной защиты

Для обеспечения надежной защиты от компьютерных вирусов необходимо применять следующий комплекс средств:

– использовать антивирусные программы;

– внедрять аппаратно-программные средства защиты;

– принимать организационные меры защиты;

– осуществлять резервное копирование наиболее ценных данных.

Так, **антивирусные программы** (например, Kaspersky, ESET NOD32, Dr.WEB, Avast) предоставляют следующие возможности.

Во-первых, регулярное автоматическое сканирование жестких дисков и подключаемых носителей на наличие вредоносных программ при каждом запуске операционной системы или внешнего носителя. Разумеется, для надежного обнаружения вредоносных программ следует иметь актуальные антивирусные базы.

Во-вторых, выполнение резидентной защиты, которая осуществляет:

– контроль изменения размеров и других атрибутов файлов;

– контроль обращений к файлам на жестком диске, перехват подозрительной активности, предупреждение пользователя о подозрительной активности.

– контроль сетевых подключений, блокировку сетевого трафика приложений, предупреждение пользователя о подозрительной сетевой активности. Блокировка сетевого трафика выполняется согласно установленным правилам. Например, для всех новых приложений подключения запрещены. Только после предоставления разрешения на подключения приложение сможет их создавать.

В-третьих, создание образа жесткого диска на внешних носителях.

Вспомогательным методом является **внедрение аппаратно-программных средств защиты**. Например, отключение перемычки на материнской плате не позволит осуществить стирание перепрограммируемой микросхемы ПЗУ (флэш-BIOS) независимо от того, кто это будет пытаться сделать: вредоносная программа, злоумышленник или пользователь [47].

Допускается также установка внешних контроллеров, приводящих в исполнение один или несколько программных средств защиты.

Соблюдение организационных мер защиты предполагает:

– выполнение правил обработки информации и использования программ;

– ограничение круга лиц, имеющих доступ к компьютеру;

– проверку с помощью антивирусной программы внешних подключаемых устройств перед их использованием, а также периодическое глубокое сканирование компьютера полностью;

– наблюдение за признаками заражения компьютера для своевременного обнаружения вредоносных программ и минимизации последствий их функционирования.

Наконец, наличие **резервных копий ценной информации** особенно актуально при потере или повреждении информации в результате технического сбоя, работы вредоносных программ либо вследствие человеческого фактора.

Копирование информации может быть выполнено в зависимости от вида копируемых файлов: образ операционной системы, файлы и архивы баз данных, полные копии жесткого диска.

Периодичность создания резервных копий и период их хранения должны зависить от частоты обновления информации на носителе.

Резервные копии информации должны храниться на отделяемых (внешних) от компьютера носителях, чтобы исключить их заражение. Хранение носителей осуществляется в отдельных сейфах, которые могут располагаться в разных помещениях. Периодически рекомендуется осуществлять ротацию носителей в местах хранения.

Зараженные вредоносными программами жесткие диски форматируют и подготавливают к новой эксплуатации: устанавливают операционную систему и прикладное программное обеспечение с дистрибутивных носителей.

Завершающим этапом является восстановление данных из резервных копий.

Вопросы для самопроверки

1. Каково назначение вредоносных программ?
2. По каким типам операционных систем делят вредоносные программы?
3. Какие классы вредоносные программы делят по вредоносным признакам?
4. Из каких частей состоит троянская программа?
5. Какие способы заражения компьютера вы знаете?
6. В какой степени вирусы могут влиять на работу компьютера?
7. Какие технологии проникновения вредоносных программ вы знаете?
8. Какие признаки заражения компьютера вредоносными программами вы знаете?
9. Какие программные средства защиты от вредоносных программ вы знаете?
10. Для чего применяют аппаратные средства защиты от вредоносных программ?
11. Какие принципы организационной защиты от вредоносных программ существуют?
12. Какие методы защиты от вредоносных программ вы знаете?

5. ПРЕДОСТАВЛЕНИЕ ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ПАРОЛЬНЫХ СИСТЕМ

Основными угрозами получения злоумышленниками несанкционированного доступа к конфиденциальной информации через парольные системы [47; 64] являются:

– утеря пользователем носителя информации, содержащего пароль;

– подглядывание пароля злоумышленником;

– преднамеренная передача владельцем пароля другому лицу;

– нежелание пользователей выполнять организационно-технические меры по защите информации;

– подбор пароля злоумышленником;

– кража базы данных учетных записей для дальнейшего анализа или подбора пароля;

– перехват вводимого пароля путем внедрения в компьютерную систему программных закладок (клавиатурных шпионов);

– перехват пароля по незащищенной сети;

– использование уязвимостей, ошибок, недокументированных возможностей реализации системы безопасности;

– атаки на основе социальной психологии (социальная инженерия).

Парольная система – программный или программно-аппаратный комплекс, который обеспечивает проведение процедур идентификации, аутентификации и авторизации субъектов на основании предъявляемых паролей. Парольная система включает в себя или функционирует совместно с подсистемами разграничения прав доступа (полномочий) и регистрации событий безопасности.

Парольные системы являются одними из основных и самых распространенных методов наделения полномочиями пользователей. При аутентификации пароль является секретом и должен быть известен только легальному пользователю.

Логическая ясность принципов функционирования и простота реализации механизмов предоставления доступа обеспечивают парольным системам широкое распространение. Однако к отдельным элементам парольных систем злоумышленники могут получать доступ под видом легального пользователя, что делает парольные системы привлекательными для атаки.

Определим основные понятия, применяемые в парольных системах.

Субъект – пользователь или программно-аппаратный комплекс, который пытается получить доступ к конфиденциальной информации.

Пароль – секретная информация, известная только легальному субъекту и парольной системе, которая предъявляется пользователем при прохождении аутентификации. В зависимости от используемого механизма аутентификации секретная информация, известная субъекту и парольной системе, может не совпадать.

Учетная запись субъекта – идентификатор и пароль субъекта, хранящиеся в парольной системе.

База данных – список всех учетных записей субъектов парольной системы.

5.1. Подходы к построению парольных систем

Основными функциональными элементами парольных систем являются:

– идентификация;
– аутентификация;
– авторизация;
– логирование и ведение учета.

Идентификация – присвоение субъектам идентификаторов при регистрации и последующее распознавание предъявляемого идентификатора из перечня существующих [47; 3].

Идентификатором является уникальная информация, позволяющая различать субъектов (пользователей) системы. Идентификатором субъекта может выступать имя пользователя, личный номер, электронный адрес, имя учетной записи пользователя и т.п.

Аутентификация – проверка соответствия предъявленного пароля паролю идентифицированного субъекта, хранящемуся в парольной системе. Для проверки соответствия паролей могут использоваться различные механизмы, например, сравнение на полное совпадение, сравнение сверток паролей, сравнение вероятностей подобия и др.

Выделяют [47] несколько основных способов аутентификации:

– аутентификация при наличии копии (свертки) пароля у обеих сторон требует создания и поддержки базы данных паролей и учетных записей пользователей, следовательно, при получении базы данных злоумышленник способен проходить аутентификацию от имени любого пользователя;

– аутентификация по некоторому проверочному значению обеспечивает более высокую степень безопасности парольной системы, поскольку

проверочные значения хотя и зависят от паролей, но не могут быть непосредственно использованы злоумышленником для аутентификации;

– аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты (подробнее – в п. 5.1.4);

– криптографические протоколы аутентификации описывают требуемую последовательность действий для обеих сторон, сочетаются с генерацией и распределением криптографических ключей для шифрования информационного обмена между сторонами (использование может быть ограничено законодательством).

В зависимости от количества используемых методов аутентификации выделяют однофакторную (применяется только один метод) и многофакторную (используется несколько методов) аутентификации. Например, если пользователь входит в интернет-банкинг только с использованием пароля, то применяется однофакторная аутентификация, а если при совершении платежа пользователю нужно дополнительно ввести код 3D-Secure, полученный на мобильный телефон, то применяется многофакторная аутентификация.

По уровню доверия выделяют одностороннюю и взаимную аутентификации. При односторонней аутентификации только субъект доказывает свою подлинность, а при взаимной аутентификации подлинность доказывает и субъект, и парольная система. Взаимная аутентификация, как правило, реализуется криптографическими средствами на уровне протоколов. Так, например, взаимная аутентификации реализуется протоколами TLS/SSL для работы веб-сайтов по HTTPS-протоколу, чтобы обезопасить пользователя от ввода конфиденциальных данных на фишинговых сайтах.

Авторизация – наделение субъектов правами доступа (полномочиями) на основании идентификатора. Авторизация выполняется после завершения успешной аутентификации.

Логирование и ведение учета во время функционирования парольных систем обеспечивают сбор событий информационной безопасности и активности пользователей. Сбор информации может выполнятся внутри самой парольной системы и (или) передается в SIEM-системы, которые обеспечивают хранение и анализ в реальном времени событий (тревог) безопасности для реагирования на них до наступления существенного ущерба.

На основании анализа собранных данных может выполняться автоматическое реагирование в реальном времени на основании предварительно заданных критериев. Автоматическое реагирование может включать в себя

блокировку пользователя, ограничение действий пользователя, уведомление специалиста по безопасности о подозрительном событии.

В числе основных компонентов парольной системы выделяют:

– носитель с паролем (не обязательный компонент, если пароль хранится в памяти человека);

– интерфейс предъявления пароля (интерфейс пользователя);

– интерфейс управления учетными записями (интерфейс администратора);

– компонент взаимодействия с другими подсистемами безопасности (например, системой логирования, системой оповещения и др.);

– базу данных учетных записей, которая обеспечивает хранение паролей.

Компоненты парольной системы могут быть реализованы как в одном приложении и работать в пределах одной вычислительной машины, так и в рамках распределенной системы аутентификации, все элементы которой являются самостоятельными подсистемами и работают на выделенных вычислительных машинах.

5.1.1. Способы предъявления паролей

В зависимости от способа ввода паролей выделяют следующие типы парольных систем:

– ручной ввод пароля;

– ввод техническими устройствами;

– биометрический ввод.

Ручной ввод пароля. Наиболее распространенный способ ввода пароля, т.к. является самым простым для внедрения и самым дешевым. При таком вводе пароля человек лично хранит и вводит пароль в систему из-за чего возникают недостатки ручного ввода, вызванные человеческим фактором:

– стремлением к выбору простого пароля;

– хранением паролей на бумажках или других незащищенных носителях;

– вводом пароля так, что другие пользователи могут подсмотреть пароль;

– возможностью намеренной или под влиянием заблуждений передачи пароля другому лицу;

– возможностью утери носителя с паролем.

Ввод техническими устройствами. В технических устройствах выполняется хранение секрета легального пользователя, с помощью которого выполняется аутентификация. Для получения доступа пользователь прикладывает (подключает) устройство хранения пароля к устройству проверки пароля. Широко распространенными техническими устройствами являются:

- идентификаторы Touch Memory;
- бесконтактные радиочастотные карты;
- пластиковые карты;
- USB ключи;
- SMART-карты.

Данные системы обладают высокой надежностью и скоростью, т.к. пользователю не требуется вводить руками пароль, а надежность пароля может быть достаточно высокой. Недостатками являются стоимость технических устройств, сложности их внедрения, возможность утери устройств с последующим доступом злоумышленником.

Биометрический ввод. Под биометрическим вводом понимается использование для аутентификации пользователя индивидуальных признаков человека. В качестве биометрических характеристик, которые могут быть использованы при аутентификации, достаточно часто применяют следующие:

- отпечатки пальцев;
- геометрическая форма рук;
- узор радужной оболочки и сетчатки глаз;
- форма и размеры лица;
- особенности голоса;
- биомеханические характеристики рукописного и клавиатурного почерка.

Парольные системы с биометрическим вводом обеспечивают идентификацию и аутентификацию конкретного человека, а не абстрактную сущность базы данных. Данное свойство является отличительным достоинством парольных систем с биометрическим вводом от систем других типов. Однако системы с биометрическим вводом требуют обучения под конкретных пользователей, зачастую достаточно длительного. В них существует возможность ошибочных отказов и ошибочных подтверждений при аутентификации пользователей. Специальные технические устройства для чтения биометрических характеристик, как правило, достаточно дорогостоящие.

5.1.2. Реакция парольных систем для противодействия попыткам подбора паролей

Реакция парольной систем – ответ парольной системы на действия пользователя. В зависимости от перечня реализованных реакций парольной системой обеспечивается стойкость к подбору паролей. Список возможных реакций парольных систем и получаемый эффект выглядят следующим образом [47]:

– скрытие идентификатора последнего работающего пользователя – усложняет задачу при попытке подобрать пароль;

– скрытие символов на экране для вводимого пароля – препятствует подсмотру злоумышленником пароля;

– установление минимальной длины пароля (на начало 2019 г. – 16 символов и больше) – усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального перебора»;

– использование в пароле различных групп символов – усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального перебора»;

– проверка и отбраковка пароля по словарю – усложняет задачу злоумышленника при попытке подобрать пароль по словарю;

– установление максимального срока действия пароля – усложняет задачу злоумышленника по подбору паролей методом «тотального перебора», в том числе без непосредственного обращения к системе защиты (режим «offline»);

– установление минимального срока действия пароля – препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию;

– ведение журнала истории паролей – обеспечивает дополнительную степень защиты по ограничению попыток входа и позволяет проводить аудит системы защиты;

– применение эвристического алгоритма, бракующего пароли на основании данных журнала истории, – усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма;

– ограничение числа попыток ввода пароля – препятствует интерактивному подбору паролей злоумышленником;

– использование задержки при вводе неправильного пароля – препятствует интерактивному подбору паролей злоумышленником;

– отсутствие постоянной блокировки учетной записи при попытке подбора пароля до снятия блокировки администратором – препятствует злоумышленнику намеренно заблокировать работу легального пользователя (реализовать угрозу нарушения доступности информации);

– запрет на выбор пароля самим пользователем и автоматическая генерация паролей – исключает возможность подобрать пароль по словарю. если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального перебора»;

– поддержка режима принудительной смены пароля пользователя – обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля;

– принудительная смена пароля при первой регистрации пользователя в системе – защищает от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи.

5.1.3. Хранение паролей

Одной из важнейших функций парольной системы является хранение паролей (информации о паролях) в базе данных учетных записей. Хранение паролей может выполняется согласно трем принципам [47]:

– в открытом виде;

– в виде хеш-значений (сверток);

– в шифрованном виде.

Хранение паролей в открытом виде является самым простым, но и самым небезопасным способом, т.к. при получении доступа к базе данных (таблице) злоумышленник получит доступ ко всем паролям.

При хранении паролей в хешированном или в шифрованном виде обеспечивается большая степень защищенности, т.к. при получении доступа к базе данных получить сразу исходный пароль будет невозможно.

Для получения исходного пароля для хешированных значений необходимо сначала определить алгоритм хеширования, а потом «подбирать» пароли по словарю либо «тотальным перебором». Перебор паролей выполняется до тех пор, пока не будет получено полное совпадение рассчитанной свертки пароля и свертки, хранящейся в базе данных.

Процесс расчета сверток паролей является достаточно трудоемким с точки зрения вычислительных ресурсов, поэтому злоумышленники могут воспользоваться уже готовыми расчетами сверток. Для исключения возможности подбора паролей по готовым сверткам используются механизмы, обеспечивающие уникальность сверток, – к паролю для расчета хеш-функции

добавляют некоторую случайную или псевдослучайную информацию. Например, в самом простом виде к паролю может быть добавлен идентификатор учетной записи базы данных или имя пользователя. Однако при таком хранении пароль пользователя нельзя восстановить, а можно только установить новый.

Получение исходного пароля для шифрованных значений выполняется путем дешифрования базы данных учетных записей. Криптостойкость алгоритмов шифрования способна обеспечивать надежную защиту паролей при условии надежного хранения секретного ключа [47].

Секретный ключ для шифрования базы данных учетных записей может генерироваться и храниться в системе программным способом или с использованием внешних носителей, а также вводится администратором при запуске системы.

Расшифровка шифрованных значений паролей возможна либо в случае использования некриптостойких алгоритмов шифрования, либо в случае компрометации пароля. Для наиболее безопасного хранения паролей используют комбинацию второго и третьего способов: сначала вычисляют свертки паролей, а потом выполняется шифрование полученных сверток.

5.1.4. Передача пароля по сети

Многие компьютерные сети обладают уязвимостью, которая позволяет прослушивать и перехватывать трафик, передаваемый по сети. Прослушивание трафика выполняется с помощью физического подключения сетевого адаптера к компьютерной сети и переключения сетевого адаптера в беспорядочный режим (promiscuous mode). В беспорядочном режиме сетевой адаптер принимает (прослушивает) весь трафик, передаваемый по локальной сети, в т.ч. не предназначенный для данного сетевого адаптера. В итоге из перехваченного трафика злоумышленник может извлекать незащищенные данные аутентификации.

Защищают данные аутентификации, передаваемые по компьютерной сети, следующим образом:

– обеспечивают физическую защиту компьютерной сети;
– используют шифрование пакетов;
– применяют сквозное (оконечное) шифрование.

Физическая защита компьютерной сети является дорогостоящей процедурой, которую возможно выполнить только для собственных сетей. В неконтролируемых сетях или сетях общего пользования гарантировать физическую защиту сети невозможно. Шифрование пакетов реализуется

дополнительным программным обеспечением или дополнительным оборудованием, например, виртуальными частными сетями (VPN) или шлюзами шифрования. Сквозное (оконечное) шифрование реализуется встраиванием в саму парольную систему, чтобы обеспечивать шифрование передаваемых данных между получателем и отправителем (интерфейсом пользователя и базой данных учетных записей).

Пароли (данные аутентификации) между интерфейсом пользователя и базой данных учетных записей могут передаваться [47]:

– в открытом виде;

– в зашифрованном виде;

– в виде сверток;

– без непосредственной передачи информации о пароле («доказательство с нулевым разглашением»).

Передача паролей в открытом виде абсолютно недопустима с точки зрения защиты конфиденциальности информации. Тем не менее, на практике передача паролей в открытом виде встречается достаточно часто вследствие незащищенности используемых сетевых протоколов (например, HTTP, TCP, TELNET, FTP и др.), большинство которых были разработаны десятки лет назад. Например, если выполняется авторизация пользователя на веб-сайте по протоколу HTTP (без использования SSL-сертификата), а не по протоколу HTTPS, то пароль и другие конфиденциальные данные пользователя сайта могут передаваться в открытом виде.

Осознавая данную проблему, передовые компании по предоставлению интернет-сервисов (Google, Mozilla, Яндекс и др.) всячески стимулируют внедрение SSL-сертификатов на веб-сайты, но, например, в Беларуси по-прежнему значительное число веб-сайтов остается незащищенными.

При **передаче паролей в зашифрованном виде или в виде сверток по сети без гарантированной физической защиты** возникают следующие угрозы безопасности [47]:

– перехват и повторное использование информации;

– перехват и восстановление паролей;

– модификация передаваемой информации с целью введения в заблуждение проверяющей стороны;

– имитация злоумышленником действий проверяющей стороны для введения в заблуждение пользователя.

Снижение вероятности возникновения указанных угроз возможно путем применения механизма одноразовых паролей. Механизм одноразовых паролей основан на принципе «один пароль используется только один раз».

Применение данного принципа не позволяет злоумышленнику повторно использовать перехваченные данные. Однако человек не способен запомнить большое количество одноразовых паролей, поэтому требуется применять дополнительные технологии, например:

– скретч-карты со списком одноразовых паролей;

– физические аппаратные токены, которые синхронизируют по времени пароли у пользователя и на сервере;

– математические алгоритмы, которые воспроизводят цепочку хешей (множества одноразовых паролей) по одному ключу или паролю;

– доставка одноразовых паролей по альтернативным каналам связи, например, SMS-сообщением.

Метод доказательства с нулевым разглашением (Zero knowledge proof, ZKP) позволяет доказывающей стороне (пользователю) доказать проверяющей стороне (парольной системе) знание пароля без разглашения каких-либо данных о самом пароле. Процесс доказательства значения строится на обмене сообщениями между доказывающей и проверяющей сторонами. Цель доказывающего – убедить проверяющего в истинности некоторого утверждения. Проверяющий либо принимает, либо отвергает доказательство. Доказательство носит вероятностную, а не абсолютную природу. При увеличении циклов общения вероятность истинного утверждения должно стремиться к единице, а вероятность ложного утверждения – к нулю.

Примером доказательство знания пароля с нулевым разглашением может служить «Пещера нулевого разглашения», описанная в работе «Как объяснить протокол доказательства с нулевым разглашением вашим детям» Жана-Жака Кискатера [69].

5.2. Обеспечение криптостойкости паролей

Для оценки качества применяемых паролей необходимо ввести количественные характеристики, которые могут быть вычислены при передаче по сети или хранении паролей в базе данных.

Под качественной характеристикой понимают криптостойкость паролей – вероятность подбора паролей в течение его срока действия (P).

Под количественными принимают следующие характеристики паролей [47]:

– длина пароля (L) – количество символов из которых состоит пароль;

– мощность алфавита паролей (A) – число символов в алфавите (например, мощность паролей, состоящих из прописных букв латинского алфавита, – 26);

– мощность пространства паролей (S) – вычисляется с помощью длины пароля и мощности алфавита паролей: $S = AL$;

– срок действия пароля (T) – промежуток времени, по истечении которого пароль становится недействительным;

– скорость проверки пароля (V) – для интерактивного режима определяется как максимальная скорость обработки одной попытки проверки пароля проверяющей стороной; для режима «offline» (перехваченного шифрованного или хешированного пароля) – как максимальная скорость вычисления значения для одного пароля.

Вероятность подбора пароля рассчитывается с помощью выражения

$$P = -\frac{V \cdot T}{S},$$

где подбор выполняется непрерывно в течение срока действия пароля при выбранной мощности пространства паролей со скоростью проверки пароля.

Исходя из представленного выражения, снизить вероятность подбора паролей можно [47]:

– увеличением времени проверки пароля. В интерактивном режиме за счет интерактивном режиме вводят задержку при вводе неправильного пароля, для режима «offline» – увеличивают вычислительную сложность алгоритма шифрования или хеширования;

– сокращением времени действия пароля;

– увеличением гарантированной мощности пространства паролей за счет увеличения минимальной длины паролей или увеличения мощности алфавита паролей.

Воспользуемся примером [47] для определения минимальной мощности пространства паролей (зависящей от A и L) в соответствии с заданной вероятностью подбора пароля P в течение его срока действия T.

Задано $P = 10^{-6}$.

Необходимо найти минимальную длину пароля, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль.

Пусть скорость интерактивного подбора паролей $V = 10$ паролей/мин. Тогда в течение недели можно перебрать 10 х 60 х 24 х 7 = 100 800 паролей. Далее, учитывая, что параметры S, V, T и P связаны соотношением, получаем:

$$S = -\frac{100\ 800}{10^{-6}} = 100\ 800 \cdot 106 = 1{,}008 \cdot 1011 = 1011;$$

$AL = 1011$.

Следовательно, для выполнения заданных условий S значения A и L могут принимать: $A = 10$, $L = 11$; $A = 26$, $L = 8$ или $A = 36$, $L = 7$.

Вопросы для самопроверки

1. Чем отличаются понятия идентификации, аутентификации и авторизации?
2. Какие основные компоненты парольных систем вы знаете?
3. Какие способы ввода пароля вы знаете?
4. Зачем необходимо накладывать требования на реакцию парольных систем при вводе данных?
5. На каких принципах основана стойкость паролей?
6. Какие способы хранения паролей вы знаете?
7. Зачем защищать передачу данных о паролях по сети?
8. Какие способы защиты передачи пароля по сети вы знаете?

6. ШИФРОВАНИЕ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Криптография представляет собой совокупность методов преобразования данных (шифрования), направленных на то, чтобы сделать передаваемые данные бесполезными для злоумышленника. Современная криптография предполагает, что сам алгоритм шифрования потенциально известен злоумышленнику, а защита данных обеспечивается только секретностью ключа [68].

Криптографическое преобразование информации (шифрование, алгоритм шифрования) – это зависящее **от ключа** (секретного параметра преобразования) взаимно однозначное математическое преобразование, которое ставит в соответствие блоку открытой цифровой информации (**исходный текст**) блок шифрованной цифровой информации (**шифротекст**). Для извлечения зашифрованных данных применяется обратный процесс – **дешифрование**.

6.1. Алгоритмы шифрования

Существует два основных типа алгоритмов шифрования, классификация которых представлена на рисунке 6.1:

- симметричные;
- асимметричные.

Симметричное шифрование. В алгоритмах симметричного шифрования отправителем и получателем используется общий ключ (секрет) для шифрования и дешифрования сообщения. Общий ключ передается отправителю и получателю по отдельному защищенному каналу до начала обмена сообщениями. Ключ шифрования на обеих сторонах хранится в секрете от злоумышленника [68]. Функциональная схема симметричного криптографического обмена представлена на рисунке 6.2.

В качестве преимуществ алгоритмов шифрования с симметричными ключами выделяются [47]:

- высокая производительность;
- высокая стойкость (при прочих равных условиях стойкость криптографического алгоритма определяется длиной ключа).

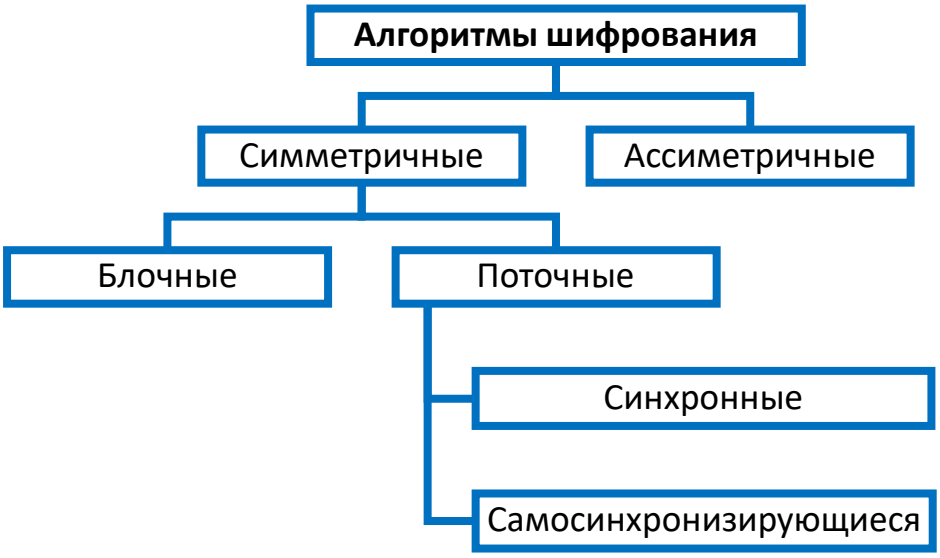


Рисунок 6.1. – Классификация алгоритмов шифрования

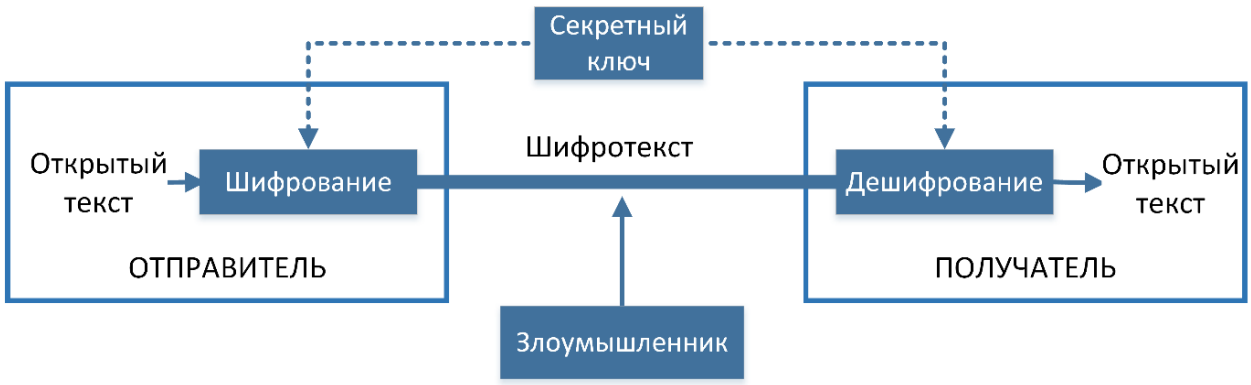


Рисунок 6.2. – Функциональная схема симметричного шифрования

Среди недостатков алгоритмов шифрования с симметричными ключами называют [47; 69]:

– необходимость использования надежного механизма передачи ключа, поскольку для шифрования и дешифрования сообщения используется общий ключ;

– огромное количество необходимых ключей, число которых растет в геометрической прогрессии в зависимости от числа участников коммуникации (например, для обмена сообщениями между 10 пользователями необходимо иметь 45 ключей, а для 1000 пользователей – уже 499 500);

– невозможность обеспечить такие свойства информации, как аутентичность и неотрекаемостъ.

