Я. С. Гродзенский

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УЧЕБНОЕ ПОСОБИЕ

• ПРОСПЕКТ •
Москва
2020

УДК 004.056(075.8)
ББК 32.973-018.2я73
Г86

Автор:
Гродзенский Я. С., кандидат технических наук, доцент МИРЭА — Российского технологического университета.

Гродзенский Я. С.

Г86 Информационная безопасность : учебное пособие. – Москва : РГ-Пресс, 2020. – 144 с.

ISBN 978-5-9988-0845-6
DOI 10.31085/9785998808456-2020-144

В учебном пособии согласно требованиям государственных образовательных стандартов рассматриваются вопросы обеспечения информационной безопасности предприятий. Целью данного пособия является знакомство читателя с основными понятиями в области информационной безопасности, угрозами и методами реагирования, а также международными и национальными стандартами в области информационной безопасности, в основу которых положен мировой опыт борьбы с киберпреступлениями.

Материал, составивший содержание пособия, соответствует программам курсов «Информационная безопасность», «Защита информации», читаемых студентам и магистрантам.

Предназначено для студентов, обучающихся по техническим и экономическим специальностям и направлениям, преподавателей технических вузов, менеджеров, экономистов и инженеров. Может быть использовано при подготовке кадров, а также при повышении квалификации специалистов.

УДК 004.056(075.8)
ББК 32.973-018.2я73

Изображение на обложке foxaon1987/Shutterstock.com

Учебное издание

Гродзенский Яков Сергеевич

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Подписано в печать 20.12.2019. Формат 60×90 $^{1}/_{16}$.
Печать цифровая. Печ. л. 9,0. Тираж 500 (1-й завод 100) экз. Заказ №

ISBN 978-5-9988-0845-6
DOI 10.31085/9785998808456-2020-144

Ya. S. Grodzenskiy

INFORMATION SECURITY

TUTORIAL

• PROSPEKT •
Moscow
2020

Author:
Grodzenskiy Ya. S., Candidate of Engineering Sciences, Associate Professor of the MIREA — Russian Technological University.

Grodzenskiy Ya. S.

Information Security : Tutorial. — Moscow : RG-Press, 2020. – 144 p.

ISBN 978-5-9988-0845-6

DOI 10.31085/9785998808456-2020-144

This study guide is focused on information security basics. The reader will be introduced to the key information security notions along with the classification of information security practices. The book covers, among other topics, personal data protection, measures against unauthorized access, prevention of data leaks through technical communication channels, cryptographic information protection, and network security. Particular attention is given to information security risk assessment and ISO 27001 standard.

This book is designed for students learning information security basics as well as for a wide range of readers taking interest in the information security sphere.

ISBN 978-5-9988-0845-6
DOI 10.31085/9785998808456-2020-144

СПИСОК ОСНОВНЫХ СОКРАЩЕНИЙ

АРМ — автоматизированное рабочее место
АС — автоматизированные системы
ИБ — информационная безопасность
ИСПДн — информационная система персональных данных
ИТ — информационные технологии
КИИ — критическая информационная инфраструктура
МСЭ — межсетевые экраны
НСД — несанкционированный доступ к информации
ПО — программное обеспечение
ПЭМИН — побочные электромагнитные излучения и наводки
РД — руководящий документ
СВТ — средства вычислительной техники
СЗИ — средства защиты информации
СКЗИ — средства криптографической защиты информации
СКУД — системы контроля и управления доступом
СМИБ — система менеджмента информационной безопасности
СТР-К — специальные требования и рекомендации по технической защите конфиденциальной информации
СУИБ — система управления информационной безопасностью
ФЗ — федеральный закон
ФСТЭК — Федеральная служба по техническому и экспертному контролю

ВВЕДЕНИЕ

Бурное развитие отрасли информационных технологий, подобно гигантской океанской волне, несет с собой как большие возможности, так и серьезные угрозы, прежде всего, угрозы информационной безопасности (ИБ). По данным Центра стратегических и международных исследований (*англ*. The Center for Strategic and International Studies) США, в 2014 году объем убытков от киберпреступлений составил 445 миллиардов долларов США, в 2017 году, по данным компании McAfee, приблизился к 600 миллиардам, а в 2021 году убытки от киберпреступности, согласно прогнозам Cybersecurity Ventures, могут подняться до 6 триллионов.

Количество зафиксированных инцидентов ИБ в 2013 году превысило 42 миллиона, т.е. в среднем происходило более 115 тысяч кибератак в день. В течение 2016 года было заблокировано более 81 миллиарда угроз только решениями японской компании — разработчика программного обеспечения для кибербезопасности *Trend Micro*, что на 56% больше, чем годом раньше, т.е. каждую секунду блокировалось примерно три тысячи атак.

Россия стабильно входит в тройку стран, на территории которых детектируется наибольшее число кибератак. В середине 2017 года по данным лаборатории Касперского количество обнаруживаемых атак составляло около 300 в секунду. Изменилась и картина киберпреступлений. Если на рубеже XX и XXI веков основную угрозу представляли компьютерные вирусы, то сейчас это в первую очередь атаки на веб-приложения, целенаправленные (*англ*. Advanced Persistent Threat) угрозы мобильным устройствам.

В учебных программах многих вузов появилась дисциплина «Информационная безопасность», по которой один за другим выходят учебники и монографии, укажем только на несколько, что появились в последнее время [1–5]. Целью данного учебного пособия является знакомство читателя с основными понятиями в области ИБ, угрозами ИБ и методами реагирования, а также международными и национальными стандартами в этой области, в основу которых положен мировой опыт борьбы с киберпреступлениями.

Основной материал пособия изложен в 16 разделах. В первом даются понятия и основные принципы ИБ, классификация методов обе-

спечения ИБ. Обзор современных национальных и международных стандартов в области ИБ приведен во втором разделе. В третьем рассказывается об особенностях обработки персональных данных в соответствии с законодательством Российской Федерации, а в четвертом речь пойдет о способах несанкционированного доступа к информации и методах его предотвращения. Пятый раздел знакомит с понятием утечки информации по техническим каналам и борьбы с инцидентами такого рода. О понятии криптографии и о методах криптографической защиты идет речь в шестом разделе. В седьмом разделе читатель познакомится с понятием электронной подписи, областями ее применения и техническим обеспечением ее использования. Восьмой раздел посвящен управлению уязвимостями ИБ. Одной из наиболее важных составляющих ИБ является сетевая безопасность, которой посвящен девятый раздел.

Неправильно написанное или сконфигурированное веб-приложение может стать для злоумышленника способом получить данные о ее клиентах. Как предотвратить инциденты такого характера? Об этом — десятый раздел. Мобильные устройства стали неотъемлемой частью работы для большинства людей. Об угрозах, подстерегающих пользователей мобильных устройств, и борьбе с ними — одиннадцатый раздел. Двенадцатый раздел посвящен самому важному аспекту для компаний — защите информации ограниченного доступа, включая коммерческую тайну. Нормативная база, а также технические методы защиты информации компаний рассматриваются в этом разделе. Отдельное место занимают вопросы обеспечения ИБ в промышленном производстве и управлении качеством, где цена ошибки может быть очень высока.

Об основных угрозах ИБ, возникающих на производстве, и методах борьбы с ними, а также о методах обеспечения ИБ в управлении качеством читайте в тринадцатом разделе. В связи с принятием Федерального закона от 26.07.2017 187-ФЗ о безопасности критической информационной инфраструктуры (КИИ) стала весьма актуальной и эта тема, ей посвящен четырнадцатый раздел. Вопросы анализа рисков ИБ чрезвычайно важны, поскольку дают возможность объективно оценить угрозы и распределить усилия и ресурсы для защиты от них. Читайте об этом в пятнадцатом разделе. Основным стандартом в области ИБ является ISO 27001. В шестнадцатом разделе можно узнать о том, что должны предпринять организации для соответствия этому стандарту.

1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ). ОСНОВНЫЕ ПРИНЦИПЫ ИБ. ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. КЛАССИФИКАЦИЯ МЕТОДОВ И МЕР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Отрасль ИБ в России формируется под влиянием двух основных факторов — мировых тенденций развития информационных технологий (ИТ) и меняющегося, в связи с этим характера киберугроз. Серьезную роль на вектор развития отрасли оказывают также изменения российского законодательства и международных стандартов. Количество нормативно-правовых документов в России, касающихся только банковской сферы, приближается к 150. Существует и множество разнообразных стандартов в области ИБ. При этом надо отметить, что многие из международных стандартов ИСО (Международной организации по стандартизации) и МЭК (Международной электротехнической комиссии) нашли свое применение в российской системе стандартизации.

Не стал исключением и ГОСТ Р ИСО/МЭК 17799-2005 — «Практические правила управления информационной безопасностью». В соответствии с этим стандартом ИБ — это защита конфиденциальности, целостности и доступности информации. Разберем эти три свойства ИБ. Конфиденциальность информации — это обеспечение доступа к информации только авторизованным пользователям.

Необходимо отметить, что конфиденциальная информация — это вполне юридически значимое понятие, которое нашло свое отражение как в различных национальных стандартах, так и в законодательных актах. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07. 2006 № 149-ФЗ в статье 5 говорит, что «Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)». В статье 7 этого закона дано следу-

ющее определение общедоступной информации. «К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен».

Общедоступная информация делится на информацию, доступ к которой не может быть ограничен, т.е. которая в соответствии с законодательством должна быть общедоступной, например, на основании «Правил отнесения информации к общедоступной информации, размещаемой государственными органами и органами местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных», утвержденными Постановлением Правительства РФ от 10.07.2013 № 583 и ту, которую общедоступной делают физические и юридические лица по собственному желанию. Так, размещая резюме в открытых источниках, вы по собственному желанию делаете свои персональные данные общедоступными.

Что касается информации ограниченного доступа, то в российском законодательстве упоминается более 50 видов тайн (видов информации ограниченного доступа). Их перечень приводится в Приложении № 1. Эти виды тайн (информации ограниченного доступа) относятся или к конфиденциальной информации или государственной тайне. В свою очередь конфиденциальная информация подразделяется на:

— персональные данные;
— коммерческую тайну;
— служебную тайну;
— профессиональную тайну.

Целостность информации — это состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. Одним из известных способов проверки целостности информации является использование хэш-функции (*англ.* hash function от hash — «превращать в фарш», «мешанина» https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F - cite_note-_ff142c473b3a285a-1) — функции, осуществляющей преобразование массива входных данных произвольной длины в выходную установленной длины, выполняемое определенным алгоритмом. Об этом подробно рассказывается в разделе 7.

Доступность информации — это состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно, но в рамках предоставленных им прав. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Говоря о методах обеспечения доступности, следует упомянуть системы бесперебойного питания, решения для резервного копирования, резервирования и дублирования мощностей. Управление доступностью является частью планирования непрерывности бизнес-процессов, подробно описанного в ГОСТ Р ИСО 22301-2014 «Системы менеджмента непрерывности бизнеса. Общие требования». Кроме того, доступность может быть нарушена злоумышленниками извне, например, путем осуществления DDOS-атак (*англ.* Distributed Denial of Service — распределенный отказ в обслуживании) на веб-сайты. И для защиты от таких атак требуется применять специальные программно-аппаратные решения.

Несмотря на то что ключевыми свойствами ИБ являются конфиденциальность, целостность и доступность, также важное значение имеют неотказуемость, подлинность, подотчетность и достоверность.

Неотказуемость — это способность удостоверить имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты. Обеспечение неотказуемости является одной из задач организации удостоверяющего центра на основе PKI (*англ.* Public Key Infrasracture — инфраструктура открытых ключей). Другим примером выполнения функции неотказуемости является электронная подпись, использующая однонаправленную хэш-функцию.

Подлинность — это свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Способом проверки подлинности личности является использование электронной подписи. Также, для аутентификации и авторизации, а соответственно подтверждения личности пользователей широко распространены разнообразные методы двухфакторной аутентификации.

Подотчетность — это обеспечение идентификации субъекта доступа и регистрации его действий. Подотчетность включает в себя идентификацию и аутентификацию, предоставление надежных маршрутов пользователя к системе, в том числе, включая защищенный канал связи, а также регистрацию всех действий пользователей в системах. Рассматривая аутентификацию, заметим, что она бывает односторонней, когда клиент доказывает свою подлинность серверу и двусторонней, т.е. взаимной.

Достоверность — это свойство соответствия предусмотренному поведению и результатам. Например, потеря целостности информации на веб-портале оператора связи, сделанная посредством SQL-инъекции (*англ.* Structure query language — язык структурированных запросов) и выразившаяся в подмене реквизитов получателя платежа, приводит к потере достоверности, так как получаемые в виде сгенерированной веб-страницы результаты отличаются от тех, которые должны быть.

Говоря об угрозах конфиденциальности, заметим, что некоторые виды информации ограниченного доступа охраняются законом, на-

пример, Федеральным Законом № 152-ФЗ «О персональных данных». Ответственность за разглашение тех или иных сведений конфиденциального характера установлена в уголовном кодексе РФ и других нормативно-правовых актах. Для защиты персональных данных в законодательстве предусмотрены организационные и технические меры их защиты. Но такие меры расписаны не для всех видов информации ограниченного доступа. Например, техническая защита информации, составляющей коммерческую тайну, находится в ведении компаний. Иными словами, закон вводит ответственность за разглашение коммерческой тайны, но не требует от компании вводить специальный режим. Требования по обеспечению целостности и доступности информации содержатся в нормативно-правовых актах, например, в Стандарте Банка России по обеспечению ИБ.

Иногда угрозы ИБ возникают из-за халатности сотрудников, которые забывают флэшки с ценной информацией, а также из-за техногенных сбоев, например, отключения электричества, или непреднамеренных ошибок при написании программного обеспечения. При расчете рисков ИБ можно опираться на частоту таких инцидентов, и проектировать защитные меры, исходя из данных статистики. Случайные угрозы наряду с преднамеренными можно минимизировать за счет применения организационных и технических мер. Например, с помощью шифрования можно защитить данные на компьютерах и съемных носителях. На рис. 1 приведена классификация угроз ИБ и их возможных источников.

Но специалисты по ИБ борются, прежде всего, с преднамеренными угрозами, исходящими от внешних и внутренних нарушителей, о защите от которых мы и будем говорить далее. Активные и пассивные угрозы относятся к преднамеренным угрозам. Отличие активных угроз от пассивных заключается в том, что первые непосредственно влияют на функционирование информационных систем. К ним могут относиться применение зловредного программного обеспечения (ПО) с целью заражения компьютера (например, вирусами-шифровальщиками), или, например, SQL-инъекция при атаке на веб-сайт.

Пассивные угрозы, как правило, представляют, собой различные виды несанкционированного сбора информации, не влекущего ее изменения и в ряде случаев, могут являться подготовительной стадией для активной угрозы. Распространенными методами реализации пассивных угроз являются снифферы (от *англ.* snif — нюхать), задачей которых является сбор и анализ трафика из локальной сети, кей-логгеры, фиксирующие ввод данных с клавиатуры и несанкционированные RDP (*англ.* Remote Desktop Protocol — протокол удаленного рабочего стола). Нельзя не упомянуть о большом количестве зловредного ПО, которое под видом легитимных программ, может собирать информацию с мобильных устройств.