Примерами распространенных алгоритмов симметричного шифрования являются [68]:

– DES;

– TripleDES (3DES);

– AES (Rijndael);

– ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

В зависимости от области применения симметричные алгоритмы делятся на блочные и поточные. Блочные алгоритмы шифруют информацию блоками заданного размера (например, по ГОСТ 28147-89 размер блока равен 64 бита), при этом в кодировании участвует только шифруемый блок и секретный ключ.

Поточные алгоритмы используют в случаях, если передача данных может быть начата и завершена в произвольные моменты времени.

В поточных алгоритмах кодирование каждого последующего символа зависит от всех предыдущих символов. Из-за этой особенности поточных алгоритмов возникают ошибки дешифрования в случае утери (пропуска) символов при передаче данных. Устранение ошибок исправляется путем применения синхронизации между шифратором и дешифратором.

Шифраторы и дешифраторы делят на синхронные и самосинхронизирующиеся. Синхронные осуществляют синхронизацию в момент создания связи, а самосинхронизирующиеся способны восстанавливать синхронизацию во время передачи данных. В литературе шифраторы и дешифраторы для поточного шифрования называют сремблерами, а процесс преобразования данных – скремблированием.

В современной практике поточные алгоритмы мало применяются, т.к. в современных системах передачи данных применяются сети с коммутацией пакетов, криптостойкость которых проще обеспечивать блочным шифрованием.

Асимметричное шифрование. В отличие от симметричных алгоритмов ассиметричные алгоритмы используют в своей работе два ключа: открытый, который распространяется свободно, без ограничений и предосторожностей, и закрытый – секретный [68].

Открытый и закрытый ключи генерируются таким образом, что они могут работать только в паре: первый используется только для шифрования, а второй только для дешифрования. Расшифровать и дешифровать одним и тем же ключом невозможно.

Примером ассиметричного шифрования может служить шкатулка, оборудованная специальным замком. Ее замок имеет два типа ключей. Первый позволяет только закрывать шкатулку, второй – только открывать. Ключи, которые только закрывают шкатулку, можно смело раздавать всем желающим или даже положить возле самой шкатулки, а ключ, который используется для открывания шкатулки, должен быть один и его необходимо хранить только у того, кому разрешено открывать эту шкатулку. Таким образом, вложить в шкатулку сообщение и ее закрыть может любой желающий, а извлечь из шкатулки и прочитать это сообщение – только тот, кому это сообщение предназначено.

Данный механизм шифрования идеально подходит для публичных сетей передачи данных, в т.ч. для сети Интернет. При установлении соединения клиент запрашивает у сервера открытый ключ. Полученным открытым ключом выполняется шифрование данных с последующей передачей их на сервер. Переданные данные расшифровать может только сервер, который имеет парный секретный ключ. Злоумышленник при перехвате шифротекста и открытого ключа не сможем извлечь открытый текст; все, что сможет сделать злоумышленник, – это зашифровать и передать получателю какое-нибудь сообщение. Функциональная схема ассиметричного шифрования представлена на рисунке 6.3.

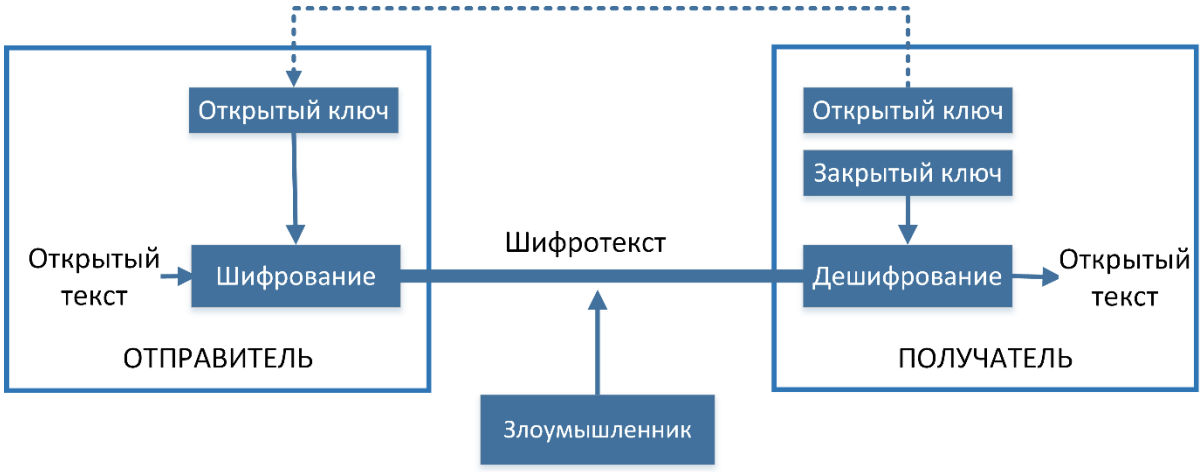


Рисунок 6.3. – Функциональная схема асимметричного шифрования

Функциональная схема отражает только одностороннюю передачу данных. Для двустороннего обмена данными необходимо:

– выполнить генерацию пары ключей и на отправителе, и на получателе;

– выполнить взаимный обмен открытыми ключами;

– выполнять шифрование передаваемых данных с помощью полученного открытого ключа второй стороны;

– выполнять дешифрование получаемых данных своим закрытым ключом.

В ассиметричном шифровании механизм использования ключей выгодно отличается от механизма симметричного шифрования, т.к. количество ключей не возрастает в геометрической прогрессии в зависимости от количества участников коммуникации. В такой схеме для распространения предназначен только один ключ – открытый.

Надежное и удобное распространение открытых ключей миллионам пользователей может осуществляться через центры распределения ключей и удостоверяющие центры: получатель сообщения передает свой открытый ключ только в центр распределения ключей, который потом распространяется всем желающим [68]. Схема распределения ключей с использованием центра распределения ключей приведена на рисунке 6.4.

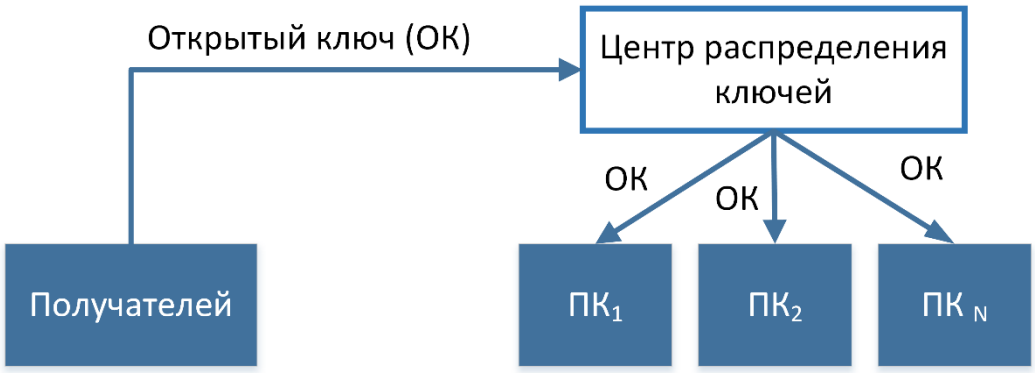


Рисунок 6.4. – Схема распределения открытых ключей с использованием центра распределения ключей

Недостатком ассиметричных алгоритмов шифрования является более высокая вычислительная сложность по сравнению с симметричными алгоритмами.

Ассиметричное шифрование в большей степени применимо в сетевых криптографических протоколах, тогда как симметричное – для шифрования данных. В некоторых случаях используется комбинирование симметричного и ассиметричного шифрования [47], что позволяет использовать преимущество обеих схем шифрования. Принцип работы комбинированных схем заключается в том, что для очередного сеанса обмена сообщениями генерируется симметричный (сеансовый) ключ. Затем этот

ключ зашифровывается и пересылается с помощью асимметричной схемы. После завершения текущего сеанса обмена данными симметричный ключ уничтожается.

6.2. Криптостойкость алгоритмов шифрования и криптоаналитические атаки

Криптостойкостью (стойкостью алгоритма шифрования) называется свойство криптосистемы противостоять криптоатаке – попытке злоумышленника расшифровать шифротекст для получения открытого текста или зашифровать свой собственный текст для получения правдоподобного шифротекста без подлинного ключа.

Чтобы криптографический алгоритм считался абсолютно стойким (теоретически нераскрываемым), он должен удовлетворять следующим условиям [47]:

– длина ключа равна или больше длины сообщения;

– ключ генерируется для каждого сообщения (каждый ключ используется только один раз);

– ключ статистически надежен (вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны);

– исходный (открытый) текст обладает некоторой избыточностью (что является критерием оценки правильности расшифровки).

Очевидно, что абсолютно стойкий криптографический алгоритм практически труднореализуем. Единственный теоретически стойкий метод на сегодняшний день – симметричное шифрование с одноразовым блокнотом, которое основано на применении в качестве ключа последовательности случайных чисел (символов) [47].

В подавляющем большинстве случаев современные алгоритмы шифрования основаны на вычислительной сложности взлома (такие криптографические алгоритмы называют достаточно стойкими) [47]. Криптостойкость алгоритмов во многом определяется длиной ключа и его непредсказуемостью («похожестью на случайность») [47].

Криптоанализ – процесс дешифровки зашифрованной информации без предназначенного для такой расшифровки ключа.

Криптографическая (криптоаналитическая) атака на шифр («взлом шифра») – методы выявления уязвимостей криптографического алгоритма и выяснения ключа.

Выделяют [68] следующие основные типы криптоаналитических атак:

– криптоаналитическая атака при наличии только известного шифротекста (задача – извлечь открытый текст);

– криптоаналитическая атака при наличии только известного открытого текста (задача – найти ключ шифрования для последующей прямой расшифровки шифротекстов);

– силовая криптоаналитическая атака методом полного перебора всех возможных ключей при известном шифротексте (задача – подобрать ключ для извлечения открытого текста);

– криптоаналитическая атака методом статистического анализа частотности символов (вероятных слов, сочетаний символов) шифротекста (задача – получить информацию о символах открытого текста).

Успешность криптоаналитической атаки, как правило, зависит от наличия у злоумышленника (иногда он именуется криптоаналитиком) следующих ресурсов:

– конкретного объема перехваченных зашифрованных сообщений;

– временных ресурсов;

– вычислительных ресурсов.

Стойким считается алгоритм, требующий от злоумышленника практически недостижимых вычислительных ресурсов, или недостижимого объема перехваченных зашифрованных сообщений, или времени раскрытия, которое превышает время жизни конфиденциальной информации [47].

Скажем, в некоторых случаях время, необходимое для проведения вычислений, может превышать время жизни (актуальности) конфиденциальной информации (например, военная тактическая информация «живет» от нескольких минут до нескольких часов, информация о выпуске продукции – до нескольких недель, тогда как некоторые персональные данные могут быть актуальны более пятидесяти лет).

6.3. Скрытие факта существование сообщения стеганографическими методами

Стеганография (от греч. στεγανός – скрытый + γράφω – пишу; буквально «тайнопись») – наука, позволяющая спрятать передаваемые данные в некотором контейнере, таким образом скрыв сам факт передачи информации.

Приемы стеганографии позволяют скрывать не содержимое конфиденциального сообщения (как это происходит в криптографии), а сам факт

его существования таким образом, что злоумышленник не сможет догадаться о наличии такого сообщения.

Приемы стеганографии показывают свою эффективность не только в случае необходимости защиты конфиденциальной информации, но и в целях охраны результатов интеллектуальной деятельности (как правило, объектов авторского права), а также для сокрытия (маскировки) программного обеспечения (информации), минуя системы мониторинга.

Очевидно, что объединение приемов криптографии и стеганографии дает значительно больший эффект в защите информации.

Базовыми понятиями в стеганографии являются следующие:

– сообщение – внедряемое послание, которое необходимо спрятать;

– контейнер (стегоконтейнер) – любой объект, используемый для тайного внедрения сообщения;

– стегосистема – методы и средства, используемые для создания скрытого канала для передачи информации;

– стегоканал – канал для передачи стегоконтейнера;

– ключ – ключ для получения скрытого содержания из контейнера (используется не всегда).

Современные стеганографические методы основываются на таких положениях [47], как:

– методы скрытия не должны нарушить аутентичность и целостность файла;

– следует исходить из того, что злоумышленник осведомлен о стеганографических методах;

– стеганографическое преобразование должно сохранять основные свойства файла-контейнера при внесении в него секретного сообщения и ключа;

– извлечение самого секретного сообщения должно представлять сложную вычислительную задачу на случай раскрытия факта существования такого сообщения.

Наиболее простые (и самые древние) стеганографические методы основаны на сокрытии тайного сообщения в открытом тексте. Такие методы могут предполагать смещение слов, предложений, абзацев путем вставки дополнительных пробелов, а также создание сообщения из определенных позиций букв (частный случай – акростих) или частей открытого текста, созданного для имитации реального сообщения.

Свойства электронных файлов предоставляют дополнительные возможности для применения стеганографических методов. В частности, для

передачи информации могут использоваться приемы текстовых редакторов, позволяющие не отображать скрытый текст на экране (например, «невидимые» поля для примечаний, белый шрифт на белом фоне и т.п.). Более продвинутый вариант – использование для передачи сообщения полей компьютерных форматов данных, а также передача сообщения в резервном секторе внешнего диска, который обычно не используется для хранения информации (так называемая «нулевая дорожка»).

Необходимо учитывать, что вышеописанные методы достаточно просты и известны более или менее продвинутому пользователю, поэтому не обеспечивают эффективной защиты и пригодны для сокрытия небольшого объема данных.

Более перспективными являются методы, использующие избыточность мультимедийных форматов: цифровой фотографии, цифрового звука и цифрового видео [47]. Мультимедийные форматы содержат большие матрицы чисел, которые описывают уровни цвета или звуковых волн в дискретном времени. Эти уровни представляются не совсем точными значениями из-за погрешности оцифровки или сжатия аналоговых сигналов, поэтому их незначительное искажение не влияет на качество восприятия. Увеличение разрешающей способности мультимедийных данных по уровням сигналов или частоте позволяет увеличивать количество скрываемой информации.

Основное преимущество таких методов состоит в том, что они позволяют скрывать и передавать большие объемы информации. В то же время статистические характеристики таких данных очевидно искажаются и требуют последующей корректировки, из чего следует, что приведенные методы также несовершенны.

Вопросы для самопроверки

1. Для чего используется шифрование данных?
2. Чем отличаются алгоритмы симметричного и асимметричного шифрования?
3. Что такое стойкость алгоритмов шифрования?
4. Какие типы угроз при шифровании вы знаете?
5. Какие средства реализации алгоритмов шифрования существуют?
6. Каким образом криптография может скрыть факт передачи сообщения?
7. Что может быть контейнером для применения стеганографии?

7. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

Межсетевые экраны (файерволы, брандмауэры)[20] являются элементами защиты компьютерной сети и персональных компьютеров.

По определению межсетевой экран служит контрольным пунктом на границе двух сетей: чаще всего – между внутренней сетью организации и внешней сетью (обычно сетью Интернет), как показано на рисунке 7.1, однако межсетевые экраны могут применяться и для разграничения внутренних подсетей корпоративной сети организации.

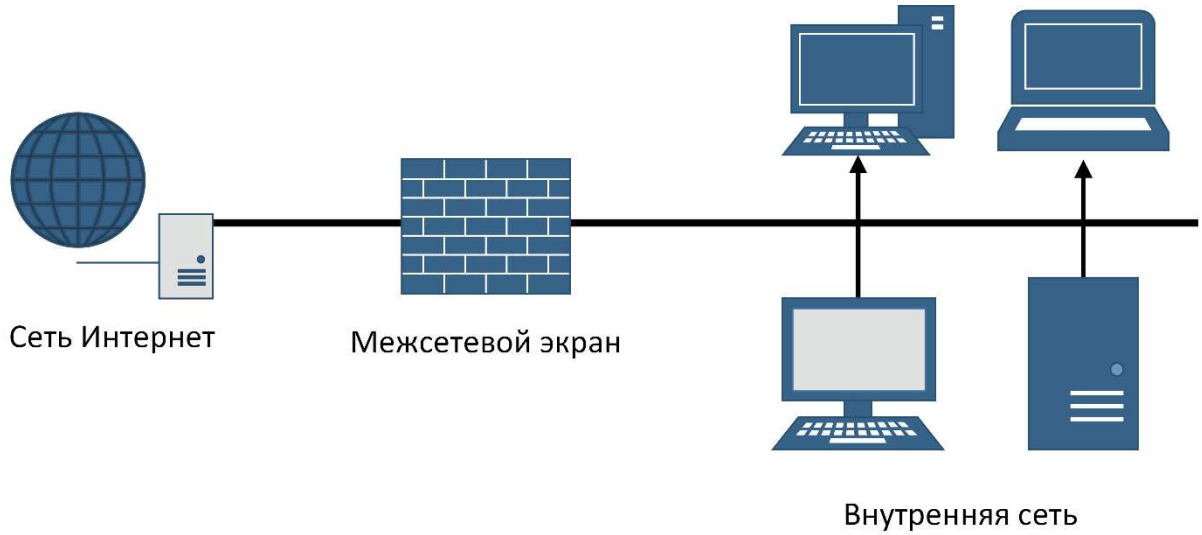


Рисунок 7.1. – Типовое размещение межсетевых экранов в вычислительной сети

Межсетевые экраны служат следующим задачам:

– контролируют весь трафик, входящий во внутреннюю сеть;

– контролируют весь трафик, исходящий из внутренней сети.

Как правило, межсетевые экраны представляются в виде системы фильтров [22], где каждый фильтр на основе анализа проходящих через него данных принимает решение – пропустить данные дальше, перебросить за экран, блокировать или преобразовать (рисунок 7.2).

[20] Англ. firewall – огненная стена, нем. brand – пожар, mauer – стена. В строительной сфере брандмауэром называется огнеупорный барьер, разделяющий отдельные блоки в многоквартирном доме и препятствующий распространению пожара. Межсетевой экран выполняет подобную функцию для компьютерных сетей [22].

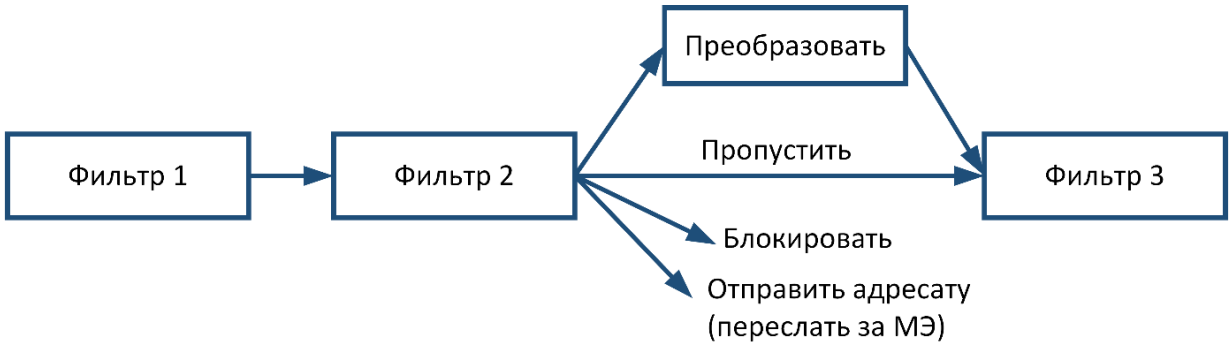


Рисунок 7.2. – Схема контроля трафика в межсетевых экранах

Например, контроль входящего трафика может запрещать все входящие подключения, кроме подключений на 443 порт, а контроль исходящего трафика – разрешать все исходящие подключения, кроме подключений к IP-адресам (или доменов) социальных сетей.

Межсетевое экранирование сопровождается протоколированием информационного обмена (ведением журналов регистрации), что позволяет администраторам сетей выявлять подозрительные действия, ошибки в конфигурации межсетевого экрана, после чего принимать решение об изменении межсетевого экрана.

7.1. Классификация межсетевых экранов

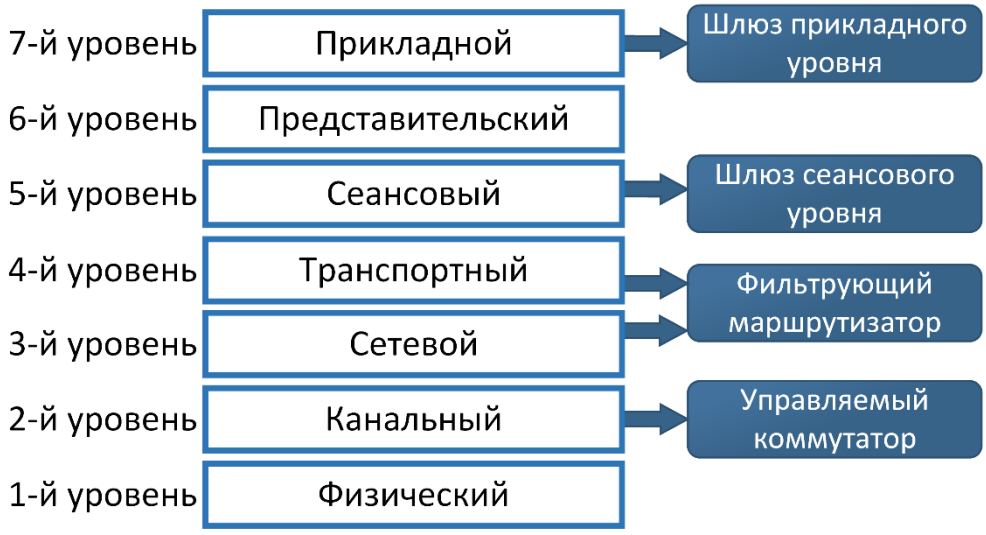


Рисунок 7.3. – Фильтрация трафика межсетевыми экранами на разных уровнях модели OSI

В дальнейшем используется следующая классификация [22] межсетевых экранов (см. рисунок 7.3):

- мостиковые экраны (второй уровень OSI);
- фильтрующие маршрутизаторы (третий и четвертый уровни OSI);
- шлюзы сеансового уровня (пятый уровень OSI);
- шлюзы прикладного уровня (седьмой уровень OSI);
- комплексные экраны (третий–седьмой уровни OSI).

7.1.1. Управляемые коммутаторы

Управляемые коммутаторы выполняют фильтрацию трафика на канальном уровне на основании MAC-адресов или VLAN ID, содержащихся в заголовках фреймов.

Технология фильтрации на основании MAC-адресов не является эффективной из-за возможности программного изменения MAC-адреса устройства. Однако технология построения виртуальных локальных сетей (VLAN – Virtual Local Area Network) является мощным и достаточно дешевым решением, которое позволяет создавать группы хостов, трафик которых полностью изолирован от других узлов сети.

В качестве достоинств межсетевых экранов канального уровня называют [22]:

- отсутствие необходимости менять настройки корпоративной сети и осуществлять дополнительное конфигурирование сетевых интерфейсов самого межсетевого экрана;
- высокую производительность в сочетании с простотой самого устройства;
- отсутствие IP-адреса (устройство функционирует на втором уровне модели OSI), вследствие чего устройство недоступно в сети и в результате злоумышленнику сложнее реализовать атаку.

7.1.2. Фильтрующие маршрутизаторы

Межсетевой экран с фильтрацией пакетов (англ. packet-filtering firewall) – маршрутизатор или компьютер, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отфильтровывать определенные виды входящих и исходящих пакетов [71]. Это достаточно старая технология (ей около 20 лет). Такие межсетевые экраны работают на третьем уровне модели OSI. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов (адреса отправителя и получателя, номера портов и др.), поэтому их иногда называют меж-

сетевыми экранами на основе порта [22]. Каждый пакет сравнивается со списками правил (адрес источника/получателя, порт источника/получателя).

Фильтрующие маршрутизаторы – недорогое средство, простое и достаточно высокопроизводительное, однако наименее безопасное из всех межсетевых экранов. Из-за своей практичности фильтрующие маршрутизаторы встраиваются в качестве обязательного компонента в большинство устройств сетевой безопасности.

Пример фильтрующего маршрутизатора – список контроля доступа (англ. ACL – access control lists).

7.1.3. Шлюзы сеансового уровня

Шлюз сеансового уровня (англ. circuit-level gateway) – межсетевой экран, который исключает прямое взаимодействие между внешним клиентом и внутренним хостом за счет функции посредничества на сеансовом уровне модели OSI [22]. Функция посредничества реализуется за счет создания виртуального соединения от внешнего IP-адреса и порта шлюза к внутреннему IP-адресу и порту целевого хоста. Виртуальное соединение обеспечивает переброс (копирование) пакетов в обоих направлениях виртуального соединения.

Установление виртуального соединения (сеанса) осуществляется после проверки допустимости запрашиваемого подключения. Допустимым сеанс является после того, как шлюз выполнит авторизацию обоих участников подключения и проверит правила квотирования на установку подключения. После установки сеанса шлюз просто выполняет копирование пакетов от источника к получателю без выполнения функций фильтрации.

Шлюзы сеансового уровня позволяют обеспечивать функцию трансляции внутренних IP-адресов при взаимодействии с внешней сетью (NAT, network address translation). Трансляция выполняется по отношению ко всем пакетам, которые направляются из внутренней сети во внешнюю сеть. При перенаправлении пакетов во внешнюю сеть реальный IP-адрес внутреннего хоста (отправителя пакета) заменяется на IP-адрес шлюза. В результате внешний хост считает, что инициирует подключение к нему не внутренний хост, а шлюз.

Благодаря шлюзам сеансового уровня исключается прямое взаимодействие между внешней и внутренней сетями, а IP-адрес шлюза становится единственным доступным IP-адресом во внешней сети [22]. Шлюзы сеансового уровня – достаточно надежные и недорогие средства экранирования

сети, обеспечивающие более высокий уровень защиты, чем фильтрующие маршрутизаторы.

Недостатком шлюзов сеансового уровня является то, что они не выполняют фильтрацию в пакетах поля данных, из-за чего существует возможность передачи во внутреннюю сеть вредоносных программ. Устраняется недостаток тем, что шлюзы сеансового уровня не являются отдельными продуктами, а функционируют в комплексе со шлюзами прикладного уровня.

Пример шлюза сеансового уровня – SOCKS прокси.

7.1.4. Шлюзы прикладного уровня

Шлюз прикладного уровня (англ. application-level gateways) – межсетевой экран, который исключает прямое взаимодействие между внешним клиентом и внутренним хостом за счет функции посредничества на прикладном уровне модели OSI (прокси). В отличие от сеансового уровня прикладной уровень модели ISO позволяет выполнить больше функций:

– идентификацию, аутентификацию и авторизацию пользователей при установлении подключений через межсетевой экран;

– в зависимости от типа авторизованного пользователя разграничивает доступ к внутренним и внешним ресурсам;

– проверку передаваемых данных на предмет наличия вредоносных программ;

– ведение логов, регистрацию событий безопасности, автоматическое реагирование на подозрительную активность, формирование отчетов;

– кэширование данных.

Для каждого прикладного протокола используется отдельный программный посредник – экранирующий агент (англ. application proxy). Каждый агент ориентирован на обработку только одного прикладного протокола (одной службы), например, HTTP, FTP, SMTP, NNTP и др.

В отличие от шлюзов сеансового уровня шлюзы программного уровня не просто перенаправляют все пакеты получателю, но еще и обрабатывают их соответствующим экранирующим агентом для передаваемого протокола. И если прикладной шлюз не может обработать пакет существующим экранирующим агентом, то пакет блокируется. Так, например, HTTP-прокси будет обрабатывать только HTTP-трафик, а все остальные пакеты будут блокироваться.

Каждый экранирующий агент при обработке пакетов может осуществлять большее количество дополнительных проверок, которые

уменьшают вероятность реализации атак. Например, выполнять проверку передаваемых файлов на наличие вредоносных программ, ограничивать выполнение подозрительных операций, ограничивать время выполнения команд и т.п.

Шлюзы программного уровня выполняют обработку трафика на программном уровне, поэтому для эффективной работы в нагруженных сетях требуется высокая производительность аппаратного обеспечения. Высокие требования к производительности аппаратного обеспечения и квалификации обслуживающего персонала являются недостатками прикладных шлюзов. Особенно существенно снижается пропускная способность прикладных шлюзов при межсетевом взаимодействии.

7.1.5. Шлюз экспертного уровня

Шлюз экспертного уровня (англ. Stateful multi-layer firewall) – межсетевой экран, который обеспечивает фильтрацию сетевого трафика с помощью многоуровневого анализа состояния пакетов.

Шлюзы экспертного уровня включают в себя элементы фильтрующих маршрутизаторов, шлюзов сеансового и прикладного уровней: обеспечивают фильтрацию сетевых пакетов по заголовкам транспортного уровня, контроль состояний сетевых соединений и фильтрацию пакетов на прикладном уровне. Фильтрация пакетов на прикладном уровне осуществляется с помощью быстрого осмотра (инспекции) пакетов с известным (дружественным) состоянием, что позволяет значительно сократить время обработки пакета.

По сравнению со шлюзами прикладного уровня шлюзы экспертного уровня имеют более высокую производительность межсетевого взаимодействия, но более низкую степень защиты из-за отсутствия глубокого анализа передаваемых данных. Как правило, шлюзы экспертного уровня обладают высокой стоимостью и сложностью внедрения.

Пример шлюза экспертного уровня – FortiGate, CheckPoint Firewall.

7.1.6. Персональные межсетевые экраны

Персональный межсетевой экран (англ. personal firewall) – межсетевой экран, устанавливаемый на персональный компьютер для контроля всего входящего и исходящего трафика независимо от прочих системных средств защиты. Контроль трафика выполняется на основании установленных политик работы межсетевого экрана и правил фильтрации трафика. Фильтрация передаваемого трафика может включать в себя сканирование на наличие вредоносных программ с помощью сигнатур.

Дополнительной возможностью персональных межсетевых экранов может являться контроль трафика на уровне исполняемых файлов и сетевых библиотек, что позволяет обеспечивать более надежную и гибкую защиту персонального компьютера.

Современные антивирусные программы могут содержать персональные межсетевые экраны, что позволяет выполнять регулярное обновление сигнатур фильтрации сетевого трафика совместно с сигнатурами вирусов. Интегрированные межсетевые экраны в антивирусные программы могут обеспечивать более надежную фильтрацию сетевого трафика с большим удобством работы пользователя.

Сложность настройки персональных межсетевых экранов обусловлена количеством персональных компьютеров в локальной сети: чем больше компьютеров, тем сложнее обеспечивать их тщательную настройку.

7.2. Политика работы межсетевых экранов

Политика межсетевого экрана определяет принцип, в соответствии с которым будет обрабатываться (фильтроваться) сетевой трафик.

Существует два вида политик работы межсетевых экранов [72]:

– запрещать все, что не разрешено в явной форме (англ. deny by default);

– разрешать все, что не запрещено в явной форме (англ. allow by default).

Для входящих и исходящих соединений могут применяться различные политики, что позволяет более гибко подходить к настройке. Например, на некоторых промышленных серверах для входящих и исходящих соединений целесообразно применять политику «запрещать все, что не разрешено в явной форме», а на обычных рабочих станциях для входящих соединений – «запрещать все, что не разрешено в явной форме», для исходящих соединений – «разрешать все, что не запрещено в явной форме».

7.3. Схемы подключения межсетевых экранов

Степень защиты и сложность настройки локальной вычислительной сети зависит от схемы подключения межсетевого экрана. Выделяют две основные схемы подключений межсетевого экрана в локальной вычислительной сети:

– схема единой защиты локальной сети;

– схема с раздельной защитой закрытой и открытой подсетей.

Для обеспечения внутренней локальной сети дополнительной защитой от внешних атак рекомендуется организация демилитаризованной зоны (ДМЗ, DMZ). Демилитаризованная зона – отдельный от локальной (защищенной) сети физический или логический сегмент сети, содержащий публичные серверы.

Назначение демилитаризованной зоны – изолировать внутреннюю сеть от публичной сети с сохранением доступа к публичным серверам и тем самым реализовывать многоуровневую стратегию защиты на сетевом уровне. Сетевой трафик не должен покидать демилитаризованную зону либо проникать в нее, минуя правила межсетевого экрана.

7.3.1. Схема единой защиты локальной сети

Схема единой защиты является наиболее простым и бюджетным решением, т.к. в ней участвует только один межсетевой экран, который устанавливается перед локальной сетью и публичными серверами (веб-сервер, файловый-сервер, почтовый сервер и другие сервера) [22]. Таким образом, весь трафик из публичной сети проходит в локальную сеть через межсетевой экран (рисунок 7.4).

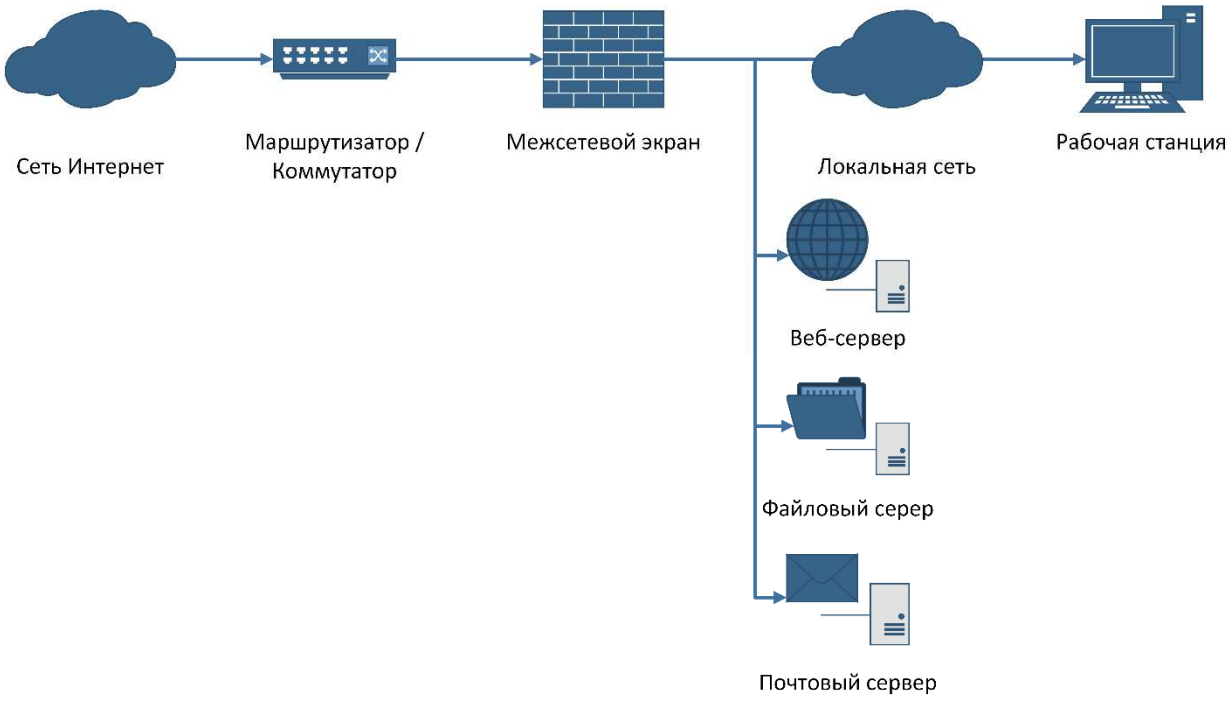


Рисунок 7.4. – Схема единой защиты локальной сети

Для настройки схемы рекомендуется применять политику «запрещать все, что не разрешено в явной форме», а межсетевой экран рекомендуется делать единственным видимым устройством из публичных сетей. При

реализации данной схемы администратору требуется выполнять тщательную настройку межсетевого экрана, чтобы обеспечивать предотвращения проникновения на персональные компьютеры локальной сети через публичные серверы.

Для разделения настроек безопасности для локальной сети и публичных серверов существуют межсетевые экраны с возможностью выделения демилитаризованной зоны. Такие межсетевые экраны имеют три сетевых интерфейса: первый интерфейс используется для подключения в публичную сеть, второй – в локальную сеть, а третий – в демилитаризованную зону (рисунок 7.5).

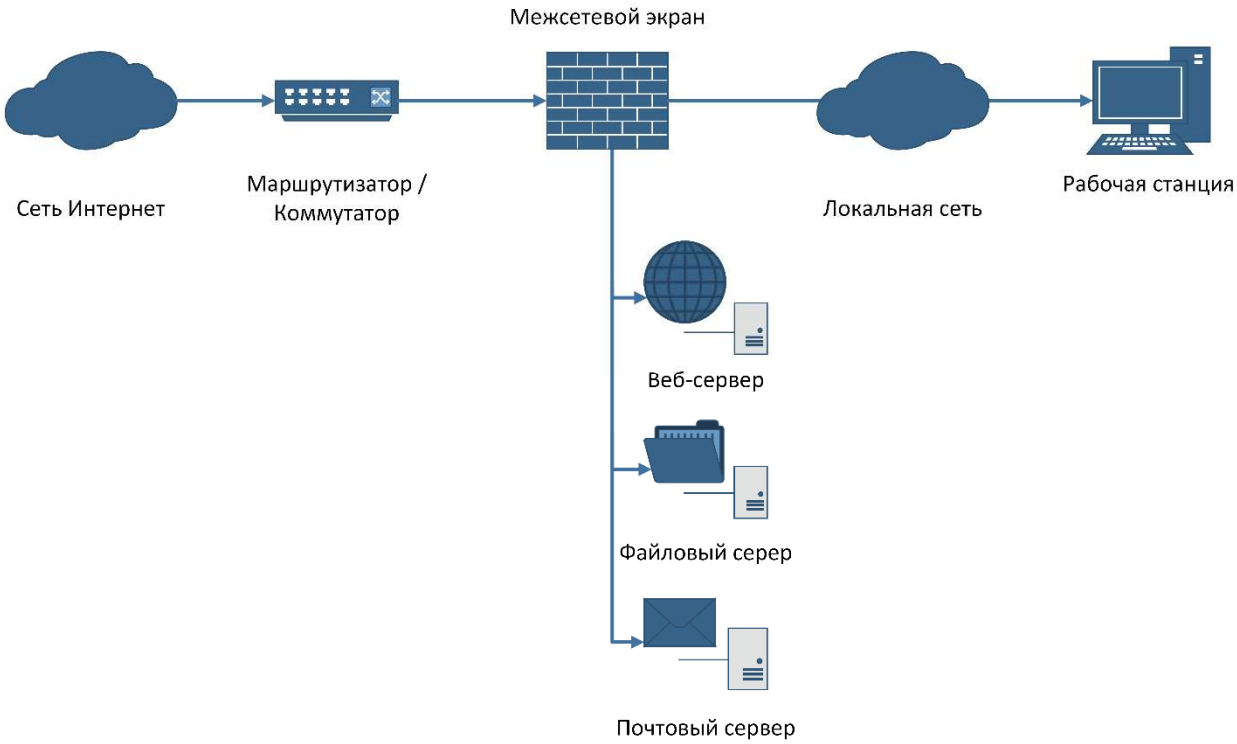


Рисунок 7.5. – Схема единой защиты локальной сети с выделением демилитаризованной зоны

Настройка правил для демилитаризованной зоны выполняется отдельно от правил локальной сети, поэтому такое подключение обладает большей гибкостью и степенью защиты.

Представленная схема проста в реализации, однако требует надежного оборудования и профессионального администрирования, поскольку межсетевой экран должен обрабатывать весь трафик, который проходит демилитаризованную зону и локальную сеть. При этом межсетевой экран становится единой точкой отказа, и в случае его взлома (или ошибки в настройках) локальная сеть окажется уязвимой [73].

7.3.2. Схема с раздельной защитой закрытой и открытой подсетей

В реализации схемы участвуют два межсетевых экрана, каждый из которых отдельно защищает открытую и закрытую сеть (рисунок 7.6). Участок между межсетевыми экранами является демилитаризованной зоной.

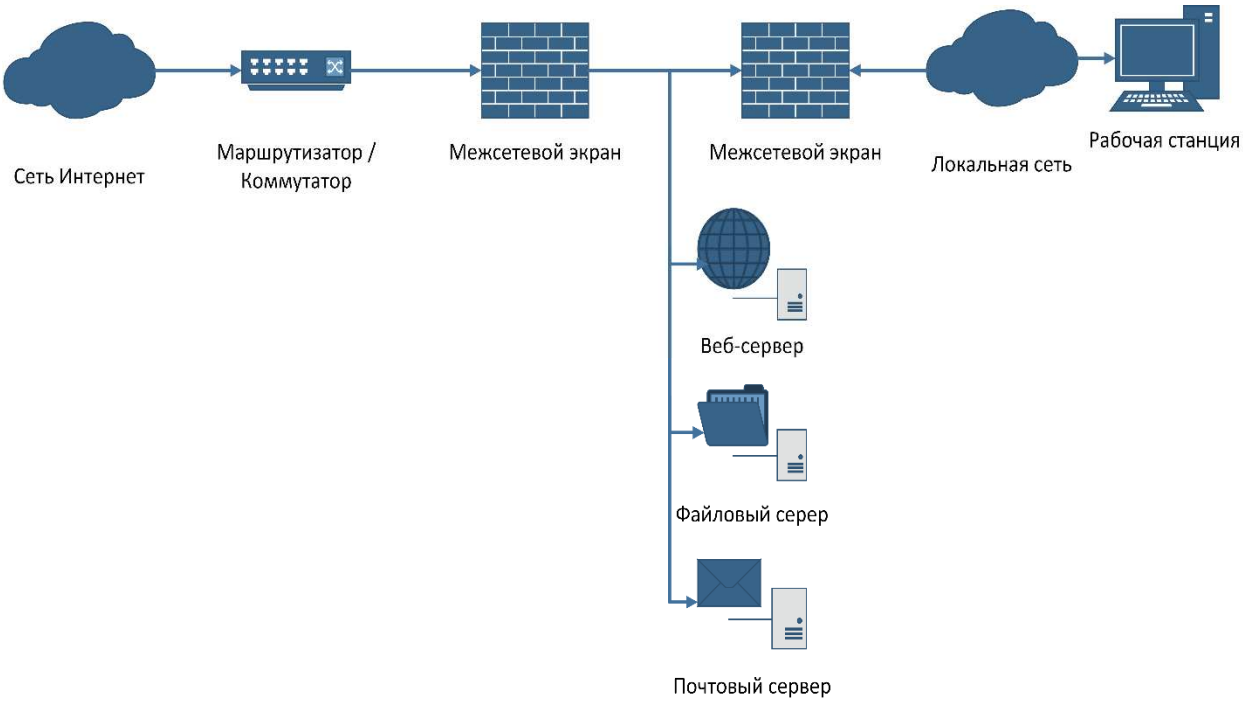


Рисунок 7.6. – Схема с раздельной защитой закрытой и открытой подсетей

Каждый межсетевой экран настраивается отдельно, что обеспечивает более высокую надежность и гибкость защиты. На внешнем межсетевом экране допускается настройка более сложных (медленных) правил фильтрации, что обеспечивает усиленную защиту без негативного влияния на производительность внутреннего сегмента сети [73].

Еще более высокий уровень защиты можно обеспечить, используя два межсетевых экрана двух разных производителей и (желательно) различной архитектуры, что уменьшает вероятность наличия одинаковых уязвимостей в обоих устройствах. Так, случайная ошибка в настройках с меньшей вероятностью появится в конфигурации интерфейсов двух разных производителей, а уязвимость в безопасности одного производителя с меньшей вероятностью окажется в системе другого [73]. Недостатком такого подхода является высокая стоимость.

Вопросы для самопроверки

1. Какие основные задачи выполняют межсетевые экраны?
2. Каким образом выполняется контроль сетевого трафика?
3. В чем основные преимущества применения мостиковых межсетевых экранов?
4. Какой принцип фильтрации трафика реализован в фильтрующих межсетевых экранах?
5. Что отличает шлюзы сеансового уровня от других типов межсетевых экранов?
6. Для какие целей используют шлюзы прикладного уровня?
7. В каких случаях целесообразно применять межсетевые экраны экспертного уровня?
8. Чем персональные межсетевые экраны отличаются от других типов межсетевых экранов?
9. Приведите пример необходимости использования динамического межсетевого экрана.
10. Какие политики межсетевого экрана целесообразно применять на серверах, а какие на рабочих станциях?
11. В чем основной недостаток схемы единой защиты локальной сети?
12. В чем основное преимущество схемы с раздельной защитой закрытой и открытой подсетей?

8. ОБНАРУЖЕНИЕ АТАК И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

8.1. Понятие системы обнаружения атак и предотвращения вторжений

Система обнаружения атак, СОА (англ. Intrusion Detection System, IDS) – это программное или программно-аппаратное средство обнаружения сетевых атак наряду со стандартными средствами защиты (межсетевыми экранами, системами резервного копирования и антивирусными средствами).

Система предотвращения вторжений, СПВ (англ. Intrusion Prevention System, IPS) – это программное или программно-аппаратное средство для обнаружения и предотвращения фактов неавторизованного доступа в компьютерную сеть либо несанкционированного доступа в информационную систему. В отличие от системы обнаружения атак система предотвращения вторжений функционирует в реальном времени и кроме функций обнаружения включает в себя и функции по блокированию (предотвращению) аномальной активности.

СОА/СПВ активно внедряются в практику обеспечения безопасности корпоративных сетей, в т.ч. и в странах СНГ, однако процессу внедрения препятствуют ряд проблем. Прежде всего, это высокая стоимость коммерческих СОА/СПВ, особенно в условиях, когда мероприятия по обеспечению информационной безопасности финансируются по остаточному принципу. При этом СОА/СПВ достаточно требовательны к ресурсам (отмечается неудовлетворительная производительность уже в сетях на 100 Мбит/с) и характеризуются большим числом ложных срабатываний и несрабатываний [22]. Такие системы требуют высокой квалификации обслуживающих их специалистов и наработанных эффективных методик анализа и управления рисками.

Типовая архитектура систем обнаружения атак и предотвращения вторжений, как правило, включает в себя компоненты [22], представленные на рисунке 8.1 и описанные ниже.

Сенсор – средство сбора информации о событиях безопасности. В различных промышленных системах могут использовать различные названия для сенсоров, например, детектор, коннектор, контроллер. Сенсор интегрируется с компонентом информационной системы, обеспечивающим сбор данных о событиях безопасности. В зависимости от выбранной политики генерации события сенсором выполняется фильтрация всех событий для обнаружения целевого события. Целевое событие сохраняется (записывается в журналы, базы данных событий) и передается в анализатор.

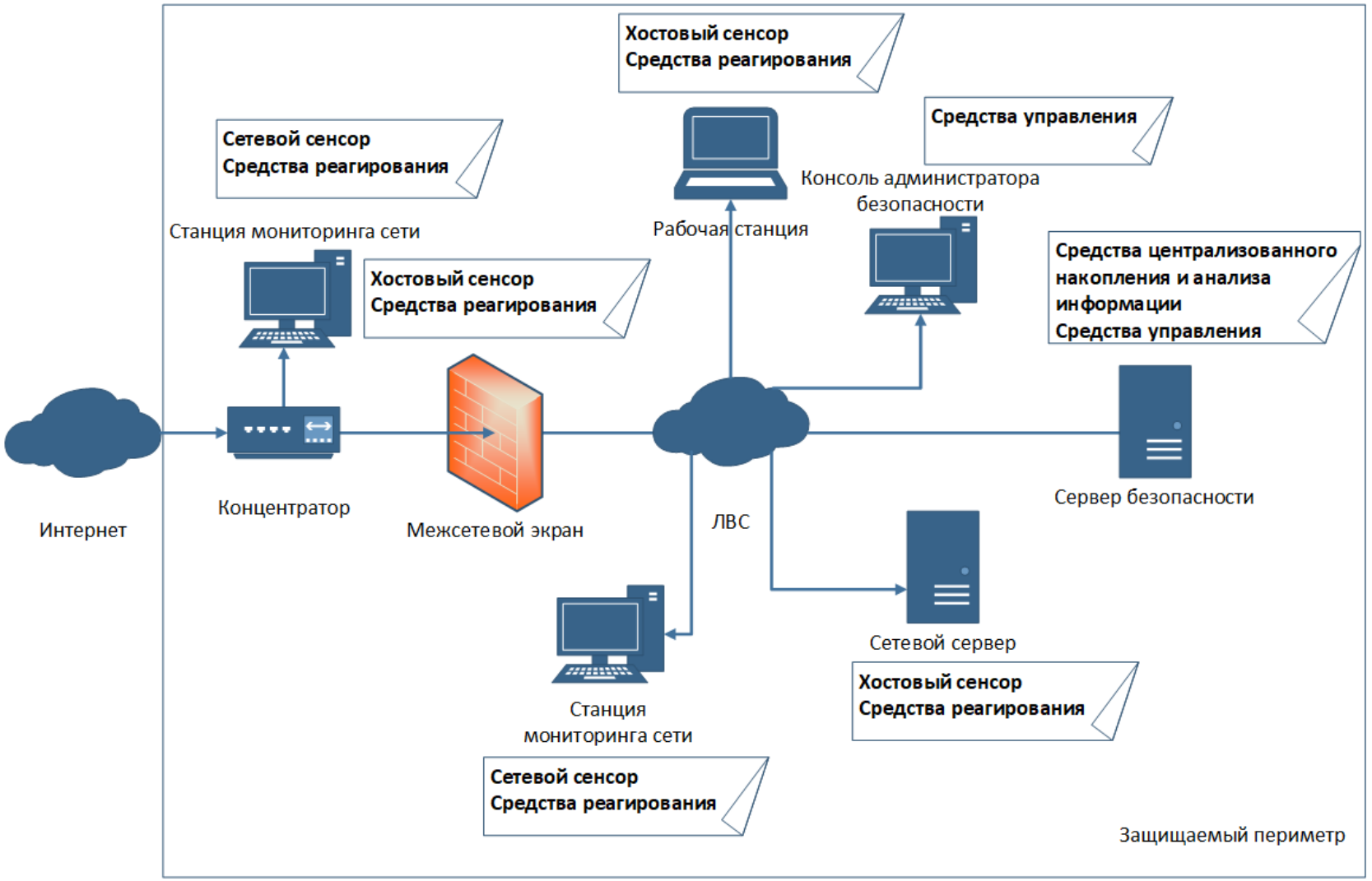


Рисунок 8.1. – Типовая архитектура системы обнаружения атак и предотвращения вторжений

В зависимости от источника обрабатываемой информации сенсоры бывают сетевыми и хостовыми. Сетевые сенсоры перехватывают трафик, передаваемый по локальной сети, выполняют анализ перехваченных данных, по результатам которого формируют события информационной безопасности. Сетевые сенсоры могут распределяться по сегментам локальных сетей, в которых развернута информационная система.

Хостовые сенсоры в качестве источников информации используют журналы событий хоста, которые регистрируют операционная система, межсетевой экран, СУБД, прикладные и специальные приложения. Хостовые сенсоры могут выполнять анализ сетевых пакетов, получаемых данных хостом.

Анализатор – средство централизованного сбора и анализа информации, полученной от сенсоров. Для анализа и хранения события безопасности преобразуются в единый вид. Преобразование, сбор и хранение событий безопасности в едином виде могут осуществляться специализированными решениями – SIEM-системами (англ. Security information and event management). SIEM-системы осуществляют управление информационной безопасностью (англ. SIM – Security information management) и управление событиями информационной безопасности (англ. SEM – Security event management).

Развертывается анализатор на серверах безопасности и может состоять из следующих составных частей: сервер сбора событий, сервер хранения, сервер корреляции, сервер аналитики. Сервер сбора информации обеспечивает централизованный сбор, нормализацию, категоризацию событий из записей журналов регистрации от различных сенсоров. Сервер хранения – нормализацию и хранение событий в локальной базе данных, осуществляет сквозной поиск и мониторинг событий безопасности. Сервер корреляции выполняет основные функции по анализу и корреляции событий безопасности на наличие подозрительных и неестественных закономерностей. Сервер аналитики предоставляет набор аналитических инструментов по обработке событий безопасности для выявления подозрительных и неестественных закономерностей, обеспечивает интерактивное графическое представление аналитических данных.

Средство реагирования размещается на станциях мониторинга сети, межсетевых экранах, серверах и рабочих станциях сети. Средство реагирования оповещает администратора безопасности (по электронной почте, SMS-сообщением на консоль администратора), блокирует сетевые подключения и пользовательские учетные записи для немедленного прекращения атак, а также протоколирует действия атакующей стороны.

Средство управления – графическая консоль администратора, которая позволяет управлять всеми компонентами системы обнаружения атак

и вторжений. Используется для настройки политик безопасности, правил обнаружения, а также для просмотра событий безопасности, проведения периодического аудита, генерации отчетов.

Защищаемый периметр – логические и физические границы защищаемой информационной системы, в пределах которых разворачивается система обнаружения атак и предотвращения вторжений. Размещать отдельные элементы СОА/СПВ опасно вне пределов защищаемого периметра, т.к. злоумышленник может их скомпрометировать, получить информацию о структуре внутренней защищаемой сети, базе правил СОА/СПВ. При необходимости вынесения элементов СОА/СПВ за пределы защищаемого периметра используют выделенные каналы связи или средства криптографической защиты.

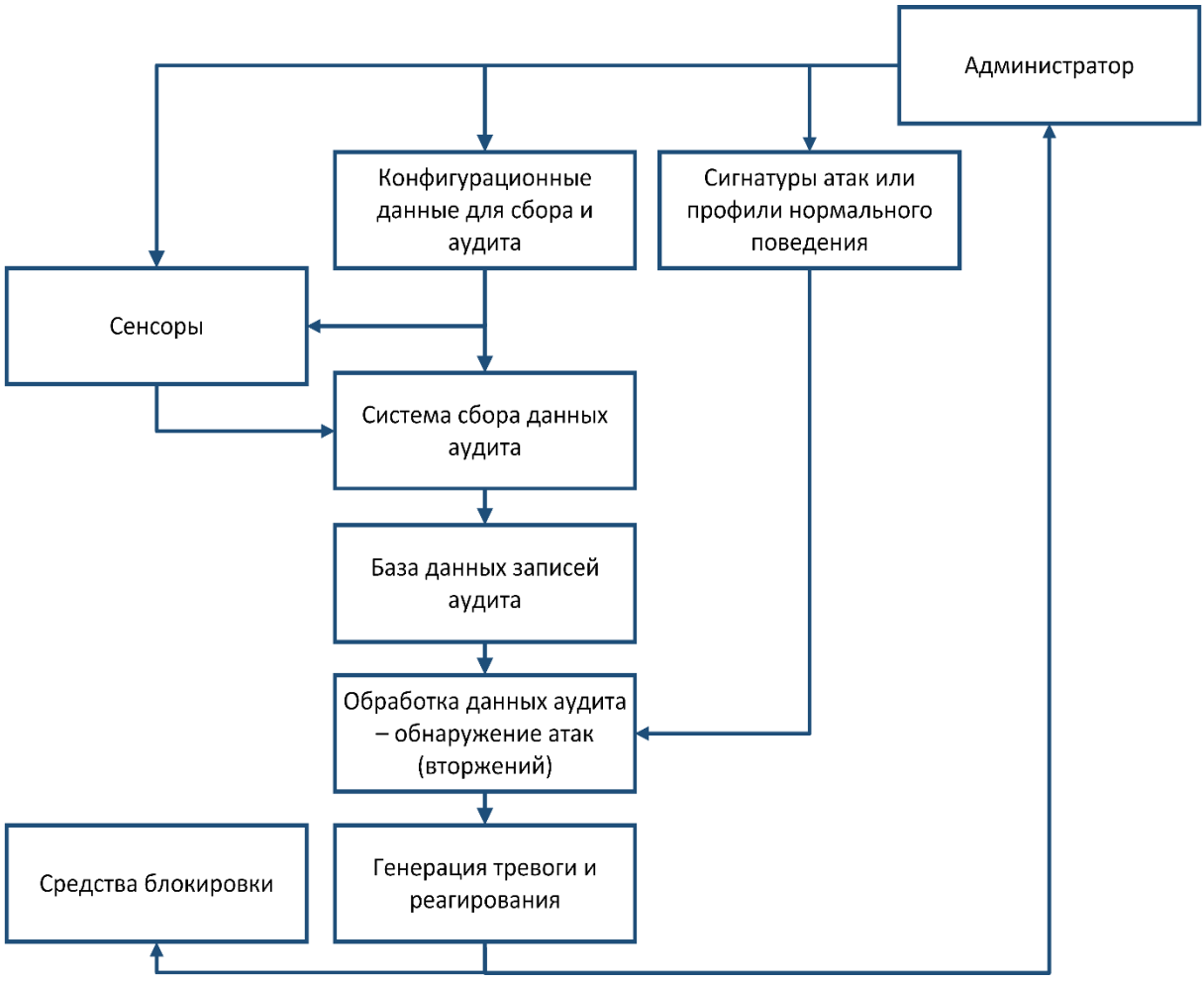


Рисунок 8.2. – Схема функционирования системы обнаружения атак и предотвращения вторжений

Схема проведения анализа данных аудита СОА/СПВ показывает последовательность операций по выявлению атаки или аномалии [72] (см. рисунок 8.2).

Администратор безопасности определяет, какие события необходимо относить к событиям безопасности, чтобы они участвовали в обнаружении атак (вторжений). Определение таких событий является сложной экспертной задачей, т.к. от этого зависят пропуски или ложное обнаружение атаки (вторжения).

Кроме типов событий администратор безопасности определяет периоды хранения журналов, т.е. глубину анализа и занимаемое дисковое пространство базы данных.

8.2. Классификация систем обнаружения атак и предотвращения вторжений

Системы обнаружения атак классифицируют по типичным функциям, особенностям проектирования, реализации (рисунок 8.3).