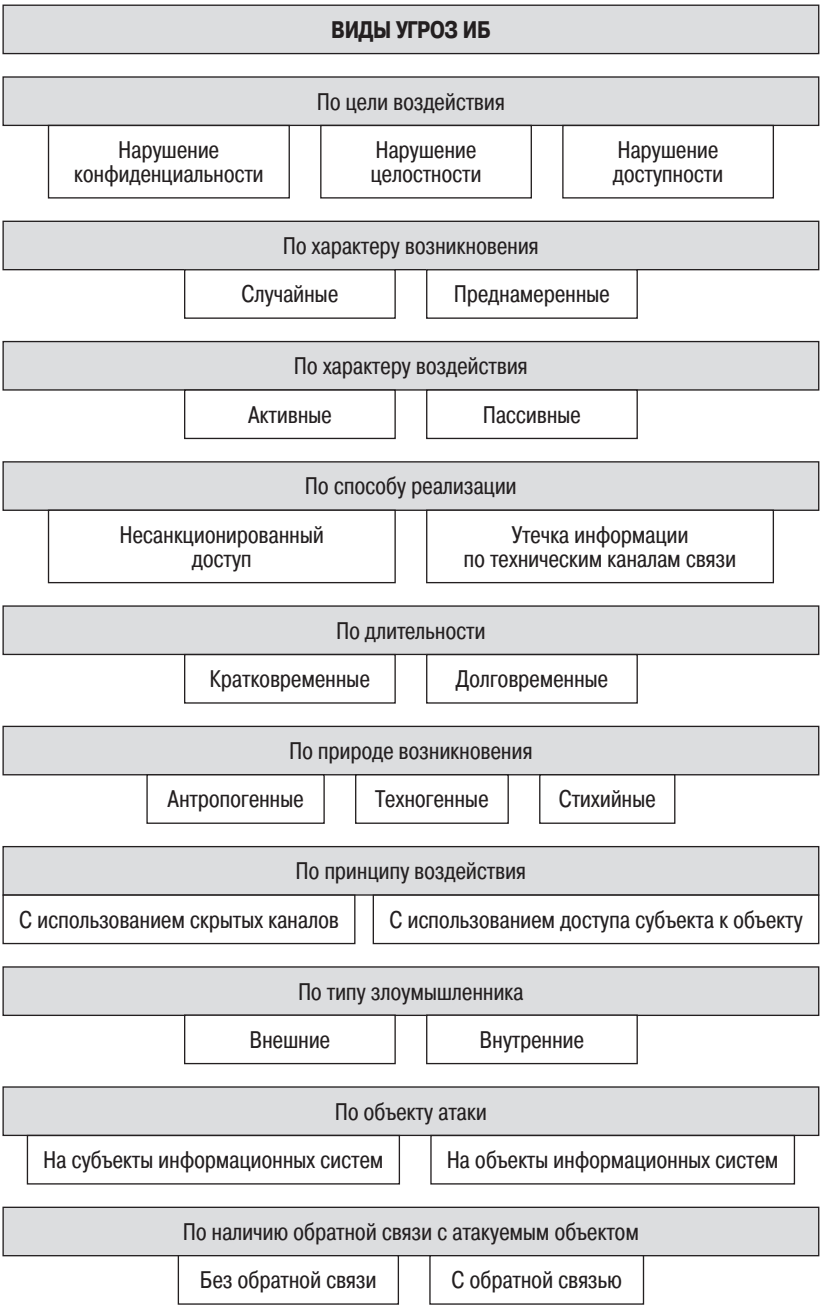

Рис. 1. *Классификация угроз ИБ*

Современные способы реализации угроз ИБ сочетают методы социальной инженерии и инструментальные программно-аппаратные средства для получения несанкционированного доступа. Хорошо отработанной схемой у хакеров, позволяющей получить доступ к информации, является использование фишинга, распространенного вида мошенничества с использованием электронных писем в сочетании с анализом уязвимостей программного обеспечения, электромагнитное, термическое, механическое, акустическое воздействие, а также использование специальных технических средств для записи речевой, визуальной информации и каналов ПЭМИН (побочных электромагнитных излучений и наводок).

Атаки могут быть разной продолжительности. Если вирусы-вымогатели действуют практически мгновенно, т.е. достаточно просто открыть вложение в письме или скачать приложение по ссылке и вся информация на компьютере становится зашифрованной, то особенностью самого современного типа атак, которые принято называть целенаправленными, является длительность их подготовки и осуществления.

В течение определенного времени организация-жертва изучается, после чего с помощью сочетания методов социальной инженерии и уязвимостей программного обеспечения на компьютеры определенных сотрудников устанавливается вредоносное шпионское программное обеспечение, выполняющее определенные функции, например, отправка снимков экрана, логирование нажатий на клавиши или банальный запуск RDP-подключения. Целевая атака может занимать от двух-трех месяцев до года.

Угрозы могут исходить как от внешних злоумышленников так и от внутренних, например, нелояльных сотрудников. С внешними угрозами все более ли менее понятно — в первую очередь, они исходят от хакеров, которые действуют целенаправленно по чьему-либо заказу, а также представителей аутсорсеров, выполняющих подрядные работы в ИТ-системах, и которые также могут оказаться преступниками, использующими доступ к данным организации-заказчика для собственных целей. Что касается внутренних злоумышленников, то именно от них очень часто исходит основная угроза, так как они изначально имеют гораздо больший доступ к информации, чем те, кто не является сотрудником компании.

Антропогенные угрозы ИБ связаны с действиями человека, техногенные — с недостатками технических средств или программного обеспечения, используемого в компьютерных сетях. К стихийным источникам угроз относятся форс-мажорные обстоятельства («обстоятельства непреодолимой силы»): наводнения, пожары, техногенные катастрофы и т.д. Когда мы говорим о внутренних источниках угроз, то помимо злоумышленников внутри компании, источником внутренней угрозы может быть нерадивый администратор, вовремя не устраняю-

щий уязвимости, или сотрудник, не предпринимающий меры предосторожности на рабочем месте. Так или иначе, все инциденты ИБ связаны с несовершенством системы ее обеспечения. Только сочетание организационных и технических мер может обеспечить сохранность информации, т. е. уменьшить риски для конфиденциальности, целостности и доступности информации.

В некоторых случаях злоумышленникам требуется непосредственный доступ к атакуемой информационной системе, а во многих случаях достаточно удаленного доступа с использованием скрытых каналов. Как правило, второй вариант становится доступен благодаря наличию не устраненных уязвимостей, в том числе «нулевого дня», в операционных системах или прикладном программном обеспечении, позволяющих получить привилегированный доступ к рабочей станции. Целью атаки может быть или субъект, работающий в информационной системе или объект, который к ней относится. Как уже говорилось выше, злоумышленники используют как методы социальной инженерии, так и недостатки в программном обеспечении.

Часть атак на объекты инфраструктуры требует ответа от атакуемого объекта (субъекта), например, при рассылке фишинговых писем требуется открыть ссылку или вложение, в котором активировать макрос или исполняемый файл, после чего будет активирован канал удаленного доступа к компьютеру, а в некоторых случаях этого не требуется, например, при организации DDOS-атаки (*англ.* Denial of Service — «отказ в обслуживании») – хакерской атаки на веб-сервер компании, целью которой является приведение веб-сайта в неработоспособное состояние путем большого числа запросов к нему (флуд-атака — одна из разновидностей DDOS-атаки). Также, атаки могут быть классифицированы по уровню модели OSI (*англ.* Open System Interconnection — взаимодействие открытых систем), на котором происходит атака. Методы и меры обеспечения ИБ на предприятии динамически меняются по мере изменения модели угроз информационным системам и появления новых типов атак на инфраструктуру. Подразделяются все меры ИБ на три основных типа: организационные, физические и технические.

К техническим мерам относится проектирование и внедрение средств защиты информации (межсетевые экраны, антивирусы, средства защиты от несанкционированного доступа и т.д.), к организационным — разработка, внедрение и контроль исполнения локальных нормативных актов, организационно-распорядительной документации в сфере защиты информации, например, положение о коммерческой тайне, или политика в области обработки персональных данных, а также проведение обучающих семинаров и тренингов по ИБ для сотрудников. Физические меры включают в себя систему контроля и управления доступом на территории предприятия.

Организационные меры обходятся предприятию дешевле, нежели технические. Как пример, для предотвращения атак на рабочие места сотрудников можно отключить интернет на данных компьютерах, но в этом случае работа компании может быть парализована. Поэтому, защита информации — это всегда разумный компромисс и сочетание всех вышеприведенных мер на основе оценки рисков ИБ. В любом случае необходимо сверяться с требованиями законодательства. Например, если осуществляется проект по защите персональных данных, то необходимо ознакомиться с Федеральным Законом от 27.07.2006 № 152-ФЗ «О персональных данных», затем с Постановлением Правительства РФ от 01.11.2012 № 1119, чтобы определить уровни защищенности персональных данных, и с Приказом ФСТЭК России от 18.02.2013 № 21 для выбора приемлемых технических мер защиты.