К числу классификационных признаков относят следующие:

- методология обнаружения;
- типы сенсоров;
- принцип развертывания;
- источник событий;
- время анализа;
- характер реакции.

По методологии обнаружения. Выделяют три основных подхода – обнаружение известных сигнатур, обнаружение аномального поведения (подозрительных и неестественных закономерностей) и гибридный подход, объединяющий обнаружение сигнатур и аномального поведения.

По сенсорам. Сенсоры являются неотъемлемой частью системы обнаружения атак. В зависимости от используемых сенсоров СОА делят на хостовые, сетевые и гибридные. Системы обнаружения вторжений, как правило, используют только хостовые сенсоры, а системы обнаружения атак могут включать и сетевые, и хостовые сенсоры. СОА, использующие и сетевые, и хостовые сенсоры одновременно, называют гибридными.

По принципу развертывания. В зависимости от принципа развертывания СОА делят на локализованные и распределенные. Все компоненты локализованных СОА функционируют в рамках одной сети, одного сервера или одного устройства. Локализованные СОА имеют более простую настройку и имеют более узкую специализацию.

Рисунок 8.3. – Классификация систем обнаружения атак и предотвращения вторжений

Для распределенных СОА каждый компонент может быть развернут на отдельном устройстве, каждое из которых может находиться в удаленном сегменте сети. Распределенные СОА более сложны в настройке и более дороги в обслуживании, но обладают большим масштабированием, охватывают большее количество угроз, способны выдерживать высокую нагрузку.

По источнику данных. Основными источниками событий безопасности, которые участвуют в обнаружении аномальной активности, являются сетевые пакеты, журналы событий, объекты информационной системы. Под журналами событий понимаются не только собственно журналы СОА/СПВ, но и системные журналы, которые ведутся операционной системой, СУБД, приложениями. Под объектами информационной системы понимают отдельное аппаратное устройство, прикладное программное обеспечение, в которое интегрирован сенсор. Сгенерированное событие объектом информационной системы передается непосредственно в анализатор, минуя системный журнал.

По времени анализа. Обнаружение атак и вторжений может выполняться в режиме реального времени или в отложенном режиме. В отложенном режиме события безопасности анализируются через некоторый интервал времени по мере разгрузки вычислительных мощностей системы обнаружения. Эффективность систем с реальным временем ограничивается предельной вычислительной сложностью алгоритмов обнаружения и пропускной способностью. Эффективность систем с отложенным анализом снижается из-за временной задержки для реагирования на атаку (вторжение).

По характеру реакции. Реакция СОА/СПВ делится на пассивные и активные. Под пассивными реакциями понимается генерация сигнала тревоги, например, отсылка сообщений специалисту по безопасности в панель управления, по электронной почте, SMS-оповещением, телефонным звонком. Под активными реакциями понимается вызов определенных функций системы защиты информации, которые способствуют предотвращению или минимизации атаки, например, блокирование учетных записей пользователей, блокирование сетевого трафика, изменение конфигураций или режимов работы устройств, программного обеспечения.

8.3. Вспомогательные средства обнаружения атак и вторжений

Вспомогательными средствами обнаружения атак и вторжений, которые не относятся к СОА/СПВ, но позволяют выявлять факт атак или вторжения, являются [72; 22]: средства контроля целостности; виртуальные ловушки; обманные системы.

Средства контроля целостности позволяют отслеживать внесение изменений в передаваемые данные или файлы, хранящиеся на хосте. Контроль внесения изменений осуществляется в три этапа.

На первом этапе выполнятся установка программного агента, который вычисляет свертки (хеши) для всех отслеживаемых файлов или данных. Вычисленные свертки сохраняются в специальную базу данных. Сохраненные свертки и соответствующие им файлы принимаются за действительные.

На втором этапе осуществляется периодический пересчет всех сверток и сравнение их с сохраненными ранее действительными значениями. Если обнаруживается расхождение в вычисленных свертках, то соответствующий этой свертке файл признается недействительным.

По недействительным файлам осуществляется реагирование на третьем этапе. В качестве реагирования могут отправляться уведомления (тревога) администратору безопасности и/или автоматическое блокирование доступа (исполнение) файла.

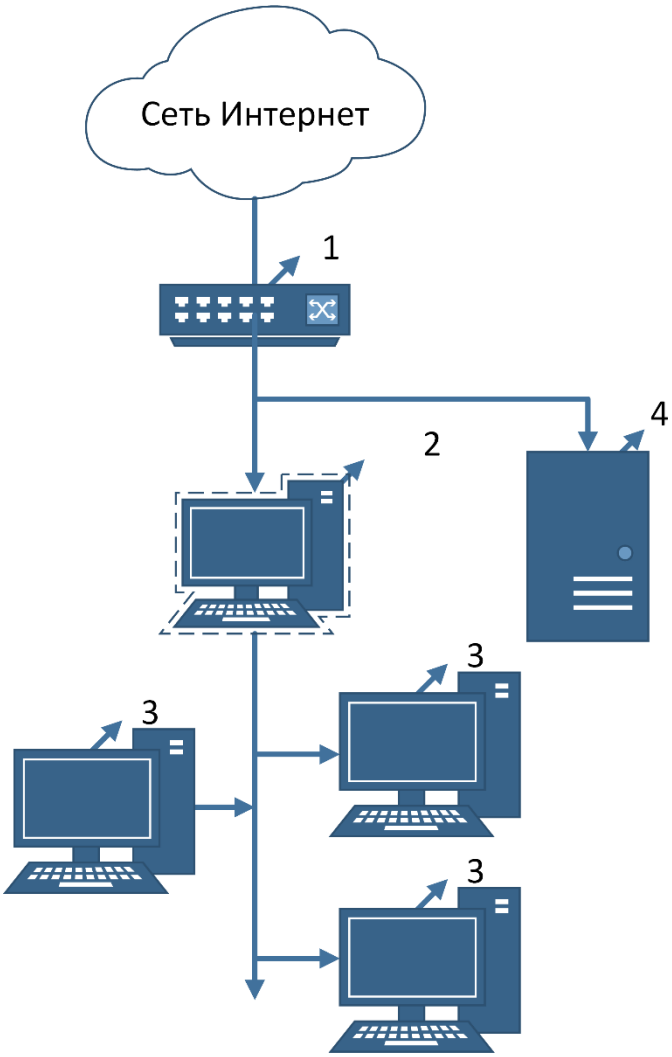
Виртуальная ловушка (англ. honeypot – горшочек с медом) – специально подготовленный хост (приманка), предназначенный для того, чтобы его взломали злоумышленники.

В процессе взлома виртуальная ловушка регистрирует и контролирует все действия злоумышленника на уровне сети и составляющих систем: системные журналы средств защиты, сетевые данные, записи аудита. Под составляющими системами защиты понимаются межсетевые экраны, парольные системы, антивирусные программы, системы обнаружения атак и вторжений и другие системы. Сбор данных должен выполняться скрытно, чтобы злоумышленник не мог обнаружить, что его действия фиксируются. Для зафиксированных данных должна обеспечиваться защита от изменений или уничтожений. Ведение штатного аудита выполняется в обычном режиме.

По результатам анализа собранной информации делается вывод о средствах, используемых злоумышленником, и методах борьбы с ними.

Обычно виртуальная ловушка представляет собой отдельный компьютер или прикладной сервер, размещенный в локальной сети (рисунок 8.4).

Локальная сеть подключена к внешней сети, через которую злоумышленники будут пытаться получить доступ. Примерами готовых решений, которые позволяют создавать собственные виртуальные ловушки, являются: Deception Toolkit, Cybercop Sting, Resource Mantrap, Honeypot.



1 – маршрутизатор; 2 – виртуальная ловушка; 3 – прикладной сервер; 4 – сервер регистрации

Рисунок 8.4. – Размещение виртуальной ловушки в локальной сети

Обманная система – специально подготовленная информационная система, предназначенная для атаки злоумышленника. В отличие от виртуальной ловушки обманная система состоит не только из одного хоста, а включает в себя набор прикладных серверов, рабочих станций, локальных сетей и средств их защиты.

Обманная система разворачивается параллельно основной информационной системе в специальном отведенном месте защищаемой локальной сети. Трафик атакующего направляется в обманную систему при обнаружении атаки с помощью СОА. В обманной системе собираются все действия злоумышленника аналогично виртуальным ловушкам, только в масштабе не одного хоста, а целой информационной системы.

8.4. Сетевые сканеры безопасности и генераторы трафика для обнаружения уязвимостей

Сетевые сканеры безопасности – программные или программно-аппаратные средства, которые выполняют проверку хостов на наличие уязвимостей. При выполнении сканирования составляется карта сетевых узлов в локальной сети, определяются открытые порты, установленные операционные системы и используемые приложения. В зависимости от используемых приложений выполняется проверка на наличие всех актуальных уязвимостей.

Обнаруженные уязвимости могут быть вызваны отсутствием средств защиты, ошибками конфигурации программного обеспечения и средств защиты, наличием ошибок в исходном коде программного обеспечения, «черных ходов», человеческого фактора и пр. При обнаружении уязвимостей могут использоваться два основных механизма: сканирование и зондирование [22; 72].

Сканирование – пассивный анализ полученных ответов по косвенным признакам без подтверждения факта наличия уязвимости. Сканирование является наиболее быстрым и простым механизмом поиска уязвимостей.

Зондирование – механизм активного анализа, который пытается производить сетевую атаку на хост для фактического подтверждения наличия уязвимости. Механизм зондирования работает медленнее механизма сканирования и может вызывать сбои в работе проверяемого узла, но при этом является более точным.

Одной из разновидностей сетевых сканеров безопасности, использующих механизм зондирования, являются генераторы сетевого трафика. Генераторы трафика выполняют нагрузочное тестирования сетевых устройств и подтверждение наличия уязвимостей на уровне приложений. С помощью генераторов трафика может проверяться подверженность атакам типа «отказ в обслуживании» (Denial Of Service, DoS).

По результатам сканирования составляется отчет о найденных уязвимостях и выдаются рекомендации по их устранению.

В настоящее время существует большое количество сканеров: коммерческие (например: XSpider 7.8, FortiScan, VBA32.CS, Rapid7, MaxPatrol и др.); свободно распространяемые (например, Nmap, w3af, N-Stealth Security Scanner и др.); универсальные и специализированные на определенном классе уязвимостей.

Вопросы для самопроверки

1. Какие основные компоненты системы обнаружения атак и вторжений вы знаете?
2. По какому алгоритму выполняется анализ данных аудита?
3. По каким функциям делят системы обнаружения атак и вторжений?
4. В чем принципиальная разница работы системы обнаружения атак и вторжений при обнаружении сигнатур и аномалий?
5. Какие основные преимущества децентрализованных систем обнаружения атак и вторжений вы знаете?
6. Какие источники сбора данных для анализа вы знаете?
7. В каких случаях целесообразно применять системы обнаружения атак и вторжений с анализом в режиме реального времени?
8. Какие дополнительные средства обнаружения атак и вторжений вы знаете?
9. Какие правила использования виртуальных ловушек вы знаете?
10. Какие механизмы обнаружения уязвимости сети вы знаете?
11. Чем отличается сканирование от зондирования?

9. ВИРТУАЛЬНЫЕ ЗАЩИЩЕННЫЕ СЕТИ

Виртуальная защищенная сеть (с англ. Virtual Private Networks, VPN) – технология объединения локальных сетей и отдельных хостов поверх сетей общего пользования.

Иными словами, если в сети общего пользования есть два хоста, между которыми происходит обмен информацией, конфиденциальность и целостность которой необходимо защитить, то между ними создается виртуальный туннель (соединение). Такой туннель называют виртуальным т.к. соединение между хостами является не жестким (постоянным), а логическим, и существует только во время прохождения трафика [22]. Доступ к передаваемой информации в виртуальном туннеле максимально затруднен как для активных, так и для пассивных внешних наблюдателей.

В зависимости от применяемых протоколов и назначения VPN может обеспечивать соединения трех видов: узел–узел, узел–сеть, сеть–сеть (рисунок 9.1).

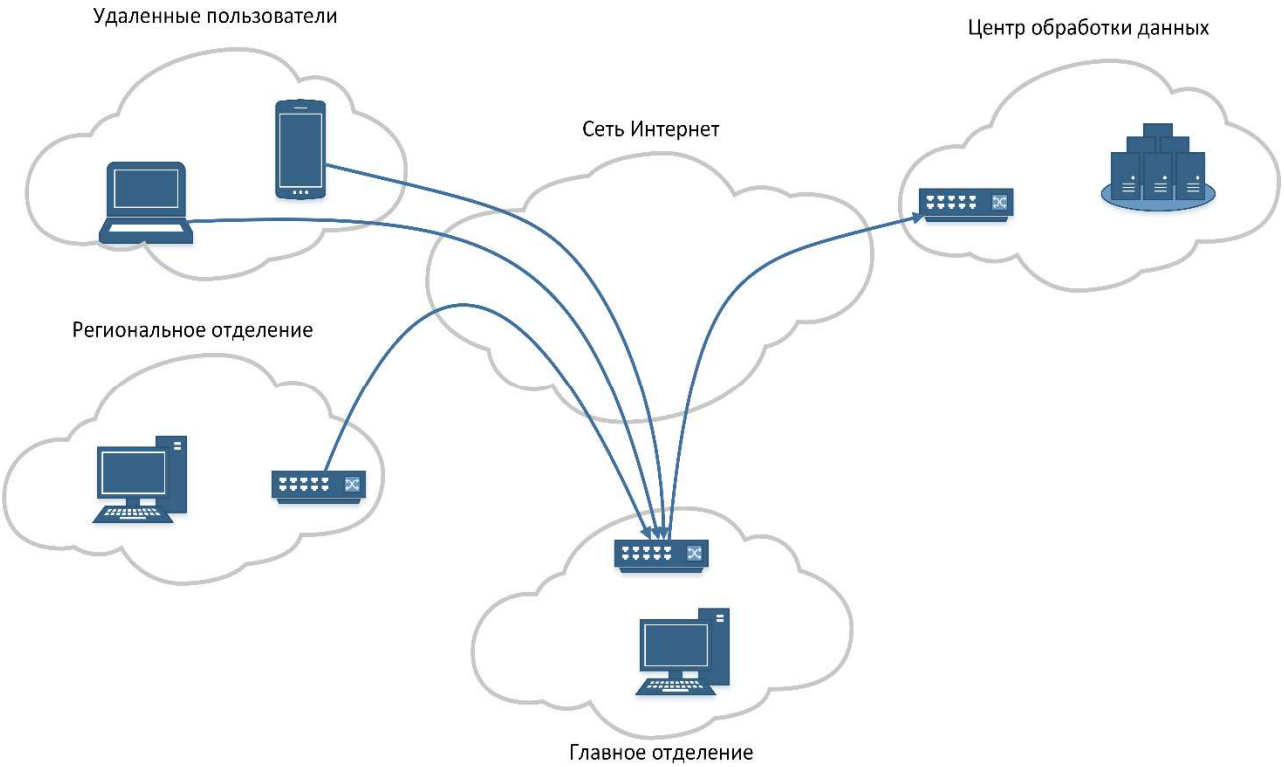


Рисунок 9.1. – Пример соединения узлов и сетей через VPN

Технология построения VPN предназначена для предотвращения несанкционированного доступа к конфиденциальным данным, передаваемым по открытым сетям, и несанкционированного доступа к внутренним ресурсам локальной сети в результате несанкционированного входа в локальную сеть [22].

9.1. Функции и компоненты виртуальных защищенных сетей

Технология построения VPN выполняет в сфере защиты информации множество функций, основные из которых:

- идентификация и аутентификации взаимодействующих сторон;
- шифрование передаваемых данных;
- проверка целостности переданных данных.

Эти функции реализуются посредством криптографических методов защиты информации и взаимосвязаны. Внедряются криптографические методы в виртуальном туннеле, который обеспечивает логическое соединение двух конечных узлов сети.

Создается туннель с помощью механизма инкапсуляции протоколов: пакеты транспортируемого протокола помещаются в поле данных пакетов несущего протокола. Преобразование пакетов транспортируемого протокола выполняется с помощью протокола инкапсуляции (встраивания).

На рисунке 9.2 представлен пример схемы построения VPN между двумя локальными сетями. На схеме изображены две локальные сети (10.10.1.0/24 и 10.20.1.0/24), инициатор туннеля, терминатор туннеля, виртуальный туннель и маршрутизируемая сеть.

Трафик транспортируемого протокола из локальной сети 10.10.1.0/24 поступает на интерфейс 10.10.1.1/24 инициатора туннеля. Инициатор туннеля выполняет инкапсуляцию поступивших пакетов в пакеты несущего протокола и перебрасывает их на другой свой интерфейс 178.100.1.1/24. Интерфейс 178.100.1.1/24 инициатора туннеля подключен к сети общего пользования, через которую несущий (маршрутизируемый) протокол передается на интерфейс терминатора туннеля 178.200.1.1/24.

Терминатор туннеля выполняет обратную инкапсуляцию данных из несущего протокола в транспортируемый протокол. Извлеченный транспортируемый протокол передается на интерфейс 10.20.1.1/24, а затем поступает к адресату в локальной сети.

Передаваемые пакеты между инициатором и терминатором являются пакетами IP-протокола, а инкапсулируемые пакеты могут принадлежать к любым протоколам, в т.ч. немаршрутизируемым.

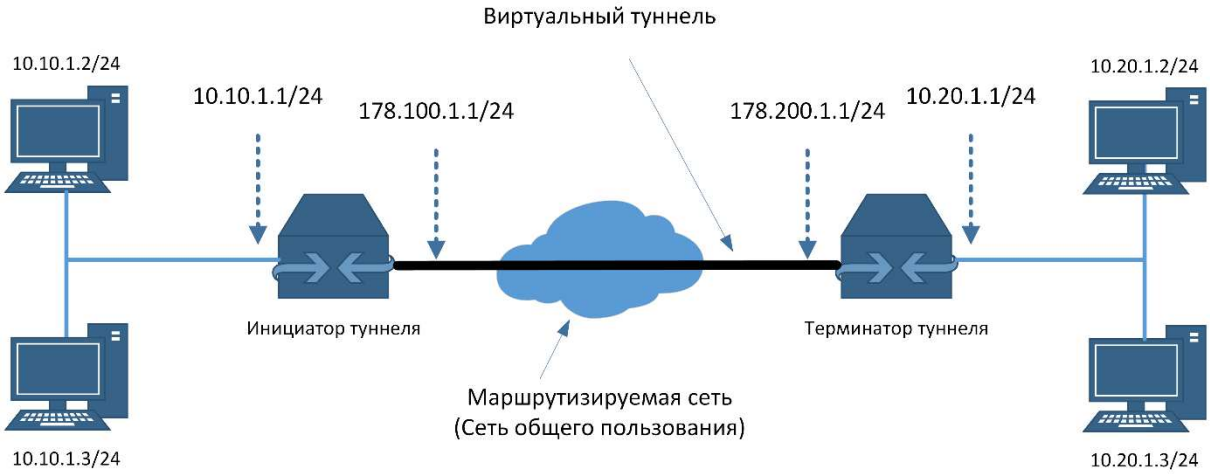


Рисунок 9.2. – Схема построения VPN между двумя подсетями

В результате между локальными сетями образуется виртуальный туннель. Сам по себе виртуальный туннель не обеспечивает защищенность передаваемых данных, однако процедура инкапсуляции позволяет встраивать в преобразование пакетов криптографические методы защиты информации. Внедрение в инкапсуляцию шифрования данных обеспечивает конфиденциальность информации, а цифровой подписи – целостность и подлинность передаваемых данных. Применение процедуры аутентификации между взаимодействующими сторонами обеспечивает проверку подлинности подключения.

Для обеспечения согласованного обмена данными между инициатором и терминатором туннеля выполняется настройка допустимых протоколов аутентификации, шифрования, подсчета цифровой подписи.

Основными недостатками VPN называют следующие:

– VPN увеличивает нагрузки на вычислительные ресурсы, т.к. во-первых, для преобразование данных и их шифрования требуется выполнение большего числа вычислительных операций; во-вторых, увеличивается объем передаваемых данных;

– VPN ограничивает возможность анализа передаваемого трафика вследствие его шифрования, из-за чего снижается эффективность функционирования СОА/СВП;

– VPN является единственной точкой подключения к сети, в связи с чем повреждение канала связи с провайдером или атака на шлюз VPN, направленная на отказ в обслуживании, лишают возможности выполнить подключение к защищаемой сети;

– при использовании VPN передаваемые данные защищены, однако IP-адрес, к которому выполняется подключение, является видимым (доступным), что хотя и не угрожает конфиденциальности напрямую, но позволяет однозначно идентифицировать сеть при подключении;

– подключение через VPN не гарантирует полную конфиденциальность пользователя при работе с сетевыми ресурсами; так, например, по файлам cookie сайты могут распознавать пользователя независимо от его подключения.

9.2. Защита данных на различных уровнях модели OSI

Модель OSI описывает этапы преобразования данных при их передаче по вычислительной сети. Модель содержит семь уровней. При передаче данные в отправителе информации преобразуются от седьмого уровня к первому, а в приемнике – от первого к седьмому (рисунок 9.3).

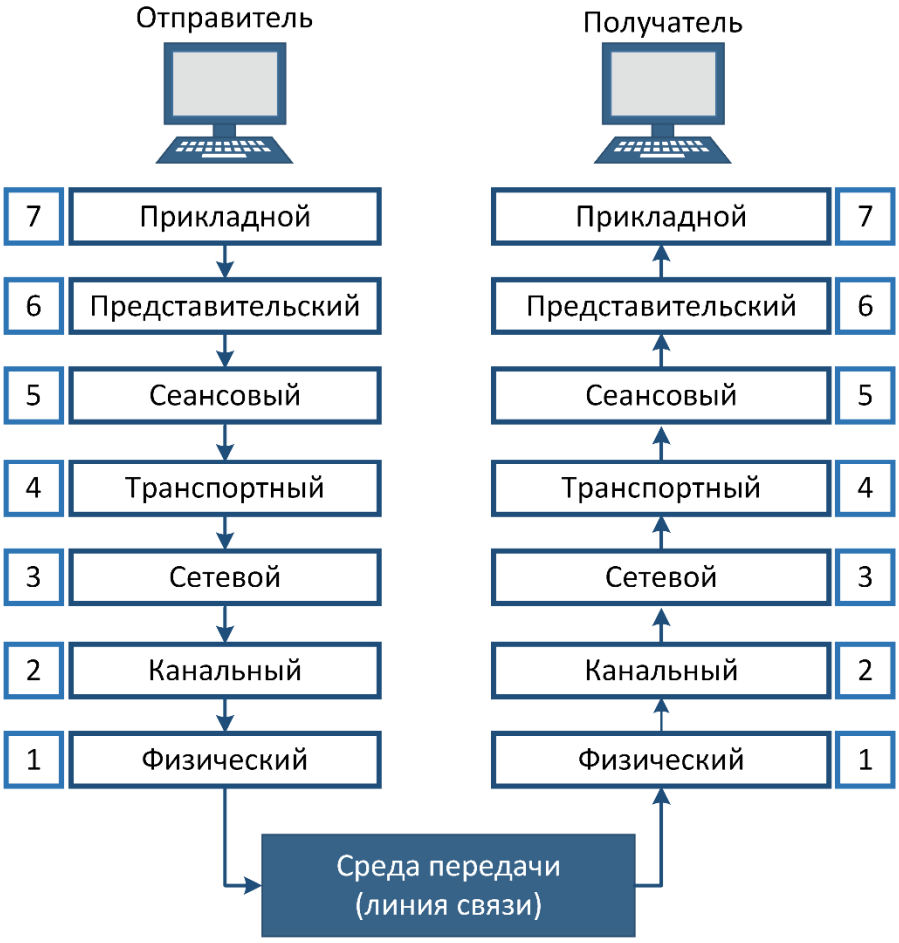


Рисунок 9.3. – Процесс преобразования данных в модели ISO

Согласно модели OSI за процесс преобразования данных на верхних трех уровнях отвечают прикладные приложения, на четвертом уровне выполняется смешанное преобразование и приложениями, и сетевыми службами, сетевым оборудованием, а на первых трех уровнях – только сетевыми службами, сетевым оборудованием (рисунок 9.4).

Рисунок 9.4. – Преобразование данных на уровнях модели OSI

Построение защищенного туннеля может выполняться на различных уровнях модели OSI. В зависимости от использованного уровня зависит совместимость защищенного туннеля с прикладными приложениями. Чем выше уровень модели OSI используется, тем сильнее зависимость VPN от разработчиков конкретного приложения, а чем ниже уровень модели OSI – тем больше прозрачность для приложений.

Если VPN использует протокол одного из верхних уровней, то такой способ защиты не зависит от того, какие сети (IP или IPX, Ethernet или ATM) применяются для транспортировки данных. С другой стороны, приложение при этом становится зависимым от конкретного протокола защиты, т.е. для приложений подобный протокол не является прозрачным и приложение должно быть доработано с учетом использования протокола защиты [22].

Вторым недостатком построения VPN на высоком уровне модели OSI является ограниченная область действия. В таком случае защита данных выполняется только для одной сетевой службы, например, FTP, HTTP, SMTP.

Выделяется [22] три группы VPN:

– VPN второго (канального) уровня;

– VPN третьего (сетевого) уровня;

– VPN пятого (сеансового) уровня.

VPN первой группы обеспечивают создание защищенных туннелей типа «точка–точка» (маршрутизатор – маршрутизатор, рабочая станция – маршрутизатор). Примерами являются L2F (Layer 2 Forwarding), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol).

VPN сетевого уровня обеспечивают инкапсуляцию протокола IP в протокол IP. Такие VPN позволяют поддерживать несколько отдельных защищенных туннелей между объединяемыми сетями. Примерами являются IPSec, SKIP.

VPN сеансового уровня обеспечивают передачу данных через определенный порт с помощью защиты транспортного уровня TLS. Примером является протокол SOCKS 5.

9.3. Типы организуемых сетей

Решения для построения VPN выбираются в зависимости от типа организуемой сети. Выделяют три принципиально различных типа сетей: удаленный доступ, интрасеть, экстрасеть.

Виртуальные частные сети с поддержкой удаленного доступа позволяют сотрудникам компании подключаться к сети компании, например, во время удаленной работы, во время командировки или даже с помощью мобильного телефона во время выхода из офиса или дома. Сети с поддержкой удаленного доступа характеризуются следующими особенностями:

– низкая стоимость организации подключения. Зачастую используются бесплатные программные средства свободного распространения;

– настройка выполняется достаточно просто, как правило, пользователь с минимальной квалификацией способен установить и настроить подключение к сети. Данные для настройки подключения предоставляются сетевым администратором для каждого пользователя;

– высокая масштабируемость, которая позволяет обеспечивать подключения пользователей с различных типов устройств и операционных систем;

– при подключении обязательно используется аутентификация пользователя для контроля подключения к сети;

– минимальная, но достаточная конфиденциальность данных, обеспечиваемая оптимальным по производительности шифрованием;

– надежность подключения не всегда гарантируется, т.к. пользователи могут подключаться через сети общего пользования.

Виртуальные частные сети для построения интрасети (внутрикорпоративной сети) позволяют организовать единую локальную сеть между подразделениями (филиалами) одной компании. Для интрасети характерно следующее:

– высокая надежность и пропускная способность, которые обеспечиваются выделенными средствами. К выделенным средствам могут относится выделенные линии, выделенное специализированное оборудование и программное обеспечение. В зависимости от критичности доступности ресурсов возможно выделение резервных (дублирующих) средств;

– допускается использование публичных сетей для организации подключения;

– конфиденциальность данных обеспечивается мощным шифрованием;

– аутентификация пользователей и контроль доступа из одной сети в другую осуществляются не всегда.

Применение VPN для построения экстрасети (межкорпоративной сети) позволяет объединить локальные сети разных компаний. Объединение сетей необходимо для защищенного обмена информацией, например, между стратегическими партнерами, провайдерами услуг, поставщиками и т.п. Экстрасети имеют свои особенности:

– обеспечивается гарантированный уровень надежности и пропускной способности. Аналогично с интрасетями могут применяться выделенные и дублированные линии связи, специализированное оборудование и программное обеспечение;

– аутентификация пользователей является обязательным требованием;

– доступ предоставляется только к определенным ресурсам. Может функционировать система защиты от несанкционированного доступа;

– применяются межсетевые экраны;

– наличие регламентов и правил доступа, которые фиксируются документально;

– высокая стоимость и сложность реализации.

9.4. Способы технической реализации VPN

В настоящее время существует бесчисленное множество решений, которые позволяют организовать VPN. Каждое решение по-своему является уникальным. Однако существуют некоторые основные подходы (способы реализации), которые позволяют группировать технические реализации VPN.

Первый способ – с помощью сетевых операционных систем, которые ориентированы на работу с локальной сетью: обеспечивают маршрутизацию трафика, создание виртуального туннеля, шифрование данных, управление пользователями по сети, авторизацию пользователей в сети, организацию доступа к общим удаленным ресурсам сети, управление политиками безопасности, правилами межсетевого экранирования и др.