Все меры по защите информации можно разделить на сдерживание, превентивные меры, корректировка, восстановление, детективные меры, компенсирующие меры, меры соответствия требованиям законодательства в области защиты информации [6]. Сдерживание — комплекс мер для предотвращения попыток совершения преступления со стороны возможного злоумышленника. К ним относятся предупреждение сотрудников об ответственности за разглашение коммерческой тайны, или информация о том, что в компании внедрена DLP-система (*англ.* Data Leak Prevention — предотвращение утечек информации).

Превентивные меры служат для предотвращения киберпреступления. Например, DLP-систему можно поставить в разрыв, чтобы весь сетевой трафик компании проходил через нее, а часть его блокировалась в соответствии при обнаружении попыток отправки за периметр компании чувствительной информации. Можно поставить ее в режиме зеркалирования трафика, когда система ничего не блокирует, а лишь анализирует трафик и оповещает офицера безопасности о возможных нарушениях ИБ. Упомянем системы класса IPS (*англ.* Intrusion Prevention System — система предотвращения вторжений), которые предотвращают попытки вторжения в сеть, но в отличие от IDS-систем (*англ.* Intrusion Detection System — система обнаружения вторжений перевод и русская аббревиатура) такие попытки только детектируют.

Такими мерами, могут являться и организационные, например, тщательная проверка персонала при приеме на работу, или программы повышения осведомленности сотрудников. Физические меры по предотвращению инцидентов включают в себя установку современных СКУД (Системы контроля и управления доступом), в том числе, с использованием современных биометрических технологий и интеграции их с системой двухфакторной аутентификации в сети компании. Корректировка — комплекс мер, предназначенных для внесения измене-

ния в систему управления информационной безопасностью (СУИБ) после того, как инцидент произошел.

Идеальным алгоритмом здесь является классический цикл Шухарта-Деминга PDCA (Планируй-Действуй-Проверяй-Корректируй). В применении к ИБ это может выглядеть следующим образом.

Мы спроектировали СУИБ в соответствии с актуальной моделью угроз (Планируй), после чего внедрили комплекс защитных мер (Действуй), в случае инцидента провели расследование (Проверяй), и скорректировали СУИБ в соответствии с изменившейся моделью угроз (Корректируй). Необходимо одно уточнение. В связи с тем, что большинство компаний имеют динамически меняющуюся инфраструктуру, третий этап цикла, а (Проверяй) необходимо проводить регулярно в виде тестов на проникновение (pen-test) и аудита ИБ, опираясь как на требования регуляторов в области защиты информации, так и рекомендации стандартов.

СУИБ — это комплекс технических, организационных и физических мер, которые включают в себя ограничение полномочий пользователей при работе в сети компании и корректировка включает внесение изменение, в том числе, в настройки системного и прикладного программного обеспечения. Восстановление требуется для реанимирования защитных мер после того, как инцидент произошел. Например, если устройство для защиты от DDOS-атак установлено с помощью изменения в записи DNS (имеет IP-адрес), то при массированной DDOS-атаке оно может быть выведено из строя, или пропускать вредоносный трафик наряду с очищенным. Восстановление защитных мер могут являться частью BCM (*англ.* Business Continuity Management — управления непрерывностью бизнеса), в которой указывается срок восстановления защитных мер.

Детективные меры предназначены для проведения расследований кибер-инцидентов с привлечением специализированных организаций. Для упрощения их работы в компании важно иметь набор прикладных решений, позволяющих в ретроспективном контексте восстановить пошагово те действия, которые предпринял злоумышленник. К таким системам относятся SIEM-решения (*англ.* Security Information and Event Management — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management

— управление ИБ) и SEM (Security event management

— управление событиями безопасности).

Компенсирующие меры позволяют обеспечить альтернативные виды зашиты информации. Данная возможность обусловлена тем, что частная модель угроз в рамках российского законодательства определяется заказчиками самостоятельно, ровно, как и выбор мер по защите от этих угроз. В связи с этим есть возможность грамотного балансирования между организационными, физическими и техническими

мерами, в рамках имеющихся финансовых и кадровых возможностей. Меры соответствия — тот набор решений, который должен быть внедрен в соответствии с законодательством Российской Федерации.

Мы рассмотрели основные типы угроз ИБ и меры защиты от них. Обеспечение ИБ призвано защитить информацию, в первую очередь, от компрометации конфиденциальности, целостности и доступности. Количество различных видов тайн, охраняемых законодательством, превышает 50. В связи с особой важностью некоторых видов информации ограниченного доступа, для них в законодательстве разработан целый ряд нормативных документов, регламентирующих порядок их обработки и защиты. Одним из них являются персональные данные, которые охраняются с особой тщательностью. Существует более двадцати видов угроз ИБ для реагирования на которые разработан целый ряд организационных и технических мер, которые мы рассмотрим в следующих разделах.

Вопросы для самопроверки

1. Какие свойства ИБ являются ключевыми?
2. Как подразделяются угрозы ИБ по природе возникновения?
3. Чем активные угрозы ИБ отличаются от пассивных?
4. В чем особенность превентивных мер по защите информации?

2. СТАНДАРТИЗАЦИЯ, СЕРТИФИКАЦИЯ И МЕТРОЛОГИЯ КАК ЧАСТЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Регулирование отрасли ИБ в Российской Федерации основано на трех группах законов и стандартов. Первая группа — это обязательные к исполнению на территории Российской Федерации руководящие документы ФСТЭК России (ранее Гостехкомиссия России) и ФСБ России, а также постановления Правительства России, Федеральные законы Российской Федерации и решения коллегии Евразийской экономической комиссии, вторая — это национальные, в том числе, отраслевые стандарты по обеспечению ИБ, и третья — это международные стандарты по обеспечению ИБ, среди которых также есть относящиеся к конкретной отрасли, например, PCI DSS (*англ.* Payment Card Industry Data Security Standard — стандарта безопасности данных индустрии платежных карт).

Стандарты могут носить обязательный или рекомендательный характер. Если финансовая организация имеет в своем распоряжении процессинговый центр, в котором обрабатываются данные пластиковых карт, то банк должен регулярно проходить аудит на соответствие требованиям упомянутому выше PCI DSS. А стандарт ISO 27001 не является обязательным к применению, но, проведя сертификацию СУИБ в соответствии с ним, можно поднять цену компании в глазах потенциальных инвесторов, в первую очередь, зарубежных. Другими словами, указанный стандарт можно считать своего рода чек-листом для проверки совершенства СУИБ. Перечень национальных стандартов в области ИБ приведен в Приложении № 2.

Правовое регулирование ИБ является мощным механизмом, позволяющим поддерживать инвестиции в ИБ на достаточно высоком уровне. Это связано, в первую очередь, с Федеральными законами, нормативными актами, а также обязательными к исполнению стандартами. Штрафы и санкции за их невыполнение ужесточаются, поэтому можно уверенно говорить о том, что они действительно двигают рынок вперед. Сложно представить, что из себя представляла

бы отрасль ИБ в России и в мире в целом, если бы государственные органы не уделяли ей столько внимания. Кроме того, стандарты являются воплощением опыта практикующих экспертов или, как принято говорить, “best practice”, и являются руководством к действию для специалистов в области ИБ. В то же время угрозы появляются намного быстрее, чем разрабатываются меры противодействия, находящие отражение в стандартах и нормативно-правовых актах.