Большинство современных операционных систем поддерживают основные функции сетевых операционных систем, однако существуют специализированные операционные системы, которые адаптированы к решению определенных сетевых задач. Например, бесплатная операционная система VyOS на основе Debian позволяет использовать виртуальную машину или компьютер как выделенный маршрутизатор, который содержит встроенный межсетевой экран, системы обнаружения вторжений и резервирования канала, балансировщик нагрузки, и таким образом создавать криптотуннели по протоколам IPsec, L2TP/IPsec, PPTP, OpenVPN.

Второй способ построения VPN предполагает использование выделенных аппаратных маршрутизаторов, которые установлены на узловых подключениях в локальную сеть.

Третий способ – VPN на основе межсетевых экранов, который применяется только для небольших сетей с ограниченным объемом передаваемой информации и является достаточно дорогостоящим. При таком способе к стандартному программному обеспечению межсетевого экрана, которое выполняет функции туннелирования и шифрования, добавляется специализированный модуль шифрования, адаптированный под определенный национальный стандарт.

Четвертый способ предполагает использование прикладного программного обеспечения, которое разворачивается на стороне сервера и на стороне клиента. Клиент и сервер VPN создают в операционной системе виртуальные адаптеры. Для трафика, поступающего на виртуальные адаптеры, выполняется инкапсуляция и шифрование с помощью специального модуля VPN, после чего шифрованный трафик передается по реальной

вычислительной сети. Для повышения уровня защищенности программное обеспеченея может размещаться за межсетевым экраном. Данный способ является одним из самых бюджетных. Популярный пример программных VPN – OpenVPN, который бесплатно устанавливается на большинство современных операционных систем (включая мобильные телефоны).

Пятый способ – применение специализированных аппаратных средств, которые содержат встроенные шифропроцессоры для увеличения производительности. Данный способ, в отличие от других, позволяет выдерживать более высокие нагрузки на вычислительную сеть, но обладает и более высокой стоимостью. Также существуют и домашние бюджетные маршрутизаторы, которые могут выполнять функции по созданию криптотуннеля.

В качестве шестого способа можно назвать комбинирование различных решений для оптимизации затрат. Так, например, клиентом к специализированному аппаратному шлюзу со встроенным шифропроцессором может поставляться программный клиент либо программный клиент с токеном для хранения ключа шифрования. Реализацией такого решения является «Bel Vpn».

9.5. Технические и экономические преимущества

Технология построения виртуальных частных сетей является эффективным средством:

– для прокладывания маршрутов между удаленными пользователями или сетями;

– для разделения (маркировки) передачи данных в сетях общего пользования, чтобы данные не смешивались;

– для обеспечения конфиденциальности и целостности передаваемых данных.

Свою высокую эффективность VPN обеспечивает за счет низкой стоимости программных или аппаратных-программных средств, их доступности для массового пользователя сети Интернет и надежности функционирования.

Доступность средств построения VPN демонстрируется наличием бесчисленного множества программных решений для серверов, персональных компьютеров и мобильных устройств под различные операционные системы. Также наличие VPN с поддержкой аппаратного ускорения даже в домашних бюджетных роутерах подчеркивает актуальность и массовую востребованность VPN.

Возможность подключения через VPN к корпоративным сетям через личные устройства сотрудников позволяет переходить на удаленную работу без особых материальных затрат. Особенно востребованность в организации удаленного рабочего места доказывает актуальность VPN в период выхода компании на международный уровень и во время пандемий.

Вопросы для самопроверки

1. Какие основные операции выполняет VPN?
2. В чем заключается основной принцип туннелирования?
3. Каким образом обеспечивается конфиденциальность передаваемых данных через VPN?
4. Какие основные преимущества и недостатки у VPN, работающих на более высоких уровнях модели OSI?
5. Назовите примеры VPN канального уровня.
6. Назовите примеры VPN сетевого уровня.
7. Назовите примеры VPN сеансового уровня.
8. Какие способы реализации VPN вы знаете?
9. В чем заключается основные технические и экономические преимущества применения VPN?

10. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ ПРИМЕНЕНИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В СЕТИ ИНТЕРНЕТ

10.1. Понятие социальной инженерии

В контексте информационной безопасности термин «социальная инженерия»[21] используется для обозначения мошеннических техник психологической манипуляции людьми в целях понуждения к совершению определенных действий и (или) получения конфиденциальной информации.

Самым слабым звеном в системе обеспечения безопасности по-прежнему являются не технологии, а живые люди. Киберпреступник в подавляющем большинстве случаев не станет тратить время на осуществление технологически сложных приемов взлома, если необходимые сведения можно получить, используя навыки в области социальной инженерии [74].

Атаки с использованием человеческого фактора не требуют значительных финансовых затрат, а также глубоких знаний в области компьютерных технологий, однако являются достаточно универсальными для проникновения в любые системы, в течение короткого времени могут иметь очень широкий охват объектов воздействия и, кроме того, достаточно сложно отслеживаются.

Приемы и техники социальной инженерии основаны на психологии масс (науке о поведении людей в группах), трансактном анализе, психологии влияния, психологии эмоций, профилировании (составлении психологического портрета человека), нейролингвистическом программировании.

Базовая схема воздействия в социальной инженерии достаточно проста и типична (к слову, в общем виде она была сконструирована белорусским психологом В.П. Шеиновым):

1. Формирование цели воздействия на объект.
2. Сбор информации об объекте воздействия.
3. Обнаружение наиболее удобных мишеней воздействия.
4. Аттракция (создание нужных условий для воздействия на объект).
5. Понуждение к нужному действию.
6. Необходимый итог [75, с. 13].

---

[21] Существует и более широкое понятие социальной инженерии, используемое для обозначения области научно-практической деятельности в социологии, однако этот аспект в настоящем пособии не рассматривается. Нередко о социальной инженерии говорят еще и применительно к методам целенаправленного воздействия на человека (группу лиц) с целью изменения или удержания его поведения в нужном направлении, однако для таких случаев существует более корректный термин – социальное программирование [75, с. 22].

Общий принцип всех атак – введение жертвы в заблуждение. Для этого могут использоваться различные тактики, направленные на эмоции, слабости или иные особенности личности: неопытность, сочувствие (жалость), жадность, стремление к быстрому результату, страх, преклонение перед авторитетами, любовь, лень, любопытство.

Для того чтобы усилить эффект от применения методов социальной инженерии, злоумышленники могут собирать информацию о потенциальных жертвах из открытых источников (например, из социальных сетей). Как правило, пользователи не уделяют должного внимания безопасности, оставляя в свободном доступе информацию о локации (а значит, о передвижениях), номера телефонов, адреса, дату рождения, основные контакты и иные значимые данные, которые могут быть использованы социальными хакерами в своих целях.

Далее будут рассмотрены основные техники, используемые злоумышленниками для незаконного получения конфиденциальной информации посредством сети Интернет, а также некоторые механизмы защиты от их применения.

10.2. Техники социальной инженерии для выманивания конфиденциальных данных

Конфиденциальные данные (пароли и логины различных сервисов, данные банковских карт) могут быть получены злоумышенником путем применения достаточно простых техник социальной инженерии.

Самый древний способ получить конфиденциальную информацию – подсмотреть ее. На этом основана техника **плечевого серфинга** (англ. shoulder surfing) – чтения конфиденциальных данных (логинов, паролей, кодов к банковским картам) как бы «из-за плеча». Разумеется, злоумышленник не всегда буквально стоит за спиной пользователя. Существенно упростить задачу может применение технических средств (например, скрытой камеры, очков с камерой, простейшего бинокля). Необходимую информацию легко подсмотреть в магазине, кафе, общественном транспорте, в офисе открытого типа – всюду, где пользователь может вводить конфиденциальные данные не только на компьютере, но и на планшете или смартфоне, а злоумышленник имеет больше шансов не привлечь внимание жертвы. Не всегда целью правонарушителя, использующего технику плечевого серфинга, являются исключительно аутентификационные или платежные данные пользователя. Любая личная информация, вынесенная из мессенджера или

социальной сети, может в дальнейшем быть использована социальным инженером в своих целях.

Защититься от плечевого серфинга можно, исключив работу с конфиденциальными данными (в т.ч. личную переписку) в общественных местах, а также ограничив широкий обзор рабочего экрана компьютера.

Наиболее известной и распространенной техникой социальной инженерии является **фишинг**.

Термин «фишинг» (англ. phishing) – неологизм, образованный как омофон от англ. password harvesting fishing – рыбная ловля, выуживание паролей [74] и обозначающий тип компьютерного мошенничества, целью которого является получение конфиденциальной информации особого рода: учетных данных (логинов и паролей) различных сервисов, реквизитов банковских карт (номер, срок действия, имя и фамилия держателя, CVC2/CVV2-код) либо номеров телефонов. Конечная цель мошенников, использующих технику фишинга, – завладеть денежными средствами пользователя либо открыть счет (карт-счет) в банке для проведения транзитных операций (в Беларуси возможно при получении данных для входа в Межбанковскую систему идентификации – МСИ: https://www.raschet.by/o-sisteme/o-msi/). В некоторых случаях фишинг используется также для получения копий личных документов (паспорта, водительского удостоверения), которые затем могут быть проданы в сети Интернет и использованы для совершения преступлений (см., например, публикации о белорусских паспортах в DarkNet [76; 77]).

Фишинг является техникой **выманивания** конфиденциальных данных, пользуется особой популярностью в среде интернет-мошенников и стремительно набирает обороты в современном мире. Осуществляется, как правило, путем личной или массовой рассылки сообщений по электронной почте, в мессенджерах, социальных сетях, на торговых интернет-площадках и аукционах. Сообщения снабжаются ссылками на так называемые фишинговые страницы, внешне копирующие, иногда почти неразличимо, официальные сайты банков или популярных платежных систем, социальных сетей, иных сервисов и содержащие форму, требующую ввести конфиденциальные данные.

Иногда фишинговые ссылки скрываются за фальшивыми рекламными баннерами, QR-кодами на установку «полезных» приложений и т.п. Набирает обороты появившийся в 2019 г. календарный фишинг: атаки на пользователей сервиса Google Календарь, предполагающие рассылку автоматических уведомлений в календаре с фишинговой ссылкой во всплывающем окне на смартфоне [78].

Основная задача киберпреступника, который использует технику фишинга, состоит в том, чтобы мотивировать пользователя перейти по предложенной ссылке на сайт и ввести в предлагаемую форму конфиденциальные данные. При этом могут называться самые разнообразные причины: утеря или необходимость проверки (обновления) данных в связи со сбоем в системе; разблокирование счета; необходимость подтвердить платеж, получить денежный перевод, приз (выигрыш в лотерею), солидное наследство или налоговый вычет; требование уплатить штраф, погасить кредит, осуществить пожертвование; необходимость защитить средства от совершающегося хищения; предложение пройти опрос за вознаграждение. Актуальной для 2020 г. в фишинговых атаках во всем мире стала тематика COVID-19 [79], когда мошенники пытались продать в сети Интернет лекарства от коронавируса и средства индивидуальной защиты (маски, респираторы), выманить штраф за нарушение самоизоляции, убедить произвести пожертвование в фонды борьбы с коронавирусом и т.п. Если целью «фишера» является получение доступа к аккаунту социальных сетей или к электронной почте (может быть промежуточным этапом в осуществлении цепочки направленных фишинговых атак), то мошенник обычно взывает к любопытству пользователя (например, предлагает посмотреть интересную фотографию или видеоролик, прочесть крайне полезную статью, узнать по фото общего друга, перейти по ссылке на интерактивную карту, отображающую актуальную информацию о пандемии и т.п.). В некоторых случаях после введения идентификационных данных на фишинговом сайте пользователь перенаправляется на страницу с изображением бесконечного значка загрузки.

Простейшая фишинговая страница может быть создана за считанные минуты. В качестве примера рассмотрим страницу входа в социальную сеть ВКонтакте. Необходимо открыть главную страницу сайта и сочетанием клавиш Ctrl+S сохранить ее. В итоге получается почти готовый макет фишинговой страницы: рисунок 10.1 отображает официальную страницу социальной сети, а рисунок 10.2 – полученный простым сохранением шаблон (добавить к нему картинку не составит труда для любого программиста).

Дело за малым: зарегистрировать домен, привязать его к хостингу и разместить там подготовленную страницу. Страница будет доступна в сети Интернет для всех пользователей, с ее помощью можно приступить к «выуживанию» регистрационных данных для социальной сети ВКонтакте.

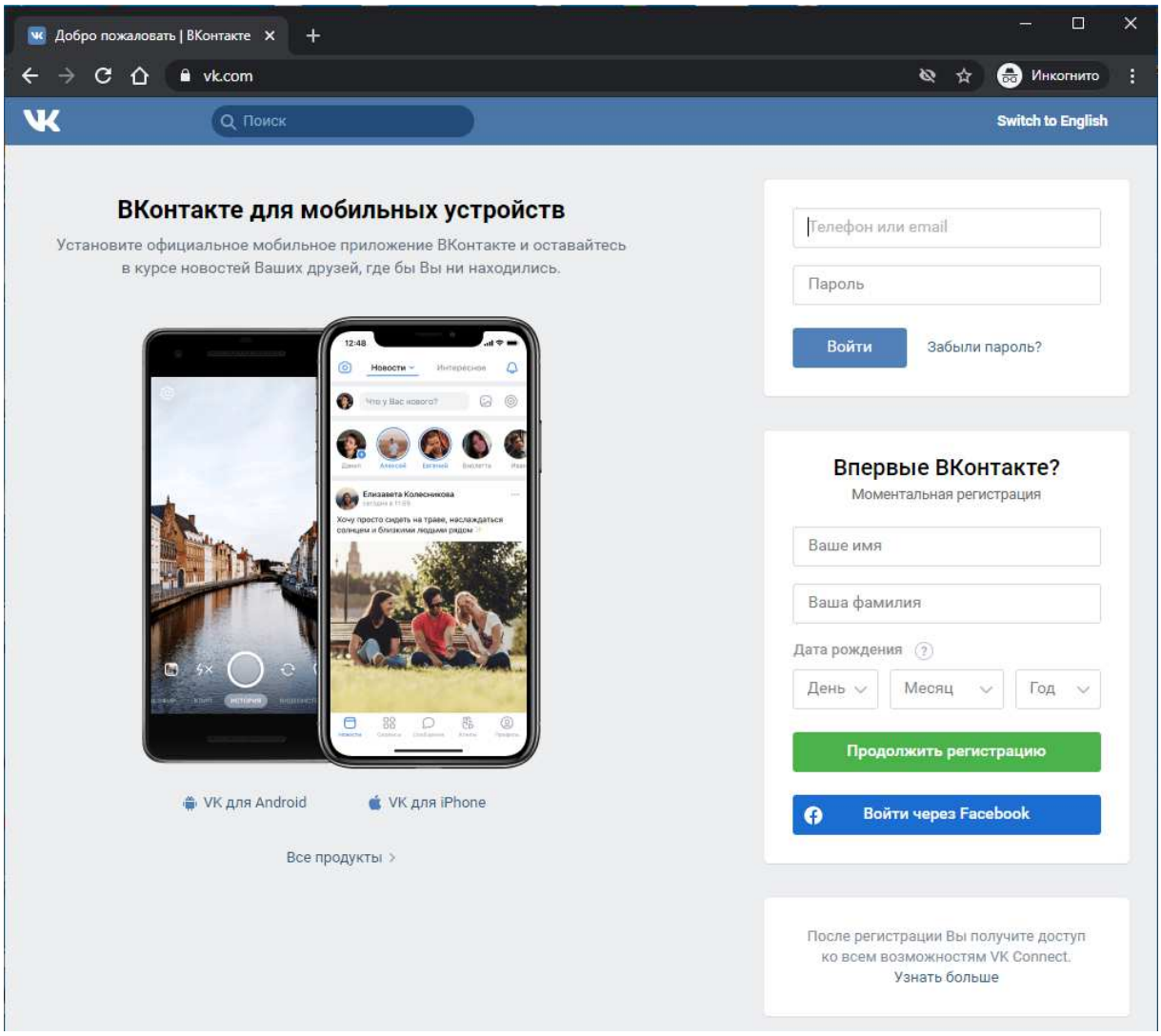


Рисунок 10.1. – Страница входа в социальную сеть ВКонтакте

В 2019 г. резко увеличился объем продаж так называемых «фишинг-китов» (от англ. Phishing Kit) – конструкторов в виде набора скриптов для массового создания фишинговых сайтов. Фишинговый набор позволяет киберпреступникам быстро возобновлять работу заблокированных вредоносных ресурсов, обеспечивая собственную неуязвимость [78].

Чтобы замаскировать доменные имена фишинговых сайтов, мошенники могут регистрировать домены с опечатками (например, www.belarysbank.by, www.belarsbank.by вместо www.belarusbank.by, www.facebouk.com вместо www.facebook.com), домены третьего и последующих уровней (например, www.prior.bank.by, www.pay.prior.bank.by вместо www.priorbank.by), аналогичные официальным домены в других доменных зонах (например, www.kufar.biz, www.kufar.com, www.kufar.be вместо www.kufar.by), а также домены, которые могут ассоциироваться

с официальными (например, www.mtb.by вместо www.mtbank.by, www.kufar-pay.by вместо www.kufar.by). Ссылка при этом может быть внешне абсолютно правильной и содержать указание на официальный домен, но перенаправлять на фишинговую интернет-страницу.

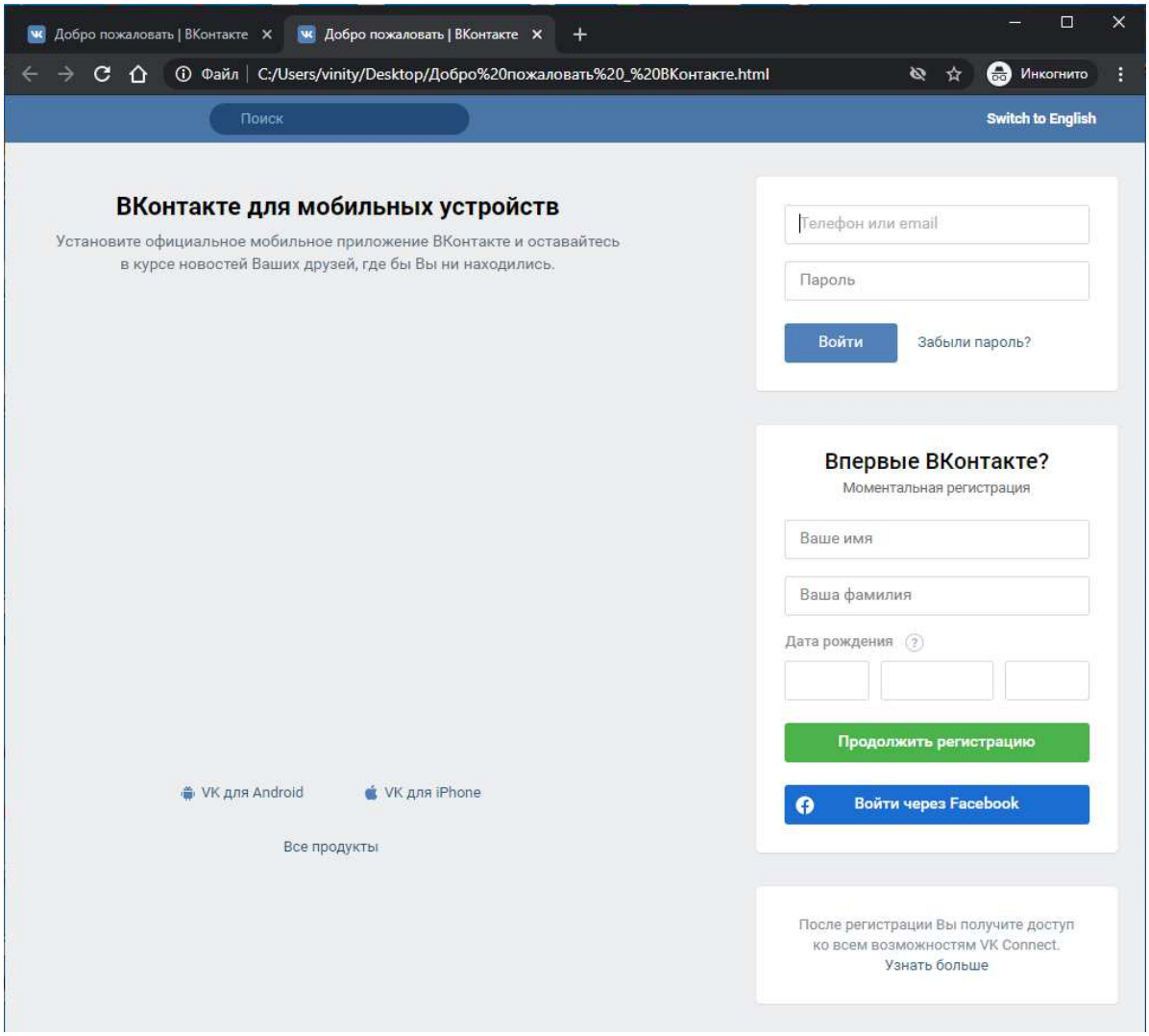


Рисунок 10.2. – Шаблон фишинговой страницы

Основной способ защиты от хищения конфиденциальных данных методом фишинговых атак – обучение безопасному поведению в сети Интернет[22]. Помимо общих рекомендаций внимательно читать сообщения и обращать внимание на детали и подозрительные данные, обычно предлагают также следующие методики:

[22] Непрерывное обучение культуре информационной безопасности – это общее правило защиты от применения методов социальной инженерии. О культуре информационной безопасности подробнее – в разделе 11.3.

1. Посещать только сайты, обеспечивающие безопасное соединение (защищенные посредством SSL-сертификата). Наличие валидного (правильного) сертификата проверяется по изображению закрытого замка в адресной строке браузера (рисунок 10.3).

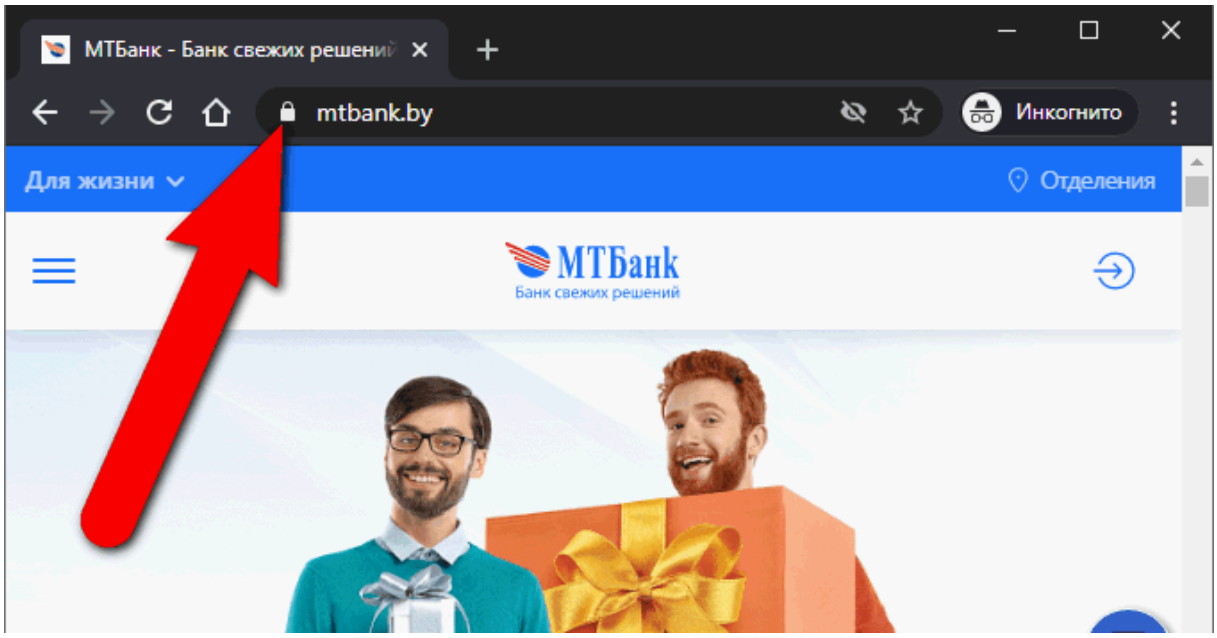


Рисунок 10.3. – Отображение сайта с валидным (правильным) сертификатом

Нельзя доверять сайтам с установленными, но не валидными SSL-сертификатами. Хотя такие сайты и открываются с приставкой https://, изображение с замком в адресной строке не отображается. Все соврменные браузеры блокируют содержимое таких сайтов и выдают предупреждение, что соединение не защищено (рисунок 10.4). Предупреждения отображаются в случаях использования самоподписанных SSL-сертификатов (без выпуска в удостоверяющих центров), неверно сгенерированных сертификатов, неверно установленных сертфикатов, сертификатов с истекшим сроком действия и т.п.

Нельзя доверять и сайтам, которые вообще не используют SSL-сертификаты: приставка https:// в адресной строке отсутсвует, изображение с замком в строке браузера не отображается, однако содержимое сайта доступно для ознакомления (рисунок 10.5).

Для обеспечения безопасного соединения иногда рекомендуют дополнительно использовать специальные DNS-сервисы, фильтрующие известные фишинговые адреса (например, OpenDNS [80].

2. Самостоятельно вводить веб-адрес в адресную строку браузера вместо использования гиперссылок из подозрительных сообщений. Использовать режим «Инкогнито».

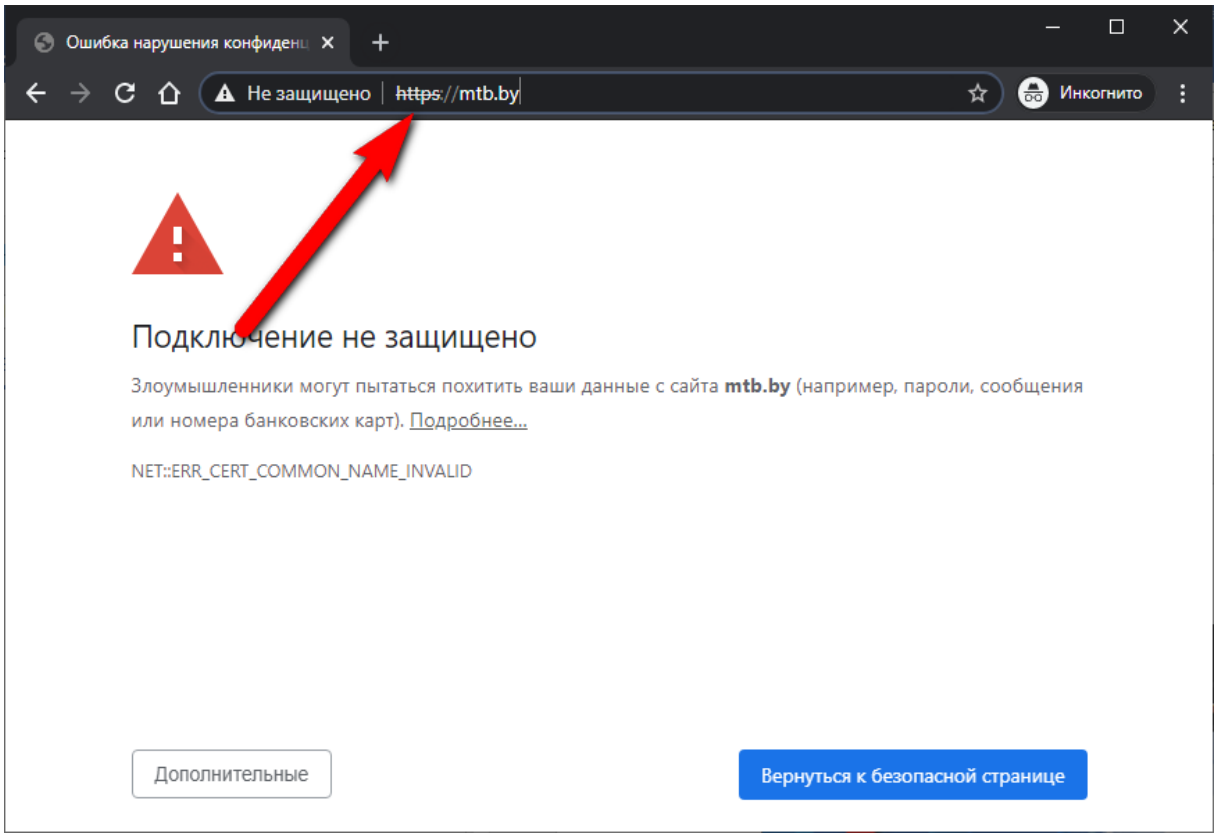


Рисунок 10.4. – Отображение сайта с невалидным сертификатом

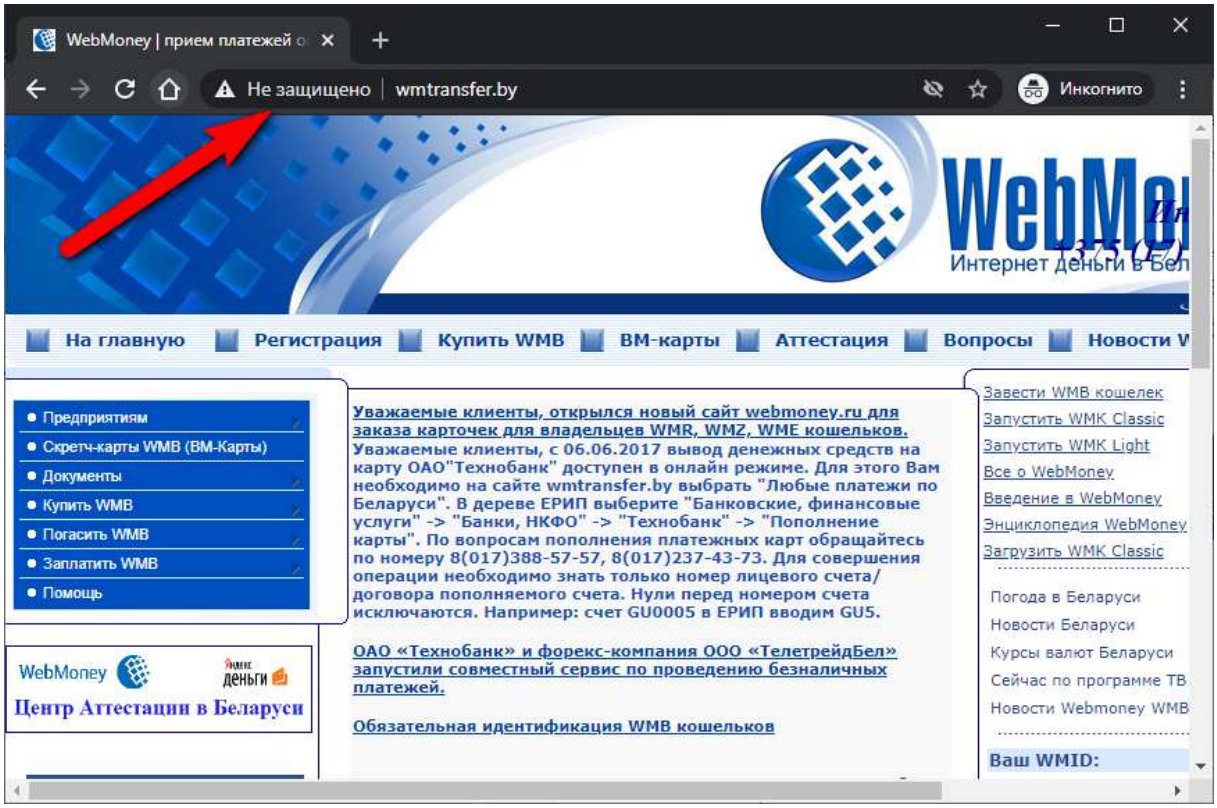
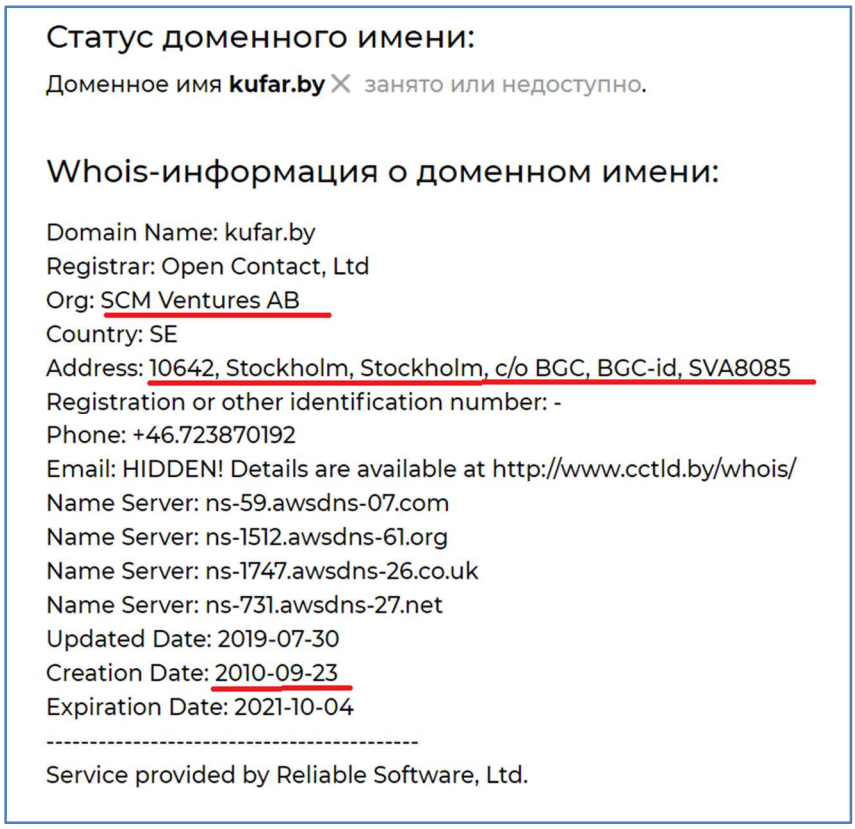


Рисунок 10.5. – Отображение сайта без SSL-сертификата

3. Проверять все контакты в адресной строке, а также выяснять, действительно ли лицом (организацией), указанным в качестве автора, направлялось сообщение с подозрительной ссылкой (актуально для электронных писем из банков, платежных сервисов, от организаций-партнеров, друзей и знакомых).

4. Проверять доменное имя, сверив его написание с официальным и изучив сведения о дате регистрации домена с помощью whois-сервисов (например, https://cctld.by/ для доменов в национальных зонах .by и .bel, белорусский сервис для других доменных имен https://hb.by/whois.aspx, зарубежный сервис https://www.whois.net/). Доменные имена фишинговых сайтов, как правило, зарегистрированы непродолжительное время, их владельцы являются физическими лицами, а представленные в whois-сервисах контакты не позволяют их идентифицировать.

Для примера предлагаем регистрационные данные официального домена популярного среди кибермошенников сервиса Kufar (www.kufar.by) (рисунок 10.6) и домена, созданного по аналогии с ним для целей фишинга (рисунок 10.7).


Статус доменного имени:

Доменное имя **kufar.by** ✕ занято или недоступно.

Whois-информация о доменном имени:

Domain Name: kufar.by
Registrar: Open Contact, Ltd
Org: SCM Ventures AB
Country: SE
Address: 10642, Stockholm, Stockholm, c/o BGC, BGC-id, SVA8085
Registration or other identification number: -
Phone: +46.723870192
Email: HIDDEN! Details are available at http://www.cctld.by/whois/
Name Server: ns-59.awsdns-07.com
Name Server: ns-1512.awsdns-61.org
Name Server: ns-1747.awsdns-26.co.uk
Name Server: ns-731.awsdns-27.net
Updated Date: 2019-07-30
Creation Date: 2010-09-23
Expiration Date: 2021-10-04

Service provided by Reliable Software, Ltd.

Рисунок 10.6. – Данные о регистрации официального домена

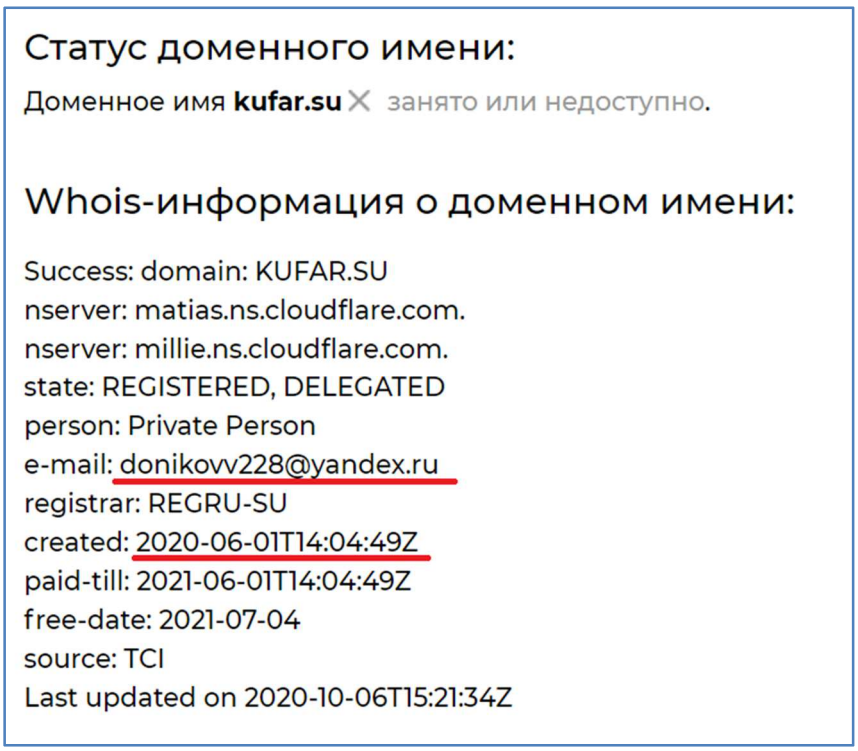


Рисунок 10.7. – Данные о регистрации домена для фишингового сайта

Сообщать о выявленных фишинговых сайтах в уполномоченные государственные органы и организации для применения юридических мер (в Беларуси – Национальный центр реагирования на компьютерные инциденты CERT.BY (www.cert.by), адрес для сообщений support@cert.by).

Фишинговые технологии постоянно развиваются, в результате чего появляются новые их модификации.

Например, **голосовой фишинг**, или **вишинг** (англ. vishing – voice phishing) предполагает выманивание регистрационных или платежных данных в телефонном разговоре по определенному сценарию либо с помощью специального робота (автоответчика). Такая мошенническая техника может проявляться в самых различных вариантах: звонок сотрудника банка со скрытого или подмененного номера с требованием предоставить данные банковской карты для ликвидации сбоя в системе или немедленного предотвращения хищения денежных средств с карт-счета; ночной звонок с мобильного телефона случайного прохожего от друга, попавшего в беду и оказавшегося без средств на такси (медицинскую помощь); звонок от похитителя, требующего выкуп за близкого родственника и т.п.

Иногда вишинг выступает техникой, дополняющей классический фишинг: сначала пользователь получает электронное сообщение, которое содержит не ссылку на фишинговый сайт, а номер телефона, позвонив по которому

и следуя четким указаниям автоответчика, пользователь также может предоставить данные своей банковской карты.

Частным случаем голосового фишинга является **претекстинг** (англ. pretexting, от pretext – повод, предлог). Суть техники состоит в подготовке сценария для взаимодействия с жертвой по телефону с целью быстрого получения от нее конфиденциальной информации. При помощи различных психологических приемов злоумышленник пытается вывести жертву из спокойного эмоционального состояния и, воспользовавшись моментом, получить необходимые данные. Обычно претекстингу предшествует подготовка – сбор личных сведений о потенциальной жертве, которые в последующем используются для того, чтобы при разговоре войти в доверие и вызвать меньше подозрений. Общая схема воздействия предполагает создание дефицита времени для принятия решения.

Основной способ защиты здесь – отсутствие спонтанных действий и тщательная проверка контактов и описанных событий прежде, чем будут сообщены регистрационные данные или переведены денежные средства.

В случае применения телефонного фишинга в виде коротких звонков с целью инициировать ответный звонок на специальный платный номер, единственной рекомендацией может быть только совет – не перезванивайте на незнакомые номера.

Смишинг (англ. SMiShing – от SMS и phishing) – телефонный фишинг посредством коротких текстовых сообщений на номер мобильного телефона. Осуществляется, как правило, с номера, который идентифицируется как банк, иная знакомая пользователю компания или организатор лотереи. В сообщении предлагается отправить ответ со специальным кодом или личными данными либо перезвонить на указанный номер телефона. В дальнейшем со счета пользователя могут быть списаны денежные средства за звонок (сообщение) на специальный платный номер, пользователь может быть перенаправлен к автоответчику по технологии вишинга либо злоумышленник просто получит доступ к отправленной конфиденциальной информации.

Общая рекомендация для защиты от фишинга – не отвечать на подобные сообщения и не перезванивать на подозрительные номера.

Смишинг также может быть техникой, дополняющей классический фишинг, когда короткое сообщение содержит ссылку на фишинговый сайт.

К слову, иногда телефонный фишинг может иметь вид простых коротких звонков на номер телефона с целью инициировать ответный звонок на платный номер.

Следующая техника выманивания конфиденциальных данных – **тайпсквоттинг** (англ. typosquatting, от typo – опечатка и cybersquatting –

кибersквоттинг[23]), является «выжидательной» и основана на человеческой невнимательности. Суть ее состоит в том, что кибермошенник регистрирует популярное доменное имя с опечаткой (например, facebool.com, kufat.by, belarusbanl.by и т.п.), создает внешне идентичную официальной страницу и рассчитывает на то, что пользователь не заметит опечатки. Для таких случаев очень активно использовалась доменная зона Камеруна (.cm): в 2009 г. каждый третий сайт в этой зоне был зарегистрирован тайпсквоттерами [81]. Кстати, конечной целью может быть не только получение конфиденциальных данных, но и распространение вредоносного программного обеспечения, поэтому для защиты рекомендуется при ручном вводе URL внимательно проверять адресную строку, прежде чем перейти к сайту.

От фишинга и его производных следует отличать **фарминг** (англ. pharming). Термин образован как омофон от англ. farming – занятие сельским хозяйством, однако в данном случае он не имеет какой-либо связи с исходным понятием – это намеренная игра слов, направленная на ассоциацию с фишингом.

Фарминг, как и фишинг, предполагает использование поддельных веб-сайтов для получения логинов, паролей и реквизитов банковских карт. Вместе с тем фарминг не является самостоятельной техникой социальной инженерии, поскольку предполагает получение данных через установку вредоносного кода на компьютер жертвы или DNS-сервер[24]. Перенаправление пользователя на поддельный сайт происходит без каких-либо сознательных действий со стороны пользователя. Злоумышленнику не требуется применять техники психологической манипуляции, равно как и взаимодействовать с пользователем в принципе.

При реализации фарминга на персональном компьютере модифицируется файл host, который будет подменять реальные IP-адреса сайтов на поддельные. Таким образом, вводя абсолютно верный URL в адресную строку браузера, пользователь все равно попадет на поддельный сайт, внешне идентичный официальному. При фарминговой атаке сервера будет произведено заражение целой системы доменных имен (DNS). Такой сервер может обрабатывать URL-запросы тысяч или миллионов интернет-пользователей,

[23] Кибersквоттинг (от англ. squatting – самовольное поселение) – регистрация доменных имен, указывающих на товарные знаки, фирменные наименования, популярные имена с целью их дальнейшей перепродажи или недобросовестного использования (например, для продвижения сайта).

[24] О методах социальной инженерии для установки вредоносного программного обеспечения – см. раздел 10.3.

каждый из которых будет перенаправлен на поддельный сайт. При этом пользователь может иметь полностью защищенное устройство (компьютер, планшет, смартфон), на котором нет вредоносного программного обеспечения [82].

10.3. Техники социальной инженерии для подкидывания вредоносного программного обеспечения с целью получения конфиденциальных данных

Классической техникой подкидывания вредоносного программного обеспечения является так называемый «**троянский конь**»[25]. По своей сути метод очень схож с фишингом и чаще всего осуществляется путем рассылки сообщений по электронной почте. Сообщения снабжаются приложениями, при загрузке которых производится установка вредоносного программного обеспечения (не только троянцев!).

Для того чтобы побудить пользователя открыть прилагаемый файл, используются аналогичные фишинговым психологические приемы. Само приложение может быть замаскировано под гиперссылку с привлекательным заголовком («обновление» антивируса, денежный выигрыш, компромат на сотрудника).

Техника «троянский конь» более персонализирована, чем фишинг, поскольку, как правило, направлена на извлечение больших объемов данных либо на постоянное считывание информации с персонального компьютера или сервера (слежение), когда все действия пользователя записываются и отправляются злоумышленнику. Иногда «троянский конь» используется также для вымогательства (например, в случаях, когда в результате воздействия вредоносного программного обеспечения вся информация на компьютере оказывается зашифрованной либо доступ к ней блокируется).

Ближайший актуальный пример использования «троянского коня» – организованная в сентябре 2020 г. масштабная кампания по рассылке и заражению вредоносным программным обеспечением пользователей белорусского национального сегмента сети Интернет, в числе которых Министерство транспорта и коммуникаций, Государственный комитет по имуществу, Национальная государственная телерадиокомпания, Министерство

[25] В настоящем разделе рассматривается только защита от применения метода социальной инженерии, именуемого «троянским конем». О защите от вредоносного программного обеспечения, включая троянские программы, – см. главу 4.

обороны, ряд других государственных органов и организаций. Злоумышленники при этом использовали актуальную в Беларуси «протестную» тематику [83].

Для защиты от применения техники «троянский конь» необходимо тщательно проверять контакты в адресной строке, идентифицировать автора сообщения, а также выяснять, действительно ли лицом (организацией), указанным в качестве автора, направлялось сообщение с подозрительной ссылкой (электронная почта отправителя может быть фиктивной; почтовый аккаунт может быть взломан). В целом рекомендуется остерегаться электронных писем, которые содержат в приложении исполняемые файлы.

Техника **«дорожное яблоко»** предполагает использование съемных электронных носителей для распространения вредоносного программного обеспечения и ориентирована на любопытство жертвы. Объект (например, USB-накопитель) оставляется в местах, где он может быть легко найден: на полу в коридоре, в лифте, у входной двери и т.п. Другой вариант – адресная передача носителя пользователю прямо на рабочее место или через третье лицо (скажем, вахтера).

Основная задача злоумышленника – мотивировать пользователя открыть содержимое электронного носителя на компьютере. Для этих целей используются самые различные способы: нанесение на объект интригующих надписей, вроде «конфиденциально», либо логотипов организации, в которую подбрасывается «дорожное яблоко»; привлекательные заголовки файлов («Заработная плата директора за январь 2020 г.», «Налоговая декларация», «Годовой отчет о прибыли» и т.п.); прикрепление к носителю ключа от неизвестной входной двери и т.п.

Для защиты от применения техники «дорожное яблоко» не следует доверять никаким случайно обнаруженным съемным носителям информации и потому не подключать их к компьютеру, даже обеспеченному защитой от вредоносного программного обеспечения (возможна программная адаптация «дорожного яблока» под известные злоумышленнику настройки безопасности системы). Рекомендуется также не принимать в дар носители информации, включая мобильные телефоны, планшеты, компьютеры с предустановленным программным обеспечением, если есть малейшая вероятность того, что на этих устройствах установлены сторонние приложения, обеспечивающие утечку конфиденциальной информации.

При использовании метода **«кви про кво»** (от лат. quid pro quo – услуга за услугу) злоумышленник предлагает пользователю услугу или иную выгоду в обмен на информацию или доступ. Наиболее частый сценарий –

телефонный звонок или электронное сообщение из службы технической поддержки с предложением дистанционно установить программное обеспечение для решения какой-либо существующей (или вымышленной) технической проблемы. В результате пользователь добровольно предоставляет данные злоумышленнику либо самостоятельно выполняет необходимые команды на компьютере или смартфоне. Чтобы ввести в заблуждение пользователя, злоумышленник может использовать заранее подготовленный сценарий выявления технической проблемы при помощи пользователя, тем самым демонстрируя ему добрые намерения.

В сущности, описанная техника может в равной степени применяться как при выманивании конфиденциальных данных, так и при подкидывании вредоносного программного обеспечения с целью получения или уничтожения (повреждения) конфиденциальных данных.

Защититься от применения техники «кви про кво» можно, если отказываться предоставлять конфиденциальные данные по телефону или в интернет-переписке, а также не совершать со смартфоном и компьютером действий, которые пользователю непонятны (неизвестны), не устанавливать неизвестное (не разрешенное в организации) программное обеспечение.

10.4. Обратная социальная инженерия

При атаке посредством обратной социальной инженерии (англ. Reverse Social Engineering, RSE) злоумышленник не инициирует контакт с жертвой, а создает условия для того, чтобы пользователь сам обратился за помощью и предоставил конфиденциальные данные. Основная задача злоумышленника в данном случае – установить доверительные отношения с жертвой, чтобы для решения проблемы пользователь обратился именно к нему.

Наиболее часто описываемый [84] сценарий обратной социальной инженерии реализуется сотрудниками организаций. Злоумышленник, пользуясь случаем, перемещает на компьютере коллеги важный файл в другой каталог либо просто изменяет его имя таким образом, чтобы он не мог быть найден. Обращаясь за помощью к злоумышленнику, жертва в панике самостоятельно просит войти в систему под ее логином и паролем, будучи убежденной в том, что иным путем восстановить файл нельзя. Успешность такого сценария зависит от того, насколько серьезной была предварительная подготовка: во-первых, жертва, утратившая важный файл, должна была обратиться в первую очередь к злоумышленнику; во-вторых, изначально необходимо было знать, какие файлы являются

критично важными; в-третьих, следовало выбрать удобный момент, чтобы создать саму проблему.

В сети Интернет атаки с использованием обратной социальной инженерии производятся, как правило, по электронной почте, однако могут иметь место и в социальных сетях. Исследования показывают, что социальные сети способствуют более высокой степени доверия даже между не знакомыми лично людьми [85]. Создание поддельного профиля, у которого будет несколько общих с жертвой «друзей», считается легкой для хакера. Например, в 2014 г. Facebook обнаружил на своей платформе 14% поддельных профилей [86].

Обратную социальную инженерию могут также использовать недобросовестные разработчики программного обеспечения, которые в процессе разработки могут встроить вредоносный код отложенного действия. В таком случае программа начнет какое-то время спустя давать сбои, а пользователи будут обращаться за помощью в устранении неполадок. Таким образом, злоумышленники будут иметь возможность получить доступ к конфиденциальной информации [87].

В отличие от обычной социальной инженерии методы обратной более трудоемки, поскольку требуют информационной подготовки и существенно растянуты по времени. Очевидно, что такой способ атаки более персонализирован и не может распространяться сразу на широкую аудиторию. При этом злоумышленника, использующего обратную социальную инженерию, достаточно сложно отследить, поскольку действует он под чужими регистрационными данными.

Обратная социальная инженерия может сочетаться с классическим фишингом, техниками «троянский конь» или «дорожное яблоко», когда пользователь, подвергаясь атаке, устанавливает на компьютер вредоносное программное обеспечение, а затем, получив во всплывающем окне контакты «технической поддержки», обращается за помощью и сообщает аутентификационные данные злоумышленнику, открывая ему доступ к системе.

Для того чтобы защититься от применения методов обратной социальной инженерии, необходимо избегать компрометации аутентификационных и иных конфиденциальных данных: не сообщать их никому и ни при каких обстоятельствах, исключить плечевой серфинг. Организациям рекомендуется письменно предупреждать сотрудников об ответственности за раскрытие такой информации. Кроме того, необходимо регламентировать правила корректного раскрытия действительно необходимой информации в интернет-переписке, по телефону, в личной беседе, а также использовать особые

процедуры подтверждения для всех, кто запрашивает доступ к конфиденциальным данным. Особое внимание следует уделять организации надлежащей технической поддержки, чтобы работнику было проще и быстрее обратиться с возникшей проблемой к внутреннему специалисту без страха быть наказанным за допущенную ошибку.

Вопросы для самопроверки

1. Дайте определение понятию социальной инженерии.
2. Изложите базовую схему воздействия в социальной инженерии. Какой этап следует считать главным и почему?
3. Опишите технику плечевого серфинга и назовите основные меры защиты от ее применения.
4. Какие существуют способы распознавания фишинговых страниц?
5. Какие признаки могут указывать на фишинговое сообщение?
6. В чем отличие классического фишинга от смишинга?
7. Как можно сочетать классический фишинг и вишинг для более результативной атаки?
8. Что такое претекстинг?
9. На чем основана техника тайпсквоттинга?
10. Почему фарминг не является техникой социальной инженерии?
11. В чем отличие техник «троянский конь» и «дорожное яблоко»?
12. Опишите суть обратной социальной инженерии. В чем ее отличие от техники «кви про кво»?

11. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ В ОРГАНИЗАЦИИ

11.1. Понятие и классификация внутренних нарушителей

В контексте информационной безопасности внутренним нарушителем (англ. insider – свой, хорошо осведомленный человек) принято называть [22, с. 96] работника организации, который в результате умышленных или неумышленных действий получает, изменяет или уничтожает конфиденциальные данные организации.

В противовес внешним нарушителям (англ. outsider – чужой, посторонний), которые осуществляют атаки на корпоративную систему безопасности извне (посредством сети Интернет, телефонной связи), внутренние нарушители имеют доступ к ресурсам организации изначально и хорошо понимают, как работает организация и как устроена ее система безопасности.

Примерами умышленных действий внутреннего нарушителя могут быть следующие:

– получение несанкционированного доступа к информационным системам и передача (распространение) конфиденциальных данных за пределы организации либо использование таких данных в личных интересах;

– несанкционированное изменение или уничтожение конфиденциальных данных в информационной системе;

– несанкционированное изменение статуса пользователя в информационной системе;

– подбор паролей к защищенному программному обеспечению либо защищенным областям дискового пространства;

– выведение информационной системы из строя, блокирование доступа к ней;

– внедрение аппаратных средств и программного обеспечения, которые позволяют преодолевать систему защиты информации и осуществлять периодическое или постоянное скрытое слежение за изменениями в информационной системе, а также обеспечивать передачу данных на внешний сервер.

Умышленные действия, связанные с внутренним нарушением системы защиты информации, всегда совершаются работниками вне пределов должностных обязанностей (несанкционированно), тогда как неумышленные

действия являются следствием непрофессионального исполнения должностных обязанностей.

Роль внутренних нарушителей не стоит недооценивать. По данным исследования Аналитического центра компании InfoWatch, 63,5% утечек конфиденциальной информации во всем мире за 2018 г. случилось в результате внутренних нарушений, а по странам СНГ доля внутренних нарушений достигает 90,5% [90].

Потенциальная вероятность нанесения ущерба организации в результате действий внутреннего нарушителя зависит от уровня доступа к конфиденциальным данным, а также характера деятельности и профессиональной подготовки работника. Скажем, системный администратор, программист или менеджер обработки данных может нанести значительно бóльший ущерб, нежели обычный неопытный пользователь, не имеющий технического образования.

Масштаб и направленность внутренней атаки может определяться еще и мотивацией нарушителя [45]. Например, наибольший вред очевидно будет причинен нарушителями, мотивированными извне: их действия определяются внешним заказчиком, они имеют прямой умысел на нарушение системы защиты информации и совершение запрещенных действий с конфиденциальными данными. Такие работники могут быть специально трудоустроены в организацию либо привлечены из числа лояльных сотрудников путем подкупа или запугивания. Это могут быть очень качественно подготовленные специалисты, обеспеченные программными и (или) техническими средствами для осуществления атак на систему защиты информации. Противостоять внутренним нарушителям, мотивированным извне, всегда сложнее.

Технически проще всего защититься от незлонамеренных внутренних нарушителей (халатных и манипулируемых работников [45]), которые не имеют прямого умысла на причинение вреда организации и не используют конфиденциальную информацию в своих личных интересах. Они создают ненаправленные угрозы: например, пытаются скопировать конфиденциальные данные для работы из дома или в командировке; норовят установить неразрешенное программное обеспечение на служебный компьютер; по чьей-либо настоятельной просьбе перенаправляют информацию на внешний адрес электронной почты; подключают к офисному оборудованию носители, содержащие вредоносное программное обеспечение и т.п. Ввиду недостаточной информированности такой работник может вообще не осознавать, что нарушает какие-то правила, однако при малейших технических

трудностях прекратит совершать запрещенные действия, потому что прямого умысла на причинение вреда организации не имеет. Однако если информационная система технически защищена плохо, если культуре информационной безопасности уделяется недостаточно внимания, такие работники легко откроют «шлюзы» для масштабных утечек конфиденциальных данных.

Наибольшее количество ограничений доступа должны иметь нелояльные работники и работники-саботажники. Первые стараются унести максимальное количество доступной информации, часто даже не осознавая ее действительной ценности и не имея представления, каким образом они будут ее использовать [45]. К этой группе работников относят, например, тех, кто намеревается сменить нанимателя и накапливает данные для последующего трудоустройства, а также работников-стажеров и практикантов, собирающих данные «про запас». Действуют такие нарушители открыто, используя предоставленные им служебные возможности.

Работники-саботажники [45], напротив, отличаются прямым стремлением нанести какой-либо вред организации (не обязательно с использованием конфиденциальной информации), причем сделать это негласно и любыми доступными способами.