П. Друкер признается основоположником концепции, которая стала основой современного менеджмента и называется «Управление по целям» — метод управления, предусматривающий предвидение возможных результатов деятельности и планирование путей их достижения. Воплощением управления по целям, является «Система *KPI*» (*англ.* Key Performance Indicators — ключевые показатели эффективности), которая помогает организации определить достижение стратегических и тактических (операционных) целей, дает возможность оценить свое состояние и позволяет проводить контроль деловой активности сотрудников и компании в целом. Стандарты описывают структуру СУИБ, поэтому определяя ее KPI можно ориентироваться на них. Конкретные средства защиты подбирают, исходя из анализа угроз и предложений по их отражению, основываясь на исследованиях независимых рейтинговых и аналитических агентств, например, Gartner. Основным Федеральным законом в области стандартизации является Федеральный закон «О техническом регулировании» от 27.12.2002 № 184. В нем определены основные цели стандартизации:

- повышение уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества, объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера, повышение уровня экологической безопасности, безопасности жизни и здоровья животных и растений;
- обеспечение конкурентоспособности и качества продукции (работ, услуг), единства измерений, рационального использования ресурсов, взаимозаменяемости технических средств (машин и оборудования, их составных частей, комплектующих изделий и материалов), технической и информационной совместимости, сопоставимости результатов исследований и измерений, технических и экономико-статистических данных, проведения анализа характеристик продукции (работ, услуг), исполнения государственных заказов, добровольного подтверждения соответствия продукции (работ, услуг);
- содействие соблюдению требований технических регламентов;
- создание систем классификации и кодирования технико-экономической и социальной информации, систем каталогизации продукции (работ, услуг), систем обеспечения качества продук-

ции (работ, услуг), систем поиска и передачи данных, содействие проведению работ по унификации.

Применительно к ИБ стандартизация применяется для:

— аудита ИБ;
— моделирования угроз ИБ;
— определения методик испытания программных средств на отсутствие не декларированных возможностей;
— определения методов защиты от несанкционированного доступа;
— защиты персональных данных и конфиденциальной информации;
— использования криптографии для обеспечения ИБ;
— управления ИБ;
— управления рисками ИБ;
— определения методов и средств обеспечения ИБ;
— защиты от специальных электромагнитных воздействий.

Говоря о соответствии предприятий требованиям стандартов и законов, нельзя не сказать о том, каким образом они проверяются. В Российской Федерации есть два основных регулятора — это Роскомнадзор и ФСБ России. Первый уполномочен проверять предприятия, в основном, на предмет правильности обработки и принятых мер по защите персональных данных, второй — деятельности, связанной с использованием средств криптографической защиты информации. Результатом проверок является предписание об устранении нарушений. Для подготовки к проверкам организации зачастую приглашают профессиональные консультационные компании, обладающие требуемыми лицензиями ФСТЭК России на деятельность по технической защите конфиденциальной информации и ФСБ России на распространение и обслуживание криптографических средств.

Вторая лицензия требуется в том случае, если в частной модели угроз существуют те виды угроз, нейтрализация которых возможна только с использованием СКЗИ, например, угрозы конфиденциальности информации, передаваемой по открытым каналам связи. Результатом деятельности такого аудита или проекта является оценка соответствия информационных систем требованиям руководящих документов или аттестация информационных систем/рабочих мест в соответствии с теми же требованиями.

Основным методом доказательства соответствия компании его требованиям стандарта является соответствующий сертификат. Как и в других отраслях, в области ИБ стандартизация и сертификация идут бок о бок, а точнее, друг за другом. После проведения мероприятий, связанных с внедрением в организации стандарта в области ИБ, проводятся сертификационные испытания и выдается сертификат соответствия требованиям тех или иных руководящих документов, например, ISO

27001. Кроме того, в РФ существует система обязательной сертификации СЗИ на проверку отсутствия не декларированных возможностей и соответствия требованиям руководящих документов ФСТЭК России. Надо сказать, что подход государственных органов в России и за рубежом несколько отличается. Например, штраф за нарушение в области персональных данных в Европе, где действует GDPR (*англ.* General Data Protection Regulation — генеральный регламент о защите персональных данных) доходят до 4% от дохода, у нас значительно меньше.

Также, отличается и сам подход к защите информации. На условном «Западе» многие годы главенствует риск-ориентированный подход, когда соизмеряется ценность информации, накапливается статистика инцидентов ее компрометации, и на этом основании вырабатывается система мер защиты, стоимость которой должна быть адекватна той информации, которую собираемся защищать и тому реальному риску для нее, который определен в результате аудита. При этом список мер по защите информации не фиксирован, а определяется в соответствии с лучшими практиками. В России же регуляторами заранее определяется список мер по защите информации, а оценка рисков ИБ не предусматривается. Серия стандартов для специалистов по ИБ ISO 27000 включает:

- обзор и терминология — ГОСТ Р ИСО/МЭК 27000-2012;
- требования к СМИБ (система менеджмента информационной безопасности) — ГОСТ Р ИСО/МЭК 27001-2006, а также свод норм и правил менеджмента ИБ ГОСТ Р ИСО/МЭК 27002-2012;
- руководство по реализации СМИБ и измерения в области ИБ — ГОСТ Р ИСО/МЭК 27003-2012 и ГОСТ Р ИСО/МЭК 27004-2011;
- менеджмент рисков в области ИБ — ГОСТ Р ИСО/МЭК 27005-2010.

Особое место в этой серии занимает безопасность сетей и приложений, для которых существуют отдельные стандарты, а также требования к органам, осуществляющим аудит и сертификацию СМИБ, и ряд других аспектов ИБ. Подчеркнем разницу между стандартами и спецификациями. Стандарты регламентируют основные требования и правила управления СМИБ, а спецификации определяют конкретную реализацию тех или иных мер защиты информации, например, IpSEC, Kerberos, TLS [18].

Метрология играет ключевую роль в процессе обеспечения ИБ. Несмотря на то что в метрологии речь идет об измерении физических величин, в широком смысле слова, метрология — это (от греч. μέτρον «мера » + λόγος «мысль ; причина ») — наука об измерениях, методах и средствах обеспечения их единства и способах достижения требуемой точности. Стандарт ГОСТ Р ИСО/МЭК 27004-2011 — «СМИБ. Измерения» «содержит рекомендации по разработке и использованию мер измерения для проведения оценки эффективности реализованной СМИБ, а также мер и средств контроля и управления или их групп по ИСО/МЭК 27001».

Это позволяет определить ключевые показатели эффективности СМИБ, и разработать методику их измерения и контроля, что позволяет поддерживать СМИБ в работоспособном состоянии в промежутках между внешними аудитами ИБ. Стандарт определяет цели, программу и модель измерений, а также факторы успеха, а кроме того, описывает процесс анализа данных и совершенствование системы измерений.

Методы измерения могут быть объективными, основанными на математических вычислениях и субъективными, основанными на суждениях. Один из многочисленных параметров СМИБ, которые можно измерять, это уровень знаний сотрудников об угрозах ИБ и основах защиты от них. Цель такого измерения — оценка осведомленности персонала в области ИБ. Практически это выглядит так. Организация проводит обучение персонала и ведет соответствующие записи в журнале. Оценивается численность персонала, получившего обучение, в процентах от общего количества сотрудников, и сравнивается с плановым показателем, после чего в процесс обучения вносится корректировка. Здесь мы видим также применение стандартного цикла Шухарта-Деминга.

Среди принципов Деминга для менеджера один посвящен вопросам обучения. Эффективно управлять изменениями на фирме могут только компетентные профессионалы. Невозможно победить в конкурентной борьбе и при этом не уделять должного внимания вопросам подготовки и переподготовки кадров. Безошибочная работа начинается с правильного понимания каждым своих обязанностей и уверенности в том, что он может их выполнить. Это означает, что каждый работник:

- know (знает) — обучен с учетом индивидуальных особенностей, выполняемой деятельности и постоянным повышением квалификации, причем знания должны быть синтетическими;
- can (может) — имеет опыт и может применить свои знания на практике;
- want (хочет) — когда он знает, что его хорошая работа будет по достоинству вознаграждена;
- do (делает) — предприятие создало все необходимые и достаточные условия для качественного выполнения работы.

Программа обучения на рабочем месте, разработанная в США и затем использованная в Японии, получила название TWI (Training within Industry) — одна из глобальных практик обучения людей на рабочем месте [7, 8].