11.2. Меры, направленные на защиту информационной системы от внутреннего нарушителя

Правовые и организационные меры защиты от внутренних нарушителей не имеют принципиальных отличий от общих подходов, о которых шла речь в разделах 2.1. и 2.2. Здесь коротко охарактеризуем наиболее подходящие для рассматриваемых целей технические меры.

1. **Противодействие несанкционированной установке модемов, телефонов, точек доступа**:

– опечатывание всех свободных разъемов, портов компьютера;

– отключение всех неиспользуемых модулей, разъемов;

– установка специализированных средств защиты, сигнализирующих о попытке вскрытия корпуса компьютера;

– использование средств, функционирующих на трех уровнях – уровне базовой системы ввода–вывода (BIOS), уровне операционной системы, уровне специализированных средств защиты информации, обеспечивающих контроль аппаратной конфигурации компьютера [22].

2. **Применение системы централизованного мониторинга безопасности с использованием технологии интеллектуальных программных агентов.**

Система защиты строится на архитектуре консоль–менеджер–агент. Так, на каждую из контролируемых систем устанавливается программный агент, который выполняет соответствующие настройки программного обеспечения, проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности информационной системы. Управление агентами осуществляется по сети центральной программой-менеджером, которая направляет управляющие команды всем агентам контролируемой ими зоны, а также сохраняет все данные, полученные от агентов в центральной базе данных. В свою очередь управление программой-менеджером (или несколькими такими программами) осуществляет администратор при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т.п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу [22]. В качестве примера такой программы можно привести DLP-систему белорусского производителя LibraDLP http://www.librasoft.by/LibraDLP_rus_web.pdf.

Технологии интелектуальных программ-агентов достаточно эффективны, но ввиду высокой стоимости широкое их применение не всегда оправданно.

3. **Стандартизация программного обеспечения.** Установка на всех рабочих компьютерах только стандартизированного программного обеспечения существенно ограничивает возможности для обхода используемых средств защиты информации (например, средств контентной фильтрации, шифрования, стеганографии, межсетевых экранов). При этом запуск и установка иного программного обеспечения (вне списка разрешенных программ) должен быть не только ограничен, но и отслеживаем.

4. **Организация резервного копирования информации** является важным элементом снижения возможного ущерба от тех действий внутренних злоумышленников, которые направлены на уничтожение или модификацию данных.

5. **Ограничение возможностей прослушивания сетевого трафика** возможно путем замены в локальной сети всех концентраторов на коммутаторы (в идеале – «интеллектуальные» управляемые коммутаторы третьего

уровня, хотя это небюджетное решение). Концентраторы открывают злоумышленнику доступ ко всему сетевому трафику в пределах сегмента локальной сети, тогда как в сети, построенной на коммутаторах, трафик направляется только тому компьютеру, которому он предназначен [22].

6. **Шифрование сетевого трафика** на прикладном или сетевом уровне (последний вариант предпочтительнее, рекомендуется протокол IPSec, подробнее см. в главе 9).

7. **Периодический автоматизированный анализ защищенности сети сканерами уязвимости.** Результатом работы сканера является достаточно подробная информация о корпоративной сети, включающая список сетевого оборудования, компьютеров с запущенными на них службами и версиями сетевого программного обеспечения, уязвимостей, присущих данному программному обеспечению, учетных записей пользователей [22].

В итоге администратор будет располагать данными о тех уязвимых местах системы, которые могут быть использованы внутренними нарушителями для вторжений, и примет решение об адекватных мерах реагирования (профилактики). Дополнительно рекомендуется [22; 71] применять средства обнаружения несанкционированного сканирования, которое может осуществляться внутренним нарушителем для более направленной атаки.

8. **Ведение учета и аудит событий информационной безопасности.** Все события, связанные с информационной безопасностью или имеющие признаки нештатных ситуаций, должны быть зарегистрированы в журналах учета. К таким событиям могут быть отнесены определенные действия пользователей (например, авторизация в системе, получение данных о клиентах, запуск программ), запуск или закрытие программ, сообщениях об ошибках или сбоях, изменение конфигурации программно-программного обеспечения, включение или выключение оборудования. События в журналах учета хранятся установленное политикой информационной безопасности время.

Регистрация событий может выполняться автоматически, с помощью автоматизированных средств или в ручном виде. Автоматически регистрация событий выполняется средствами операционных систем или прикладного программного обеспечения в момент совершения события. С помощью автоматизированных средств регистрация события совершается сотрудником, как правило, с помощью специального программного обеспечения. В ручном виде журналы обычно ведутся на бумажных носителях.

Администратору безопасности предоставляется доступ к журналам регистрации событий. В установленный регламент администратор безопасности выполняет аудит (проверку) всех зарегистрированных событий

на предмет наличия нештатных ситуаций, которые способны понизить степень информационной безопасности. Если такие нештатные ситуации в процессе аудита выявляются, то администратор безопасности формирует требования к доработкам информационной системы.

Для проведения всех работ должны быть установлены регламенты в политике информационной безопасности, такие как период хранения журналов, интервал между аудитами, время подготовки требований для доработки системы, время внесения изменение в систему.

Зарегистрированные события должны содержать сведения по следующим позициям:

– время начала и завершения работы системы;

– авторство изменений;

– ошибки системы и предпринятые корректирующие действия;

– возможность сопоставления сведений учетной записи в системе с физическим лицом – пользователем системы.

Регистрация и аудит событий не должны существенно препятствовать выполнению функциональных процедур на рабочих местах сотрудников. Доступ к средствам аудита должен быть защищен для предотвращения возможности их ненадлежащего использования.

9. **Использование виртуальных ловушек.**

Для обнаружения нарушителей информационной безопасности корпоративной среды рекомендуется использовать виртуальные ловушки, о которых более подробнее говорилось в разделе 8.3.

При внедрении виртуальных ловушек рекомендуется [22]:

– размещать ловушки, эмулирующие сервисы, на рабочих машинах администраторов и начальников вместе с рабочими сервисами;

– создавать специальные сервера, полностью имитирующих уязвимые для атаки компьютеры;

– информацию об обнаруженных нарушениях использовать в защите всех машин вычислительной сети. Периодически менять имитацию уязвимых мест в сервисах.

10. **Использовать программные и программно-аппаратные средства защиты от копирования и редактирования электронных документов.**

Программные и программно-аппаратные средства могут использовать нанесение скрытых маркировок в скачиваемые файлы. С помощью стеганографических алгоритмов в момент скачивания или редактирование файлов информация о пользователе скрыто вносится в файл (см. раздел 6.3). Таким

образом, скачивание и распространите файла не ограничивается, но возможно в последующем выявить пользователя, который скачал этот файл, и привлечь его к ответственности.

Применение парольных систем для предоставления персонального доступа авторизованным пользователям (см. главу 5) или систем управления доступом, например, на базе службы управления правами Active Directory. Доступ на чтение, редактирование, удаление может предоставляться после авторизации с помощью пароля, токена.

11. **Использование средств защиты ресурсов локальной сети** на рабочих местах и серверах: межсетевых экранов (подробнее см. главу 7), систем обнаружения атак и вторжений (подробнее см. главу 8), антивирусного программного обеспечения (подробнее см. раздел 4.4).

12. **Своевременное обновление программного обеспечения** (операционных систем, систем обнаружения атак и вторжений, межсетевых экранов и антивирусного программного обеспечения) позволяет существенно снизить вероятность причинения вреда ресурсам организации внутренним нарушителем, даже если он обеспечен техническими и программными средствами взлома.

11.3. Культура информационной безопасности

Внутренним нарушителям невозможно противодействовать исключительно формальными мерами – техническими, организационными, правовыми, поскольку все они могут быть либо неправильно использованы, либо неверно истолкованы работниками организации. По этой причине значительную роль играет культура информационной безопасности – совокупность моделей поведения в организации, которые способствуют защите информации всех видов [88]. Проще говоря, культура информационной безопасности – «это то, что происходит с безопасностью, когда люди предоставлены сами себе» [89].

Белорусские организации все еще крайне мало внимания уделяют культуре информационной безопасности, представляя ее исключительно «бумажной» безопасностью: основательно подготовленные пакеты документов остаются на полках невостребованными по причине того, что многие работники просто не способны их понять и усвоить.

Устойчивая культура безопасности требует, чтобы каждый работник организации был в нее вовлечен. При этом каждый вовлеченный в производственный процесс человек должен разделять общее видение информационной безопасности организации, понимать свои роль и обязанности и быть

надлежащим образом подготовлен для их исполнения. Как правило, работники организации, не имеющие прямых намерений причинить вред, хотят делать правильные вещи – их просто нужно этому научить.

Основу культуры информационной безопасности составляет политика информационной безопасности (подробнее см. раздел 3.3.1).

Полагаем, что ключевыми условиями для возникновения, развития и устойчивости культуры информационной безопасности являются осведомленность, ответственность и менеджмент.

Так, достаточная осведомленность о существующих угрозах и мерах защиты, образованность в вопросах информационной безопасности предотвращают некомпетентное или неправильное поведение пользователей [91]. Достаточная осведомленность может быть достигнута непрерывным обучением информационной безопасности не только путем организации семинаров, тренингов, повышения квалификации, но и периодического коллективного расследования инцидентов информационной безопасности. Обучающие процедуры не должны быть формальными (как это часто случается, например, с инструктажем новых и временных работников) и абстрактными.

Ответственность предполагает, что каждый работник понимает свою роль в информационной безопасности и наделен должностными обязанностями, позволяющими ее обеспечивать. Иными словами, ответственность не должна быть приравнена исключительно ко взысканиям (поощрениям) – это в первую очередь, вопрос правильного распределения полномочий по предотвращению, обнаружению и эффективному реагированию на инциденты информационной безопасности.

Обоснованным является убеждение, что «культура – это отношение к явлению большинства» [92]. В любом человеческом сообществе культуру формируют лидеры, авторитет которых основан на доверии [92]. Следовательно, не менее важным условием для возникновения, развития и устойчивости культуры информационной безопасности внутри организации является наличие системы управления информационной безопасностью (менеджмента информационной безопасности), которая представлена иерархией лидеров. По этой причине считается более эффективным назначение на позиции ключевых менеджеров информационной безопасности работников, которые уже разделяют ценности, отраженные в политике информационной безопасности организации, и которые, располагая доверием большинства, способны эти ценности внедрять и развивать.

Следует отметить, что вопросы культуры информационной безопасности часто выходят далеко за пределы конкретной организации и требуют

системного решения не только на государственном, но и на глобальном уровнях (см. публикацию о зарубежном опыте формирования культуры информационной безопасности в обществе [91]). Интересно, что, осознавая проблему обеспечения информационной безопасности во всем мире, Генеральная Ассамблея ООН еще в 2003 г. приняла Резолюцию [93], направленную на создание глобальной культуры кибербезопасности, и предложила государствам-участникам элементы для ее создания.

Вопросы для самопроверки

1. Дайте определение понятию внутреннего нарушителя. Выделите ключевые отличия внутренних и внешних нарушителей.
2. Приведите примеры действий внутренних нарушителей, разделив их на умышленные и неосторожные.
3. От чего зависит величина риска причинения ущерба организации внутренним нарушителем?
4. Какой тип внутреннего нарушителя является наиболее опасным для организации? Обоснуйте свой ответ.
5. От какого типа нарушителя проще всего защититься технически? Обоснуйте свой выбор.
6. Охарактеризуйте три наиболее эффективные технические меры защиты от внутреннего нарушителя. Обоснуйте свой выбор мер.
7. Что такое культура информационной безопасности организации?
8. Каковы ключевые условия формирования культуры информационной безопасности в организации?

12. ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ЗАТРАТ НА СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ

Учитывая важность проблемы конфиденциальности информации ограниченного распространения, необходимость создания в организациях системы защиты информации является непреложным фактом. Вместе с тем всегда остается открытым вопрос о рациональных объемах затрат на защиту информации и их экономической эффективности. Помимо лиц, принимающих решения, и специалистов по информационной безопасности свой взгляд на эту проблему, как правило, имеют бухгалтеры, экономисты, юристы, менеджеры и другие сотрудники, участвующие в процессах обработки информации.

Все традиционные инструменты оценки экономической эффективности затрат в качестве основного показателя рассматривают изменение прибыли хозяйствующего субъекта после внедрения инвестиционного проекта. Темпы роста прибыли, опережающие темпы роста затрат на содержание компании, являются одним из ключевых критериев финансовой устойчивости компании [94]. В то же время при анализе эффективности системы защиты информации ключевым показателем является предотвращенный (либо существенно уменьшенный) ущерб, который хоть и является материальным, однако носит вероятностный характер и не может быть измерен объективно и показан в бухгалтерском учете как соотношение прибыли и затрат [96]. По этой причине современные предприятия почти не используют инвестиционный анализ (например, путем применения ставки дисконтирования) при оценке эффективности вложений в систему защиты информации.

Довольно часто используется подход, основанный на методике оценки совокупной стоимости владения (англ. Total Cost of Owership, TCO), которая первоначально разрабатывалась как средство расчета стоимости владения компьютером. На русском языке этот подход наиболее детально описан в ряде работ С.А. Петренко [95], в т.ч. совместно с Е.М. Терехо-вой [94]. Методика позволяет оценивать только расходную часть (затраты) на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года. Лучше всего методика оценки совокупной стоимости владения зарекомендовала себя там, где требуется оценить экономическую эффективность альтернативных вариантов защиты информации при одинаковых условиях [96]. На основе полученных

данных также можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации [95].

Основная цель расчета совокупной стоимости владения – выявление избыточных статей расходов и оценка возможности возврата инвестиций, вложенных в технологии безопасности [96]. Здесь и обнаруживается главная проблема – необходимость определить составляющие совокупной стоимости владения и произвести их количественную оценку.

Все составляющие совокупной стоимости владения системой защиты информации условно разделяют [94] на прямые («видимые» пользователю первоначальные затраты, которые обычно значительно меньше и, как правило, имеют фиксированную стоимость) и косвенные («невидимые» затраты на эксплуатацию и использование, которые являются дополнительными и чаще всего не могут быть четко определены до внедрения системы защиты информации).

К группе «видимых» затрат относят [94]:

– стоимость лицензий;

– стоимость внедрения;

– стоимость обновления;

– стоимость сопровождения.

Для привлечения клиентов поставщиками готовых решений в «видимом» секторе также могут использоваться скрытые механизмы увеличения стоимости [96]. Кроме того, стоимость внедрения корпоративной системы защиты информации также не может быть окончательно определена до ее приобретения.

«Невидимые» затраты появляются после внедрения системы защиты информации, и к ним относят [94]:

– затраты на оборудование (приобретение и (или) обновление средств защиты информации, организацию бесперебойного питания и резервного копирования информации, установку новых устройств безопасности и т.п.);

– затраты на дополнительное программное обеспечение (системы управления безопасностью, VPN, межсетевые экраны, антивирусы и т.п.);

– затраты на поиск и обучение персонала, ликвидацию допущенных ошибок вследствие трудностей в работе со средствами защиты, неприятия или саботажа новых средств защиты;

– другие затраты (например, стоимость риска выхода из строя всей системы защиты информации или отдельных ее частей; затраты на юридические споры и выплаты компенсаций и штрафов).

Более детальное описание затрат см. в работе С.А. Петренко [95]. Для того чтобы учесть все прямые и косвенные затраты, необходимо в деталях представлять себе процедуру внедрения и эксплуатации системы защиты информации, а также учитывать не только единовременные, но и систематические затраты [97, с. 42–45].

Показатель ТСО системы защиты информации рассчитывается как сумма всех затрат, «видимых» и «невидимых», а затем этот показатель сравнивается с рекомендуемыми величинами для данного типа предприятия (выделяется 17 таких типов), и если полученная совокупная стоимость владения системой защиты информации значительно превышает рекомендованное значение (приближается к предельному), то необходимо принять меры к ее снижению (например, уменьшением числа специализированных элементов, настройкой программного обеспечения, внедрением альтернативных инструментов меньшей стоимости, максимальной централизацией управления системой информационной безопасности и пр.) [96].

Основной недостаток описанной методики состоит в том, что в качестве базы для сравнения используются данные и показатели ТСО для западных компаний. В отношении отечественных организаций методика требует применения так называемых поправочных коэффициентов (см. подробнее у С.А. Петренко [95]).

Набирают популярность также методики обоснования затрат на систему защиты информации, которые основаны на оценке информационных рисков (см., например, [96]). Подход особенно актуален для внедрения систем защиты информации ограниченного распространения, поскольку позволяет выбирать такой режим обработки информации, при котором эффект от ее использования с учетом позитивных и негативных последствий будет максимальным [96].

Методики оценки информационных рисков позволяют ранжировать значимость угроз (в зависимости от вероятности их наступления и предполагаемого материального ущерба). В итоге появляется возможность выделять три группы рисков [96]:

– принимаемые риски, затраты на предотвращение которых неизбежны;

– непринимаемые риски, которые имеют малую вероятность возникновения и незначительный ущерб при их реализации, а потому не учитываются при планировании затрат на систему защиты информации;

– промежуточная область рисков, которые рассматриваются только при имеющемся ресурсе на финансирование защиты информации.

Объем рисков сопоставляется с объемом предполагаемых затрат на систему защиты информации, и полученный показатель позволяет оценивать экономическую эффективность от внедрения системы защиты информации в организации.

Как бы там ни было, любой метод оценки экономической эффективности затрат на систему защиты информации является «всего лишь набором математических формул и выкладок, корректность применения которых – только вопрос обоснования» [96]. Любая методика расчета имеет общее уязвимое место – качество и достоверность данных, на основе которых производятся вычисления, поэтому основные усилия должны быть направлены на тщательный сбор и обработку первичных данных.

Вопросы для самопроверки

1. Для чего используются методики экономической оценки затрат на защиту информации?
2. Какие показатели положены в основу инвестиционного анализа затрат?
3. В чем состоит основное препятствие в применении инвестиционного анализа при оценке затрат на систему защит информации?
4. В чем состоит суть методики оценки совокупной стоимости владения системой защиты информации?
5. Какие категории затрат в методике ТСО относят к группе прямых («видимых»), а какие – к группе косвенных («невидимых»)?
6. В чем состоит преимущество использования методик обоснования затрат на систему защиты информации, основанных на анализе информационных рисков?

ЗАКЛЮЧЕНИЕ

В пособии изложены основные принципы и подходы обеспечения конфиденциальности информации в сети Интернет, которые позволяют создать целостную систему защиты информации, включающую комплекс правовых, организационных, технических и образовательных мер. Конечная цель такой системы – безопасность как отдельной личности, так и организаций, а также государства в целом.

Постоянное развитие информационных технологий создает пространство для возникновения новых уязвимостей информационных систем, которые могут быть использованы злоумышленниками в своих целях. Устранение возникающих уязвимостей возможно только в случае наличия обязательного непрерывного процесса обеспечения безопасности всего информационного обмена, который позволяет обнаруживать и устранять возникающие угрозы конфиденциальности информации в сети Интернет.

Часть угроз с присущими им рисками возможно устранить исключительно с помощью программно-технических средств, часть – с привлечением организационных и правовых средств.

На общий уровень защищенности влияет целый ряд внутренних и внешних факторов, но использование различных инструментов в комплексе позволяет либо минимизировать риски, либо предусмотреть и ликвидировать источник угрозы. Вместе с тем следует постоянно помнить, что идеальной безопасности не существует, и соотносить возможные риски с финансовыми возможностями защиты от них. Иногда более целесообразным является перенаправление (страхование) рисков либо их принятие и ликвидация последствий.

В пособии предпринята попытка описания общей модели для разработки, внедрения, поддержания функционирования, мониторинга и улучшения системы обеспечения конфиденциальности информации в сети Интернет. Однако в современных информационных системах уже существуют проблемы, которые требуют нетривиальных интегральных подходов, как, например, противодействие социальной инженерии и защита от внутреннего нарушителя, где становится особенно актуальным аудит информационной безопасности и дополнительное обучение персонала, в связи с чем отдельное внимание было уделено и этим вопросам.

Авторы надеются, что, изучив этот курс, студенты (магистранты) смогут сформировать базовые навыки организации систем защиты конфиденциальной информации в сети Интернет, которые станут основой для дальнейшего самообразования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Число пользователей интернета в мире выросло до 4,1 млрд человек [Электронный ресурс] // ТАСС: Информационное агентство. – 5 нояб. 2019. – Режим доступа: https://tass.ru/obschestvo/7080150. – Дата доступа: 01.10.2020.

2. Концепция информационной безопасности [Электронный ресурс] : утв. постановлением Совета Безопасности Респ. Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

3. Концепция национальной безопасности Республики Беларусь [Электронный ресурс] : утв. Указом Президента Респ. Беларусь от 9 нояб. 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» : в ред. Указа Президента Респ. Беларусь от 24 янв. 2014 г. № 49 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

4. Положение о технической и криптографической защите информации [Электронный ресурс] : утв. Указом Президента Респ. Беларусь от 16 апр. 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» : в ред. Указа Президента Респ. Беларусь от 9 дек. 2019 г. № 449 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

5. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З : в ред. Закона Респ. Беларусь от 11 мая 2016 г. № 362-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

6. Атаманов, Г.А. Об информации, субъектах информационных отношений и информационном праве [Электронный ресурс] / Г.А. Атаманов // Защита информации. Инсайд. – 2011. – № 2. – Режим доступа: http://gatamanov.blogspot.com/2014/07/blog-post.html. – Дата доступа: 01.10.2020.

7. Раханов, К.Я. Синтез программно-аппаратной системы оценки разборчивости речи методом ЛЧМ-сигнала: результаты эксперимента // К.Я. Раханов // Вестн. Полоц. гос. ун-та. Сер. С, Фундаментальные науки. – 2012. – № 12. – С. 20–26.

8. Железняк, В.К. Применение стеклянных трубок на оконных ограждениях для увеличения защищенности речевой информации // В.К. Железняк, К.Я. Раханов, А.В. Казютин // Вестн. Полоц. гос. ун-та. Сер. С, Фундаментальные науки. – 2019. – № 4. – С. 32–39.

9. Модельный закон Об основах регулирования Интернета (новая редакция) [Электронный ресурс] : принят на сорок пятом пленарном заседании Межпарламентской ассамблеи государств-участников Содружества Независимых Государств в г. Санкт-Петербург (постановление № 45-12 от 25 нояб. 2016 г.) // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

10. Железняк, В.К. Методология научного исследования : пособие для магистрантов и аспирантов / В.К. Железняк, А.В. Барков, Д.С. Рябенко ; под общ. ред. В.К. Железняка. – Новополоцк : Полоц. гос. ун-т, 2018. – 88 с.

11. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты : учеб. пособие / Ю.А. Родичев. – СПб. : Питер, 2008. – 272 с.

12. О средствах массовой информации [Электронный ресурс] : Закон Респ. Беларусь от 17 июля 2008 г. № 427-З : в ред. Закона от 17 июля 2018 г. № 128-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

13. Рожкова, М.А. Об имущественных правах на нематериальные объекты в системе абсолютных прав (часть первая, вводная – вещные права, интеллектуальная собственность) [Электронный ресурс] / М.А. Рожкова // Закон.ру. – 17 дек. 2018 г. – Режим доступа: https://zakon.ru/blog/2018/12/17/ob_imuschestvennyh_pravah_na_nematerialnye_obekty_v_sisteme_absolyutnyh_prav_chast_pervaya_vvodnaya. – Дата доступа: 01.10.2020.

14. Раханов, К.Я. Методы оценки защищенности речевой информации / К.Я. Раханов, В.К. Железняк // Вестн. Полоц. гос. ун-та. Сер. С, Фундаментальные науки. – 2011. – № 12 – С. 2–8.

15. Раханов, К.Я. Оценка разборчивости речи взаимной корреляцией сигнала линейной частотной модуляции в каналах утечки информации // К.Я. Раханов, В.К. Железняк, И.Б. Бураченок // Вестн. Полоц. гос. ун-та. Сер. С, Фундаментальные науки. – 2015. – № 12. – С. 22–27.

16. Раханов, К.Я. Широкополосная линейно-частотная модуляция сигнала для оценки разборчивости речи в каналах утечки информации // К.Я. Раханов, В.К. Железняк / Изв. Нац. акад. наук Беларуси. Сер. физ.-техн. наук // редкол.: П.А. Вицязь (гл. ред.) [и др.]. – Минск : Беларус. навука, 2014. – С. 88–95.

17. Раханов, К.Я. Широкополосная линейно-частотная модуляция сигнала для оценки разборчивости речи в каналах утечки информации : автореф. дис. … канд. техн. наук : 05.13.19 / К.Я. Раханов ; Полоц. гос. ун-т ; Бел. гос. ун-т информатики и радиоэлектроники. – Минск, 2013. – 23 с.

18. Об электронном документе и электронной цифровой подписи [Электронный ресурс] : Закон Респ. Беларусь от 28 дек. 2009 № 113-З : в ред. Закона от 8 нояб. 2018 г. № 143-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

19. Положение о лицензировании отдельных видов деятельности [Электронный ресурс] : утв. Указом Президента Респ. Беларусь от 1 сент. 2009 № 450 «О лицензировании отдельных видов деятельности» : в ред. Указа Президента Респ. Беларусь от 31 дек. 2019 г. № 449 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

20. Положение о порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами) [Электронный ресурс] : утв. Указом Президента Респ. Беларусь от 16 февр. 2012 г. № 71 «О порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)» : в ред. Указа Президента Респ. Беларусь от 30 сент. 2020 г. № 355 //

ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

21. Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности [Электронный ресурс] : [вст. в силу для Респ. Беларусь 1 апр. 2019 г.] : утв. Указом Президента Респ. Беларусь от 27 апр. 2018 г. № 149 «Об утверждении международного договора» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

22. Биячуев, Т.А. Безопасность корпоративных сетей : учеб. пособие / Т.А. Биячуев ; под ред. Л.Г. Осовецкого. – СПб. : СПб ГУ ИТМО, 2004. – 161 с.

23. Егошин, Н.С. Формирование модели нарушителя / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Безопасность информационных технологий = IT Security. – 2017. – Т. 24, № 4. – С. 19–26.

24. Информационное право : учеб. / Г.А. Василевич [и др.] ; под общ. ред. Г.А. Василевича и Д.А. Плетенёва. – Минск : Адукацыя и выхаванне, 2015. – 392 с.

25. Пирогов, В.Ю. Информационные системы и базы данных: организация и проектирование : учеб. пособие / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2009. – 528 с.

26. О регистре населения [Электронный ресурс] : Закон Респ. Беларусь от 21 июля 2008 г. № 418-З : в ред. Закона Респ. Беларусь от 9 янв. 2019 г. № 170-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

27. О мерах по совершенствованию использования национального сегмента сети Интернет [Электронный ресурс] : Указ Президента Респ. Беларусь от 1 февр. 2010 г. № 60 : в ред. Указа Президента Респ. Беларусь от 18 сент. 2019 г. № 350 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

28. Об утверждении Инструкции о порядке формирования и хранения сведений о посещаемых пользователями интернет-услуг информационных ресурсах [Электронный ресурс] : пост. Министерства связи и информатизации Респ. Беларусь от 18 февр. 2015 г. № 6 : в ред. пост. Министерства связи и информатизации Респ. Беларусь от 16 авг. 2016 г. № 11 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

29. Савицкий, Т. Регулирование персональных данных в Беларуси: что нужно знать [Электронный ресурс] / Т. Савицкий // KV.by: Компьютерные вести. – 6 марта 2017 г. – Режим доступа: https://www.kv.by/post/1050760-regulirovanie-personalnyh-dannyh-v-belarusi-chto-nuzhno-znat. – Дата доступа: 01.10.2020.

30. Саванович, Н. Проект Закона о персональных данных: чего ожидать белорусскому бизнесу [Электронный ресурс] / Н. Саванович // Портал ilex.Новости. – Режим доступа: https://ilex.by/news/o-proekte-zakona-o-personalnyh-dannyh/. – Дата доступа: 01.10.2020.

31. О государственных секретах [Электронный ресурс]: Закон Респ. Беларусь от 19 июля 2010 г. № 170-З : в ред. Закона Респ. Беларусь от 17 июля 2018

№ 124-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

32. О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну [Электронный ресурс] : постановление Совета Министров Респ. Беларусь от 12 авг. 2014 г. № 783 : в ред. постановления Совета Министров Респ. Беларусь от 14 сент. 2020 г. № 533 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

33. О коммерческой тайне [Электронный ресурс] : Закон Респ. Беларусь от 5 янв. 2013 г. № 16-З : в ред. Закона Респ. Беларусь от 17 июля 2018 г. № 132-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

34. Гучек, О. Коммерческая тайна в IT: что, как и зачем? [Электронный ресурс] / О. Гучек // ООО «ЮС ИнвестЪ». – 8 июня 2017. – Режим доступа: http://usiminsk.by/pub/analitics/kommercheskaya_deyatelnost-kommercheskaya_tayna_v_it_chto_kak_i_zachem.html. – Дата доступа: 01.10.2020.