Среди других параметров, измеряемых на постоянной основе, можно выделить число инцидентов ИБ, количество найденных уязвимостей в программном обеспечении, количество паролей, генерируемых вручную и в автоматизированном режиме и т.д.

Кроме серии ISO 27000 существует еще ряд стандартов, относящихся к ИБ, в первую очередь, BS 7799 Британского института стандартов, а также 800-я серия NIST (Национального института

стандартов и технологии), где подробно расписываются компенсирующие меры по защите информации. Из международных стандартов заслуживает внимания HIPAA (*англ.* Health Insurance Portability and Accountability Act — Закон об учете и безопасности медицинского страхования), где сформулированы правила конфиденциальности в целях защиты информации о здоровье пациентов, а также FISMA (*англ.* Federal Information Security Management Act), основополагающий федеральный закон США об обеспечении и управлении ИБ.

Укажем на закон Sarbanes-Oxley (SOX), определяющий достаточно жесткие требования к подготовке отчетности и внутреннему контролю, частью которого является обеспечение ИБ. Надо сказать, что данный закон обязателен для компаний, планирующих IPO (*англ.* Initial Public Offering — первичное публичное размещение акций) и выход на американский фондовый рынок, что в настоящее время актуально и для некоторых российских компаний.

Что касается российских стандартов и законов, то помимо перечисленных выше имеет смысл упомянуть СТО БР ИББС, стандарт Банка России, регламентирующий процедуры и определяющие основные механизмы защиты информации в финансовых учреждениях, а также ГОСТ Р 57580.1-2017 (Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер). Одними из основополагающих законов в области защиты информации в России являются 152-ФЗ «О персональных данных», 149-ФЗ «Об информации, информационных технологиях и защите информации», 98-ФЗ «О коммерческой тайне», 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» и ряд других. Перечень законов и нормативных актов в области защиты информации приводится в Приложении № 3.

Поскольку основным стандартом в области ИБ является ISO 27001, то наличие сертификата о соответствии системы обеспечения ИБ данному стандарту является подтверждением построенной системы ИБ, повышает уровень доверия партнеров к организации. Метрология, в широком значении этого понятия, также является очень важной, поскольку деятельность специалистов по ИБ неразрывно связана с самыми разнообразными измерениями, например, измерением количества инцидентов ИБ и обнаруженных уязвимостей.

Вопросы для самопроверки

1. Приведите пример обязательного стандарта в области ИБ.
2. Опишите области ИБ, где применяется стандартизация.
3. Наличие какого сертификата в области ИБ является подтверждением построенной системы обеспечения ИБ в компании?
4. В чем отличие стандартов от спецификаций?

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Одним из основных видов конфиденциальной информации являются персональные данные и наибольшее количество нормативных актов в области защиты информации в нашей стране относится именно к ним. В статьях 23 и 24 Конституции РФ говорится:

«1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» (статья 23).

«Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» (статья 24).

Уместно вспомнить и Европейскую конвенцию о защите прав человека и основных свобод, которую наша страна ратифицировала 30 марта 1998 года. Для наших граждан факт ратификации означает, что они вправе обращаться в Европейский Суд по правам человека при нарушении их прав в случае, если исчерпаны возможности их защиты в Российской Федерации. Вопросам персональных данных в Конвенции посвящена статья 8 «Право на уважение частной и семейной жизни».

Основным нормативным актом в Российской Федерации, регулирующим порядок обработки и защиты персональных данных, является Федеральный закон «О персональных данных» от 27.07.2016 152-ФЗ, согласно которому: «Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». При этом необходимо подчеркнуть, законодательство защищает, прежде всего, именно конфиденциальность персональных данных, т.е. их защиту от лиц, которым не предоставлен легитимный доступ к такой информации.

Отсюда необходимость эшелонированной защиты персональных данных в компаниях на всех этапах их обработки. Остановимся на персональные данных, касающихся здоровья граждан. С одной стороны, следует обеспечить защиту от утечек персональных данных о пациентах, а с другой, от вмешательства в информационные системы медицинской организации и изменения данных, например, о диагнозе, т.е. потери целостности, или выводе из строя сервера обработки данных медицинской информационной системы.

В настоящее время обработка информации происходит как в сетевом периметре организации, так и вне его (с мобильных телефонов и планшетов сотрудников, партнеров и клиентов), в том числе с использованием незащищенного интернет-соединения. Поэтому необходимо использовать VPN-подключение (*англ.* Virtual Private Network — виртуальная частная сеть) — соединение между группой отдельных сетей, которые обмениваются зашифрованными данными к корпоративным ресурсам, а также защищать информацию на мобильных устройствах с помощью EMM (*англ.* Enterprise Mobility Management — управление мобильностью предприятия — набор технологий, процессов и политик для обеспечения безопасности мобильных устройств и управления ими) — решений.

Несмотря на то что перечень мер по защите персональных данных четко регламентирован, рекомендуем анализировать все вектора атак, и предпринимать меры по защите от них, например, анализировать код приложений, которые обрабатывают персональные данные, на устойчивость к взлому. Защита персональных данных — это сочетание как технических, так и организационных мер, которые подразумевают набор организационно-распорядительных документов, в частности, политики ИБ, не позволяющих скомпрометировать информацию, обрабатываемую на персональных компьютерах, не имеющих антивирусных программ, не говоря о защите от продвинутых атак (Advanced Threat Protection) и EDR (Endpoint Detection and Response), оперирующих понятиями «индикатор компрометации».

Техническая защита конфиденциальной информации, в частности, проектирование в защищенном исполнении средств и систем информатизации, лицензируется ФСТЭК России. Техническая защита без лицензии является нарушением Федерального закона «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ. Кроме того, если есть риск компрометации персональных данных при их передаче по открытым каналам связи, необходимо внедрять средства криптографической защиты информации, такая деятельность лицензируется ФСБ России.

Как сказано выше, закон от 27.07.2006 № 152-ФЗ «О персональных данных» является основным федеральным законом, регулирующим

данную область. В нем дается определение персональных данных, принципы и условия их обработки, определяются права субъекта персональных данных и обязанности оператора персональных данных. Часто приходится слышать следующие аргументы для того, чтобы не уделять вопросу обработки персональных данных большое внимание: «мы не обрабатываем персональные данные», «персональные данные являются несущественными или не представляющими интерес», «мы не являемся оператором, так как подавали уведомление об обработке персональных данных». Эти и многие другие формулировки свидетельствуют о все еще низком уровне грамотности компаний в области российского законодательства по ИБ.

В соответствии с законом № 152-ФЗ «оператор — это государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными...»

А «обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных».

У каждой компании есть сотрудники, клиенты — физические и юридические лица, партнеры, поставщики, с сотрудниками которых ведется взаимодействие, по различным каналам связи. И если вспомнить приведенное выше определение персональных данных, то практически любая компания в России является оператором, а факт неподачи уведомления об обработке персональных данных в Роскомнадзор — это прямое нарушение закона.

Федеральные законы определяют терминологию, базовые принципы обработки персональных данных, права и обязанности субъектов персональных данных и операторов персональных данных, а непосредственный перечень мер защиты определяется подзаконными актами. Основными подзаконными актами являются Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Идеология постановления Правительства № 1119 в том, что защита персональных данных должна осуществляться дифференцированно в зависимости от актуальности угроз и уровня защищенности. Угрозы персональным данным делятся на три типа: угрозы 1-го типа актуальны для информационных систем при наличии не декларированных возможностей в системном ПО, 2-го типа — в прикладном ПО, 3-го типа — не связанные с НДВ системном и прикладном ПО.

Определение типа угроз является привилегией операторов персональных данных и должно проводиться с учетом оценки возможного вреда. Что касается уровня защищенности персональных данных, то постановлением Правительства РФ № 1119 установлено четыре уровня, которые зависят от типа угроз, категории обрабатываемых персональных данных (специальные, биометрические, общедоступные или иные), а также количества обрабатываемых записей персональных данных (более 100 000 или менее этого количества).

После определения уровня защищенности персональных данных, открываем 21-й Приказ ФСТЭК России и определяем меры защиты, которые необходимо внедрить. Технические меры защиты делятся на три класса: 4-й, 5-й и 6-й, а средства вычислительной техники (СВТ), на которых ведется обработка персональных данных, на 5-й и 6-й классы. В зависимости от уровня защищенности подбираются решения СЗИ, а также организационные меры. Для соответствия требованиям законодательств необходимо применять сертифицированные ФСТЭК России СЗИ. В 2016–2017 гг. ФСТЭК России выпустила обновление методических документов, касающихся использования межсетевых экранов и операционных систем, создав для них профили защиты. Основные меры по обеспечению безопасности в соответствии с приказом ФСТЭК России № 21:

- идентификация и аутентификация субъектов и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации и технических средств;
- защита информационной системы, систем связи и передачи данных;

— выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных и реагирование на них;
— управление конфигурацией информационной системы и системы защиты персональных данных.

Напомним, что существует понятие «модель угроз персональным данным». Она строится на основе базовой модели угроз ФСТЭК России — документа, который в формализованном виде, отражает мнение регулятора по поводу тех векторов атак, которые надо учитывать при построении системы защиты. Документ оперирует такими понятиями как источник угрозы, уязвимости ИСПДн, способ реализации угрозы, объект воздействия и деструктивное воздействие. В соответствии с Федеральным законом № 152 оператор не обязан иметь модель угроз, но ее наличие в компании де-факто признается практически обязательным. Модель отражает деятельность оператора по выявлению угроз для персональных данных, и дает понимание того, что те меры защиты, которые внедрены, соответствуют актуальным угрозам.

С 1 сентября 2015 года вступил в силу Федеральный закон № 242-ФЗ, который внес изменения в Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» — дополнен статьей 15.5 о создании «Реестра нарушителей прав субъектов персональных данных». У Роскомнадзора появилась возможность блокировать сайты, на которых персональные данные обрабатываются с нарушениями. Статья 18 Федерального закона № 152 дополнена пунктом «При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети “Интернет”, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона».

Закон широко обсуждался в средствах массовой информации и профессиональном сообществе, и не все компании пошли на перенос баз данных, расположенных за рубежом, в Россию. Часто компании заказывают услугу по приведению обработки персональных данных в соответствии с законодательством профессиональным консультационным компаниям. В ходе таких проектов проводится обследование процессов обработки персональных данных, по результатам которого составляется отчет с указанием выявленных недостатков и нарушений, и предлагаются меры по их устранению. После этого разрабатывается технический проект, модель угроз, техническое задание на внедрение средств защиты информации, комплект организационно-технической

документации и проводится оценка эффективности мер защиты информационных систем персональных данных (декларирование соответствия ИСПДн).

Потеря конфиденциальности персональных данных может приводить к тяжелым последствиям. В обязанности оператора персональных данных входит правильная обработка персональных данных и в необходимых случаях их защита. Для определения мер защиты устанавливаются уровни защищенности в соответствии с Постановлением Правительства РФ № 1119, и определяются сами защитные меры на основе Приказа ФСТЭК России № 21.

Вопросы для самопроверки

1. Как определяется уровень защищенности персональных данных?
2. Что такое «обработка персональных данных»?
3. В каких ситуациях необходимо использовать VPN для защиты персональных данных?
4. На основе какого нормативного документа определяются меры по защите персональных данных?

4. БОРЬБА С УГРОЗАМИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Обеспечение защиты от несанкционированного доступа к информации (НСД) является ключевой задачей ИБ и включает в себя целый ряд организационных и технических мер. Оно находит свое отражение в целом ряде нормативных актов и методических документов, в том числе, в упоминавшейся базовой модели угроз безопасности персональным данным ФСТЭК России. Говоря об угрозах НСД, необходимо разделять задачи выполнения требований законодательства и те меры, которые требуется принять в соответствии с актуальными угрозами ИБ, существующими в настоящее время.

30 марта 1992 г. стал знаковым днем для отрасли ИБ в России. В тот день решением Гостехкомиссии России был утвержден перечень руководящих документов по защите информации от несанкционированного доступа, среди которых:

- «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- «Защита от несанкционированного доступа к информации. Термины и определения»;
- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Позднее появились руководящие документы «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей», «Защита от несанкционированного

доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей».

Начнем с определения НСД. В соответствии с концепцией защиты СВТ и АС, НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Как мы видим, концепция предполагает отличия в части защиты СВТ и АС, поскольку СВТ изначально не содержат информацию, а в случае с АС мы уже получаем дополнительные характеристики АС, например, полномочия пользователей или модель нарушителя. Разница в защите СВТ от НСД и АС от НСД в том, что при защите СВТ от НСД внедряется комплекс программно-технических средств, а в случае защиты АС, кроме этого, еще и вводятся организационные меры.

Модель нарушителя предусматривает четыре уровня возможностей, предоставляемых им средствами, АС и СВТ, от первого, где нарушитель ограничен заранее предопределенным набором функций ПО до четвертого, когда нарушитель может управлять АС, а также запускать собственные программы с необходимыми ему функциями. В концепции приводятся основные методы НСД и направления обеспечения защиты от НСД.

Следующим документом, на который имеет смысл обратить внимание, является РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». В соответствии с этим РД установлено семь классов защищенности СВТ от НСД, где седьмой класс — самый низкий. Классы делятся на четыре группы, отличающихся уровнем защиты. Если посмотреть в таблицу показателей защищенности СВТ, то можно увидеть, что в числе этих показателей присутствует принцип контроля доступа, причем для низших классов предполагается использовать дискреционный принцип контроля доступа, а для высших - мандатный.

Дискреционный принцип управления доступом DAC (*англ.* Discretionary Access Control) — управление доступом субъектов к объектам на основе списков ACL (*англ.* Access Control List) или матрицы доступа. Это означает, что владелец объекта может полностью контролировать доступ к объекту, включая и список тех, кому разрешено изменять права доступа к объекту. Мандатный принцип управления доступом MAC (*англ.* Mandatory access control) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

В соответствии с этим принципом можно ввести в компании уровни допуска к информации и метки, и доступ к ним будет возможен при

наличии соответствующего разрешения. Это устраняет основной недостаток дискреционного принципа, и позволяет провести довольно тонкую настройку доступа к файлам. Другой технологией защиты доступа к файлам является DRM (*англ.* Digital Rights Management), использующая криптографическую защиту информации. Эта технология часто является одной из функций решений класса VDR (*англ.* Virtual Data Room — виртуальная комната данных), предназначенных для безопасного обмена файлами между сотрудниками компании и контрагентами. В указанном РД не указан такой принцип доступа как ролевой, а между тем в современности именно он начинает играть решающую роль.

Ролевой принцип управления доступом (*англ.* Role Based Access Control) — принцип управления доступом, когда права в информационных системах даются пользователям на основании их роли в компании. Данный принцип лежит в основе функционирования IDM систем (Identity Management), которые, получая информацию о сотрудниках из кадровых систем, автоматически предоставляют им права в информационных системах, взаимодействие с которыми осуществляется с помощью специальных коннекторов. Таким же образом IDM-системы отбирают права у уволенных сотрудников.

На практике имеет смысл использовать смешанную модель управления доступом в компании: ролевую модель для управления правами доступа сотрудников в информационных системах, мандатную — для повышенной защиты информации ограниченного доступа, дискреционную — для иной информации.

Несанкционированный доступ к информации возможен с использованием легитимного доступа к АС, например, администратором сети, или хакером с использованием вредоносного ПО и социальной инженерии. Поэтому важно иметь актуальную модель угроз и модель нарушителя, рассчитывать риски НСД в соответствии с международными стандартами для того, чтобы трезво оценивать все возможные вектора атак.