35. Овсейко, С. Соглашение о конфиденциальности: понятие и использование [Электронный ресурс] / С. Овсейко // АПС «Бизнес-Инфо» / ООО «Профессиональные правовые системы». – Минск, 2020.

36. Банковский кодекс Республики Беларусь [Электронный ресурс] : 25 окт. 2000 г. № 441-З : принят Палатой представителей 3 окт. 2000 г. : одобрен Советом Респ. 12 окт. 2000 г. : в ред. Закона от 17 июля 2018 г. № 133-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

37. Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация = Інфармацыйныя тэхналогіі. Метады і сродкі бяспекі. Інфармацыйныя сістэмы. Класіфікація [Электронный ресурс] : СТБ 34.101.30-2017. – Взамен СТБ 34.101.30-2007 ; введ. РБ 01.10.2017 // ЭТАЛОН-СТАНДАРТ / РУП «Белорус. гос. ин-т стандартизации и сертификации (БелГИСС), Национальный центр правовой информации. – Минск, 2020.

38. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация = Інфармацыйныя тэхналогіі. Метады і сродкі бяспекі. Аб’екты інфарматызацыі. Класіфікація [Электронный ресурс] : СТБ 34.101.30-2007. – Заменен СТБ 34.101.30-2017 ; введ. РБ 01.04.2008 ; срок действия 01.10.2017 // ЭТАЛОН-СТАНДАРТ / РУП «Белорус. гос. ин-т стандартизации и сертификации (БелГИСС), Национальный центр правовой информации. – Минск, 2020.

39. Положении о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено [Электронный ресурс] : утв. приказом Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 дек. 2019 г. № 449» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

40. Гражданский кодекс Республики Беларусь : 7 дек. 1998 г. № 218-З : принят Палатой представителей 28 окт. 1998 г. : одобрен Советом Респ. 19 ноября 1998 г. : в ред. Закона от 18 дек. 2019 г. № 277-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

41. Положение о порядке предварительной идентификации пользователей интернет-ресурса, сетевого издания [Электронный ресурс] : утв. постановлением Совета Министров Респ. Беларусь от 23 нояб. 2018 г. № 850 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

42. Рузова, И. Как избежать блокировки интернет-ресурса: правовой аспект [Электронный ресурс] / И. Рузова // АПС «Бизнес-Инфо» / ООО «Профессиональные правовые системы». – Минск, 2020.

43. Трудовой кодекс Республики Беларусь [Электронный ресурс] : 26 июля 1999 г. № 296-З : принят Палатой представителей 8 июня 1999 г. : одобрен Советом Респ. 30 июня 1999 г. : в ред. Закона от 18 июля 2019 г. № 124-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

44. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 г. № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

45. Введение в защиту информации от внутренних IT-угроз (Лекция 4. Нетехнические меры защиты. Уровни контроля информационных потков) [Электронный ресурс] / Компания InfoWatch // Национальный открытый институт «ИНТУИТ». – Режим доступа: https://www.intuit.ru/studies/courses/1013/172/lecture/4686. – Дата доступа: 01.10.2020.

46. Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Кодэкс практыкі для менеджменту інфармацыйнай бяспекі [Электронный ресурс] : СТБ ISO/IEC 27002-2012. – Введен впервые; введ. РБ 01.01.2013 // ЭТАЛОН-СТАНДАРТ / РУП «Белорус. гос. ин-т стандартизации и сертификации (БелГИСС), Национальный центр правовой информации. – Минск, 2020.

47. Власова, Л.А. Защита информации : учеб. пособие / Л.А. Власова. – Хабаровск : РИЦ ХГАЭП, 2007. – 84 с.

48. Об утверждении Положения о порядке определения уполномоченных поставщиков интернет-услуг : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 2 авг. 2010 г. № 60 : в ред. Приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 6 дек. 2019 г. № 408 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

49. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Сістэмы менеджменту інфармацыйнай бяспекі. Агульны агляд і слоўнік [Электронный ресурс] : СТБ ISO/IEC 27000-2012. – Введен впервые; введ. РБ 01.01.2013 // ЭТАЛОН-СТАНДАРТ / РУП «Белорус. гос. ин-т стандартизации и сертификации (БелГИСС), Национальный центр правовой информации. – Минск, 2020.

50. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Сістэмы менеджменту інфармацыйнай бяспекі. Патрабаванні [Электронный ресурс] : СТБ ISO/IEC 27001-2016. – Взамен СТБ ISO/IEC 27001-2011; введ. РБ 01.10.2016 // ЭТАЛОН-СТАНДАРТ / РУП «Белорус. гос. ин-т стандартизации и сертификации (БелГИСС), Национальный центр правовой информации. – Минск, 2020.

51. Об утверждении Правил подтверждения соответствия Национальной системы подтверждения соответствия Республики Беларусь [Электронный ресурс] : постановление Гос. комитета по стандартизации Респ. Беларусь от 25 июля 2017 г. № 61 : в ред. пост. Гос. комитета по стандартизации Респ. Беларусь от 20 нояб. 2018 г. № 64 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

52. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

53. Пулко, Т.А. Введение в информационную безопасность : учеб. пособие / Т.А. Пулко. – Минск : БГУИР, 2016. – 164 с.

54. Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) [Электронный ресурс] : постановление Совета Министров Респ. Беларусь от 15 мая 2013 г. № 375 : в ред. пост. Совета Министров Респ. Беларусь от 12.03.2020 №145 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

55. О подтверждении соответствия средств защиты информации [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 12 марта 2020 г. № 77 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

56. Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено [Электронный ресурс] : утв. приказом Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

57. Положение о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях нформационной безопасности, состоянии технической и криптографической защиты информации [Электронный ресурс] : утв. приказом Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

58. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель = Інфармацыйныя тэхналогіі і бяспека. Крытэрыі ацэнкі бяспекі інфармацыйных тэхналогій. Частка 1. Уводзіны і агульная мадэль : СТБ 34.101.1-2014 (ISO/IEC 15408-1:2009). – Взамен СТБ 34.101.1-2004 (ИСО/МЭК 15408-1:1999) ; введ. РБ 01.09.2014 // ЭТАЛОН-СТАНДАРТ / РУП «Белорус. гос. ин-т стандартизации и сертификации (БелГИСС), Национальный центр правовой информации. – Минск, 2020.

59. О поддержке малого и среднего предпринимательства [Электронный ресурс] : Закон Респ. Беларусь от 1 июля 2010 г. № 148-З : в ред. Закона Респ. Беларусь от 9 янв. 2018 г. №91-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

60. Ивайкина, В. GDPR один год: практика и перспективы применения [Электронный ресурс] / В. Ивайкина, Т. Савицкий // Портал ilex.Новости / ООО «ЮрСпектр». – Режим доступа: https://ilex.by/news/gdpr-odin-god-praktika-i-perspektivy-primeneniya/. – Дата доступа: 01.10.2020.

61. Воронкевич, С. Семь шагов для подготовки к новому Европейскому регламенту защиты персональных данных [Электронный ресурс] / С. Воронкевич // Dev.by. – 14 сент. 2017 г. – Режим доступа: https://dev.by/news/global-data-protection-regulation. – Дата доступа: 01.10.2020.

62. Бонина, Е. С 25 мая – штрафы до 20 млн евро за пренебрежение к персональным данным пользователей [Электронный ресурс] / Е. Бонина, Г. Маевский // TUT.BY. – 29 марта 2018 г. – Режим доступа: https://news.tut.by/economics/586863.html. – Дата доступа: 01.10.2020.

63. Выписан рекордный штраф за нарушение регламента по защите данных GDPR [Электронный ресурс] // Информационно-коммуникационный ресурс «DailyComm». – 8 июля 2019 г. – Режим доступа: http://www.dailycomm.ru/m/47866/. – Дата доступа: 01.10.2020.

64. Сикорски М. Вскрытие покажет! Практический анализ вредоносного ПО / М. Сикорски, Э. Хониг. – СПб. : Питер, 2018. – 768 с.

65. Холмогоров, В. PRO ВИРУСЫ / В. Холмогоров. – 2-е изд. – СПб. : Страта, 2017 – 162 с.

66. ESET: 99% мобильных вредоносов нацелены на ОС Android [Электронный ресурс] // ESET. 31.01.2020 / ООО «ИСЕТ Софтвеа». – Режим доступа: https://www.esetnod32.ru/company/press/center/eset-99-mobilnykh-vredonosov-natseleny-na-os-android/. – Дата доступа: 01.10.2020.

67. Борисевич, М.Н. Основы информационный технологий [Электронный ресурс] : учеб. / М.Н. Борисевич // Витеб. Ордена «Знак Почета» гос. акад. вет. медицины. – Режим доступа: http://www.vsavm.by/knigi/kniga3/. – Дата доступа: 01.10.2020.

68. Прохорова, О.В. Информационная безопасность и защита информации : учеб. / О.В. Прохорова. – Самара : СГАСУ, 2014. – 114 с.

69. Доказательство с нулевым разглашением [Электронный ресурс] // Википедия. Свободная энциклопедия / Wikimedia Foundation, Inc. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE_%D1%81_%D0%BD%D1%83%D0%BB%D0%B5%D0%B2%D1%8B%D0%BC_%D1%80%D0%B0%D0%B7%D0%B3%D0%BB%D0%B0%D1%88%D0%B5%D0%BD%D0%B8%D0%B5%D0%BC#%D0%9F%D0%B5%D1%89%D0%B5%D1%80%D0%B0_%D0%BD%D1%83%D0%BB%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%80%D0%B0%D0%B7%D0%B3%D0%BB%D0%B0%D1%88%D0%B5%D0%BD%D0%B8%D1%8F. – Дата доступа: 01.10.2020.

70. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – М. : Пресс, 2008. – 448 с.

71. Платонов, В.В. Программно-аппаратные средства защиты информации : учеб. / В.В. Платонов. –М. : Академия, 2013. – 336 с.

72. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.]. – М. : Радио и связь, 2000. – 192 с.

73. Смит, Р.Ф. Демилитаризованная зона ISA [Электронный ресурс] / Р.Ф. Смит // OSP. 20.04.2006 / Открытые системы. – Режим доступа: https://www.osp.ru/winitpro/2006/03/1156406. – Дата доступа: 01.10.2020.

74. Santiago Pontiroli. Социальная инженерия, или Как взломать человека [Электронный ресурс] / Santiago Pontiroli // Kaspersky Daily. – 20 дек. 2013 г. – Режим доступа: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/. – Дата доступа: 01.10.2020.

75. Кузнецов, М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов. – СПб. : БХВ-Петербург, 2007. – 368 с.

76. Ваш паспорт в чужих руках [Электронный ресурс] // CERT.BY. – 23.07.2020. – Режим доступа: https://cert.by/?p=1681. – Дата доступа: 01.10.2020.

77. Белорусские паспорта в DarkNet [Электронный ресурс] // CERT.BY. – 10.07.2020. – Режим доступа: https://cert.by/?p=1655. – Дата доступа: 01.10.2020.

78. Фишинг (Phishing) [Электронный ресурс] // TAdvizer. – 09.07.2020. – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3_(phishing)#.D0.9A.D0.B0.D0.BB.D0.B5.D0.BD.D0.B4.D0.B0.D1.80.D0.BD.D1.8B.D0.B9_.D1.84.D0.B8.D1.88.D0.B8.D0.BD.D0.B3. – Дата доступа: 01.10.2020.

79. Эксплуатация киберпреступниками темы COVID-19 [Электронный ресурс] // CERT.BY. – 10.07.2020. – Режим доступа: https://cert.by/?p=1584. – Дата доступа: 01.10.2020.

80. Фильтрация DNS в домене Windows на примере OpenDNS [Электронный ресурс] // WinITPro.ru. – 09.01.2020. – Режим доступа: https://winitpro.ru/index.php/2013/09/30/filtraciya-dns-v-domene-windows-na-primere-opendns/. – Дата доступа: 01.10.2020.

81. Мазур, С. Тайпо-домены: что это такое, и зачем нужно их регистрировать [Электронный ресурс] / С. Мазур // Community by Timeweb. – 25.10.2019. – Режим доступа: https://timeweb.com/ru/community/articles/taypo-domeny-chto-eto-takoe-i-zachem-nuzhno-ih-registrirovat-1. – Дата доступа: 01.10.2020.

82. Что такое фарминг и как с ним бороться [Электронный ресурс] // SecurityLab.ru. – 18.04.2019. – Режим доступа: https://www.securitylab.ru/blog/company/PandaSecurityRus/346155.php#:~:text=%D0%A4%D0%B0%D1%80%D0%BC%D0%B8%D0%BD%D0%B3%20%E2%80%93%20%D1%8D%D1%82%D0%BE%20%D0%B2%D0%B8%D0%B4%20%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0%2C%20%D0%BF%D1%80%D0%B8,%D0%B1%D0%B5%D0%B7%20%D0%B8%D1%85%20%D0%B2%D0%B5%D0%B4%D0%BE%D0%BC%D0%B0%20%D0%B8%20%D1%81%D0%BE%D0%B3%D0%BB%D0%B0%D1%81%D0%B8%D1%8F. – Дата доступа: 01.10.2020.

83. Новая кампания по заражению вредоносным ПО [Электронный ресурс] // CERT.BY. – 10.07.2020. – Режим доступа: https://cert.by/?p=1807. – Дата доступа: 01.10.2020.

84. How to Protect Insiders from Social Engineering Threats [Electronic resource] // Docs.microsoft.com / Microsoft . – Mode of access: https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10)?redirectedfrom=MSDN. – Date of access: 01.10.2020.

85. Reverse Social Engineering Attacks in Online Social Networks [Electronic resource] / Davide Balzarotti [et al.] // ResearchGate. –July 2011. – Mode of access: https://www.researchgate.net/publication/221394370_Reverse_Social_Engineering_Attacks_in_Online_Social_Networks. – Date of access: 01.10.2020.

86. What is Reverse Social Engineering? And How Does It Work? [Electronic resource] // OHPHISH. – August 12, 2020. – Mode of access: https://ohphish.eccouncil.org/what-is-reverse-social-engineering.html. – Date of access: 01.10.2020.

87. Социальная инженерия [Электронный ресурс] // 4BRAIN. – Режим доступа: https://4brain.ru/blog/%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F-%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F/. – Дата доступа: 01.10.2020.

88. Social engineering (security) [Electronic resource] // Wikipedia, the free encyclopedia / Wikimedia Foundation, Inc. – Mode of access: https://en.wikipedia.org/wiki/Social_engineering_(security). – Date of access: 01.10.2020.

89. Chris, Romeo. 6 ways to develop a security culture from top to bottom [Electronic resource] / Chris Romeo // TechBeacon. – Mode of access: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom. – Date of access: 01.10.2020.

90. В 2018 году в России 90% утечек конфиденциальной информации случились в результате внутренних нарушений, самыми уязвимыми стали государственные и муниципальные организации [Электронный ресурс] // INFOWATCH. – 30 мая 2019 г. – Режим доступа: https://www.infowatch.ru/company/presscenter/news/15706. – Дата доступа: 01.10.2020.

91. Малюк, А.А. Зарубежный опыт формирования в обществе культуры информационной безопасности / А.А. Малюк, О.Ю. Полянская // Безопасность информационных технологий. – 2016. – № 4 – С. 25–37.

92. Городилов, С. Культура информационной безопасности – современный взгляд / С. Городилов // Меркурий. – 2012. – № 159, июль. – С. 4.

93. Создание глобальной культуры кибербезопасности [Электронный ресурс] : Резолюция Генеральной Ассамблеи ООН от 31.01.2003, A/RES/57/239 / Организация объединенных наций. – Режим доступа: https://undocs.org/ru/A/RES/57/239. – Дата доступа: 01.10.2020.

94. Петренко, С.А. Оценка затрат на защиту инфорации [Электронный ресурс] / С.А. Петренко, Е.М. Терехова // Защита информации. Инсайд. – 2005. – № 1. – Режим доступа: http://www.inside-zi.ru/pages/1_2005/23.html. – Дата доступа: 01.10.2020.

95. Петренко, С.А. Политики безопасности компании при работе в Интернет / С.А. Петренко, В.А. Курбатов. – Саратов : Профобразование, 2017. – 397 с.

96. Минзов, А.С. Методика обоснования затрат на обеспечение системы информационной безопасности хозяйствующего субъекта / А.С. Минзов, С.М. Кольер // Вестн. Акад. экон. безопасности МВД России. – 2010. – № 4. – С. 12–18.

97. Цуканова, О.А. Экономика защиты информации : учебное пособие / О.А. Цуканова, С.Б. Смирнов. – 2-е изд., изм. и доп. – СПб. : НИУ ИТМО, 2014. – 79 с.

ПРИЛОЖЕНИЕ 1

Перечень технических нормативных правовых актов (серия СТБ 34.101)

1. СТБ 34.101.1-2014 (ISO/IEC 15408-1:2009) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель : введен 01.09.2014.

2. СТБ 34.101.2-2014 (ISO/IEC 15408-2:2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности : введен 01.09.2014.

3. СТБ 34.101.3-2014 (ISO/IEC 15408-3:2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности : введен 01.09.2014.

4. СТБ 34.101.8-2006 Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования : введен 01.07.2006.

5. СТБ 34.101.9-2004 Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы : введен 01.09.2004.

6. СТБ 34.101.10-2004 Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования : введен 01.09.2004.

7. СТБ 34.101.11-2009 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль

8. защиты операционной системы сервера для использования в доверенной зоне корпоративной сети : введен 01.09.2009.

9. СТБ 34.101.12-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества : введен 01.10.2007.

10. СТБ 34.101.13-2009 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в демилитаризованной зоне корпоративной сети : введен 01.09.2009.

11. СТБ 34.101.14-2017 Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования : введен 01.04.2018.

12. 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 : введен 01.11.2007.

13. СТБ 34.101.16-2009 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств коммутатора для использования в доверенной зоне корпоративной сети : введен 01.08.2009.

14. СТБ 34.101.17-2012 Информационные технологии и безопасность. Синтаксис запроса на получение сертификата : введен 01.08.2012.

15. СТБ 34.101.18-2009 Информационные технологии. Синтаксис обмена персональной информацией : введен 01.09.2009.

16. СТБ 34.101.19-2012 Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей : введен 01.08.2012.

17. СТБ 34.101.20-2009 Информационные технологии. Синтаксис криптографической информации для токенов : введен 01.09.2009.

18. СТБ 34.101.21-2009 Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном) : введен 01.09.2009.

19. СТБ 34.101.22-2009 Информационные технологии. Криптография на основе алгоритма RSA : введен 01.09.2009.

20. СТБ 34.101.23-2012 Информационные технологии и безопасность. Синтаксис криптографических сообщений : введен 01.08.2012.

21. СТБ 34.101.26-2012 Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP) : введен 01.08.2012.

22. СТБ 34.101.27-2011 Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации : введен 01.03.2012.

23. СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация : введен 01.10.2017.

24. СТБ 34.101.31-2011 Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности : введен 01.07.2011.

25. СТБ 34.101.35-2011 Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты класса Б3 : введен 01.03.2012.

26. СТБ 34.101.36-2011 Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты класса А2 : введен 01.03.2012.

27. СТБ 34.101.37-2017 Информационные технологии и безопасность. Методы и средства безопасности. Системы управления сайта. Общие требования : введен 01.04.2018.

28. СТБ 34.101.41-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения : введен 01.07.2014.

29. СТБ 34.101.42-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности : введен 01.07.2014.

30. СТБ 34.101.45-2013 Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых : введен 01.01.2014.

31. СТБ 34.101.47-2017 Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел : введен 01.09.2017.

32. СТБ 34.101.48-2012 Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров : введен 01.08.2012.

33. СТБ 34.101.49-2012 Информационные технологии и безопасность. Формат карточки открытого ключа : введен 01.08.2012.

34. СТБ 34.101.50-2019 Информационные технологии и безопасность. Правила регистрации объектов информационных технологий : введен 01.10.2019.

35. СТБ 34.101.52-2016 Информационные технологии. Методы и средства безопасности. Критически важные объекты информатизации. Классификация : введен 01.04.2017.

36. СТБ 34.101.53-2016 Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса А1-у : введен 01.04.2017.

37. СТБ 34.101.54-2016 Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса А2-у : введен 01.04.2017.

38. СТБ 34.101.55-2016 Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса Б1-у : введен 01.04.2017.

39. СТБ 34.101.56-2016 Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса Б2-у : введен 01.04.2017.

40. СТБ 34.101.57-2016 Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса В1-у : введен 01.04.2017.

41. СТБ 34.101.58-2016 Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса В2-у : введен 01.04.2017.

42. СТБ 34.101.59-2016 Информационные технологии и безопасность. Задание по безопасности. Методические указания по разработке : введен 01.04.2017.

43. СТБ 34.101.60-2014 Информационные технологии и безопасность. Алгоритмы разделения секрета : введен 01.09.2014.

44. СТБ 34.101.61-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности : введен 01.07.2014.

45. СТБ 34.101.62-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41 : введен 01.07.2014.

46. СТБ 34.101.65-2014 Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS) : введен 01.09.2014.

47. СТБ 34.101.66-2014 Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых : введен 01.09.2014.

48. СТБ 34.101.67-2014 Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов : введен 01.09.2014.

49. СТБ 34.101.68-2013 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41 : введен 01.07.2014.

50. СТБ 34.101.69-2014 Информационные технологии и безопасность. Криптология. Термины и определения : введен 01.02.2015.

51. СТБ 34.101.70-2016 Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах : введен 01.04.2017.

52. СТБ 34.101.72-2018 Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций : введен 01.08.2018.

53. СТБ 34.101.73-2017 Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования : введен 01.01.2018.

54. СТБ 34.101.74-2017 Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования : введен 01.10.2017.

55. СТБ 34.101.75-2017 Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования : введен 01.10.2017.

56. СТБ 34.101.76-2017 Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования : введен 01.04.2018.

57. СТБ 34.101.77-2016 Информационные технологии и безопасность. Алгоритмы хэширования : введен 01.10.2016.

58. СТБ 34.101.78-2019 Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей : введен 01.10.2019.

59. СТБ 34.101.79-2019 Информационные технологии и безопасность. Криптографические токены : введен 01.10.2019.

60. СТБ 34.101.80-2019 Информационные технологии и безопасность. Расширенные электронные цифровые подписи : введен 01.10.2019.

61. СТБ 34.101.81-2019 Информационные технологии и безопасность. Протоколы службы заверения данных : введен 01.10.2019.

62. СТБ 34.101.82-2019 Информационные технологии и безопасность. Протокол постановки штампа времени : введен 01.10.2019.

ПРИЛОЖЕНИЕ 2

Перечень технических нормативных правовых актов в области (серия СТБ ISO/IEC 27000)

1. СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь : введен 01.01.2013.
2. СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования : введен 01.10.2016.
3. СТБ ISO/IEC 27002-2012 Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности : введен 01.01.2013.
4. СТБ ISO/IEC 27003-2014 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности : введен 01.02.2015.
5. СТБ ISO/IEC 27004-2014 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения : введен 01.02.2015.
6. СТБ ISO/IEC 27005-2012 Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности : введен 01.01.2013.
7. СТБ ISO/IEC 27006-2018 Информационные технологии. Методы обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности : введен 01.05.2018.

ПРИЛОЖЕНИЕ 3

Перечень основных нормативных правовых актов в сфере технической и криптографической защиты информации и по вопросам регулирования национального сегмента сети Интернет

1. Концепция национальной безопасности Республики Беларусь : утв. Указом Президента Респ. Беларусь от 9 нояб. 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» : в ред. Указа Президента Респ. Беларусь от 24 янв. 2014 г. №49.

2. Концепция информационной безопасности : утв. постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь».

3. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З : в ред. Закона Респ. Беларусь от 11 мая 2016 г. № 362-З.

4. О регистре населения [Электронный ресурс] : Закон Респ. Беларусь от 21 июля 2008 г. № 418-З : в ред. Закона Респ. Беларусь от 9 янв. 2019 г. № 170-З.

5. О государственных секретах : Закон Респ. Беларусь от 19 июля 2010 г. № 170-З : в ред. Закона Респ. Беларусь от 17 июля 2018 № 124-З.

6. О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну : постановление Совета Министров Респ. Беларусь от 12 августа 2014 года № 783: в ред. постановления Совета Министров Респ. Беларусь от 14 сент. 2020 г. № 533.

7. О коммерческой тайне : Закон Респ. Беларусь от 5 янв. 2013 г. № 16-З : в ред. Закона Респ. Беларусь от 17 июля 2018 г. № 132-З.

8. Гражданский кодекс Республики Беларусь : 7 дек. 1998 г. № 218-З : принят Палатой представителей 28 октября 1998 г. : одобрен Советом Респ. 19 ноября 1998 г. : в ред. Закона от 18 дек. 2019 г. № 277-З.

9. О мерах по совершенствованию использования национального сегмента сети Интернет : Указ Президента Респ. Беларусь от 1 февр. 2010 г. № 60 : в ред. Указа Президента Респ. Беларусь от 18 сент. 2019 г. № 350.

10. Об утверждении Инструкции о порядке формирования и хранения сведений о посещаемых пользователями интернет-услуг информационных ресурсах : постановление М-ва связи и информатизации Респ. Беларусь от 18 февр. 2015 г. № 6 : в ред. постановления М-ва связи и информатизации Респ. Беларусь от 16 авг. 2016 г. № 11.

11. О некоторых вопросах совершенствования использования национального сегмента глобальной компьютерной сети Интернет : постановление Совета Министров Респ. Беларусь от 29 апр. 2010 г. № 644 : в ред постановления Совета Министров Респ. Беларусь от 20 дек. 2019 г.

12. Об утверждении Положения о порядке ограничения (возобновления) доступа к интернет-ресурсу : постановление Оперативно-аналитического центра при Президенте Респ. Беларусь, М-ва связи и информатизации Респ. Беларусь, М-ва информации Респ. Беларусь от 3 окт. 2018 г. № 8/10/16.

13. О некоторых мерах по совершенствованию защиты информации : Указ Президента Респ. Беларусь от 16 апр. 2013 г. № 196 : в ред. Указа Президента Респ. Беларусь от 9 дек. 2019 г. № 449.

14. О совершенствовании государственного регулирования в области защиты информации : Указ Президента Респ. Беларусь от 9 дек. 2019 г. № 449.

15. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 г. № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

16. Положение о лицензировании отдельных видов деятельности : утв. Указом Президента Респ. Беларусь от 1 сент. 2009 № 450 «О лицензировании отдельных видов деятельности» : в ред. Указа Президента Респ. Беларусь от 31 дек. 2019 г. № 449.

17. Положение о порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами) : утв. Указом Президента Респ. Беларусь от 16 февр. 2012 г. № 71 «О порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)» : в ред. Указа Президента Респ. Беларусь от 30 сент. 2020 г. № 355.

18. Об утверждении Инструкции о порядке проведения оценки соответствия возможностей соискателя лицензии (лицензиата) лицензионным требованиям и условиям : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 30 нояб. 2010 г. № 86 : в ред. Приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 9 окт. 2019 г.

19. Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) : постановление Совета Министров Респ. Беларусь от 15 мая 2013 г. № 375 : в ред. постановления Совета Министров Респ. Беларусь от 12 марта 2020 г. № 145.

20. Об утверждении Положения о порядке проведения государственной экспертизы средств технической и криптографической защиты информации : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 26 авг. 2013 г. № 60 : в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февр. 2020 г.

21. Об утверждении Инструкции о порядке согласования выполнения работ и (или) оказания услуг, составляющих деятельность по технической и (или) криптографической защите информации, в государственных органах и государственных организациях : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 16 нояб. 2010 г. № 82 : в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 9 окт. 2019 г. № 336.

22. Об утверждении Правил подтверждения соответствия Национальной системы подтверждения соответствия Республики Беларусь: постановление Гос. комитета по стандартизации Респ. Беларусь от 25 июля 2017 г. № 61 : в ред. постановления Гос. ком. по стандартизации Респ. Беларусь от 20 нояб. 2018 г. №64.

23. О подтверждении соответствия средств защиты информации [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 12 марта 2020 г. № 77 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

24. Об утверждении Положения о порядке определения уполномоченных поставщиков интернет-услуг : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 2 авг. 2010 г. № 60 : в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 6 дек. 2019 г. № 408.

Учебное издание

РАХАНОВ Константин Яковлевич
РАХАНОВА Надежда Александровна

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Рекомендовано учебно-методическим объединением по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-40 80 04 «Информатика и технологии программирования»

Редактор *Т. А. Дарьянова*
Дизайн обложки *Е. А. Балабуевой*

Подписано в печать 16.02.2021. Формат 60x84 1/16. Бумага офсетная.
Ризография. Усл. печ. л. 11,14. Уч.-изд. л. 10,81. Тираж 30 экз. Заказ 28.

Издатель и полиграфическое исполнение –
учреждение образования «Полоцкий государственный университет».

Свидетельство о государственной регистрации
издателя, изготовителя, распространителя печатных изданий
№ 1/305 от 22.04.2014.

Ул. Блохина, 29, 211440, г. Новополоцк.