Говоря о защите информации от несанкционированного доступа, надо иметь в виду, что всегда профилактика предпочтительнее лечения. Другими словами, превентивные, предупреждающие меры являются одними из наиболее важных. К ним относятся:

— сегментация сети с использованием групповых политик;
— использованием смешанного принципа управления доступом, о котором мы говорили выше;
— использование IDM-систем для управления правами доступа сотрудников;
— защита привилегированных учетных записей от компрометации (*англ.* PIM — Privileged Identity Management);
— использование межсетевых экранов нового поколения с функционалом обнаружения вторжений в сеть и защиты от них,

а также решений по защите от продвинутых атак, установленных на периметре и конечных точках;
- контроль целостности ключевых компонентов средства защиты информации и объектов файловой системы;
- своевременный патч-менеджмент, т.е. установка обновлений операционных систем и прикладного ПО на серверах и рабочих станциях, в том числе с помощью сканеров уязвимостей;
- использование доверенной информационной среды;
- контроль действий приложений;
- использование антивирусной защиты;
- использование парольной политики с запретом использования простых паролей и регулярной сменой пароля;
- использование двухфакторной, в том числе биометрической аутентификации;
- использование СКЗИ для защиты информации на конечных устройствах и в процессе ее передачи по каналам связи;
- использование решений для управления доступом к данным класса DAG (*англ.* Data Access Governance) для аудита действий пользователей в файловых «шарах»;
- использование решений класса EDR (*англ.* Endpoint Detection and Response), использующих профилирование, для определения вредоносной активности на конечных станциях, не определяемой сигнатурным методом;
- использование EMM-решений (*англ.* Enterprise Mobility Management) для предотвращения вектора атаки через вредоносное ПО на мобильных устройствах, с помощью помещения корпоративной информации в крипто контейнер;
- использование технологий Security Awareness для повышения осведомленности пользователей об угрозах ИБ.

Обратим внимание, что в зависимости от метода эксплуатации различных СЗИ их цель может варьироваться от предотвращения инцидентов, т.е. превентивных мер до детектирования. Например, межсетевой экран (МСЭ) может эксплуатироваться в режиме зеркалирования, когда на него подается копия трафика с устройств в сети, но при этом он не блокирует его, а только осуществляет анализ, так и в разрыв, когда МСЭ блокирует трафик в соответствии с политикой безопасности.

Промышленную эксплуатацию СЗИ в режиме блокировки трафика надо производить после их тонкой настройки. Если не провести тщательную настройку правил блокировки почтового трафика в DLP-системах (*англ.* Data Leak Prevention — защита от утечек информации), работа компании мгновенно может быть парализована, поскольку правила фильтрации «из коробки» зачастую требуют дополнительной настройки под заказчика, и без этого количество ложных срабатываний будет очень большим, впрочем как и в противном случае, может

«утекать» информация, которую систему не сочтет конфиденциально. Что касается DLP, то несмотря на то, что эти системы предназначены для борьбы с внутренними злоумышленниками, зачастую имеющих легальный доступ к информации, так как эти решения контролируют весь трафик, то в случае атаки на хост извне, DLP это зафиксирует, поэтому такие системы можно рассматривать как элемент защиты от НСД.

Каждая компания имеет индивидуальные особенности, и при внедрении таких систем важно наличие профессионального аналитика, который в состоянии настроить правила срабатывания на инцидент для конкретной компании в зависимости от ее профиля, бизнес-процессов, организационной структуры, и тех видов информации ограниченного доступа, которые не обрабатываются.

К детективным мерам, в первую очередь, можно отнести SIEM-системы (*англ.* Security Information and event Management), решения класса Data Governance, системы обнаружения вторжений (*англ.* IDS — Intrusion Detection System), сейчас являющиеся частью функционала межсетевых экранов (МСЭ), а также системы контроля за работой сотрудников и систему видеонаблюдения. Перечисленные системы, используя в том числе функционал профилирования и UEBA (*англ.* User and Entity Behavior Analytics — системы поведенческого анализа), круглосуточно накапливают информацию обо всех событиях в сети и выявляют аномалии или инциденты, после чего подается сигнал в службу информационной безопасности.

В настоящее время в крупных организациях на основе внедренных SIEM-систем и workflow-систем класса IRM (*англ.* Incident Response Management) созданы SOC и (*англ.* SOC — Security Operations Center — центр мониторинга информационной безопасности) — подразделения, круглосуточно выявляющие инциденты, скапливающиеся в SIEM-системах, и реагирующие на них.

Если инцидент произошел, и служба ИБ узнала о нем не из отчетов СЗИ, а, например, от клиента организации, данные которого были похищены, то проводится расследование. Злоумышленнику свойственно заметать следы преступления, в частности, удалять файлы с записями о событиях, то расследовать киберпреступление, как и любое другое, легче всего по горячим следам. Поэтому, столь важно внедрять именно превентивные меры по защите информации, которые снижают вероятность того, что инцидент произойдет. Что касается того, какие решения нужны, в первую очередь, конкретной компании, то здесь имеет смысл еще раз вернуться к риск-ориентированному подходу, оценке активов и возможного ущерба для них, после чего определить приемлемый остаточный риск и подобрать необходимые СЗИ.

Гораздо сложнее приходится с внутренними злоумышленниками, инсайдерами, которые имеют легитимный доступ к информации. Здесь на помощь, помимо уже упомянутых DLP-систем и автоматизирован-

ных систем контроля сотрудников, приходят организационные меры, в том числе, ранее упомянутое сдерживание — к примеру, информирование сотрудников об ответственности за разглашение коммерческой тайны, оповещение о введенном режиме коммерческой тайны и т.д.

Как уже говорилось, конкретный список решений по защите от НСД определяется требованиями законодательства и теми рисками для компании, которые рассчитаны с учетом частной модели угроз, т.е. актуальных векторов атак (виды угроз приведены в разделе 1), а также тех СЗИ, которые уже внедрены. Для расчета рисков полезно использовать автоматизированные решения класса GRC (Governance, Risk management and Compliance), которые рассматривают риски ИБ по модели «бизнес-процесс — информационные системы — аппаратное обеспечение». В них существует «workflow, в графическом интерфейсе которого прорисовываются бизнес-процессы организации, и на них накладывается информация об активах, как правило, есть возможность импорта информации из CMDB (*англ.* Configuration Management Database — база данных управления конфигурации) источников или сканеров безопасности.

Оценка рисков бывает количественная и качественная. Качественная оценка оперирует понятиями высокий, средний и низкий уровень риски, количественная оценка стоимостью активов и стоимостью реализации рисков. При этом один из классических подходов к оценке рисков учитывает количество инцидентов для того или иного актива за прошлые годы. Дело в том, что стоимость защитных мер, рассчитанная с учетом вероятности инцидента, основанной на статистике, не должна превышать ущерба от потери актива. Но если, например, в течение 10 лет не было кражи коммерческой тайны из организации, это не значит, что такое не случится в будущем. Вопросы управлении рисками ИБ рассматриваются в разделе 15.

Защита от несанкционированного доступа — это базовая задача специалистов по ИБ, которая решается с помощью применения различных организационных и технических защитных мер. В случаях, предусмотренных законодательством, для защиты информации от НСД необходимо действовать на основе Руководящих документов ФСТЭК России. С точки зрения технических мер, защита от НСД — это комплекс превентивных мер (IDM-решений, патч менеджмент) и мониторинга инцидентов ИБ, например, SIEM-системы.

Вопросы для самопроверки

1. Для чего нужен патч-менеджмент?
2. В чем отличие мандатного управления доступом от ролевого?
3. От каких угроз защищают EMM-решения?
4. Есть ли разница в защите СВТ от НСД и АС от НСД?

5. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Принято считать, что все способы компрометации информации, которые существуют в современном мире, используют исключительно вредоносное ПО, устанавливаемое на рабочие станции и сервера. Но это далеко не так. Когда речь идет, например, о государственной тайне, служебной тайне или другой информации, представляющую особую ценность, киберпреступниками могут быть использованы программно-аппаратные решения, основанные на иных принципах.

Они могут быть гораздо более изощренными нежели шпионские программы, распространяемые через электронную почту, флэшки или мессенджеры, но когда в организации, ставшей целью злоумышленников, приобретены и используются межсетевые экраны нового поколения, сканеры уязвимости, антивирусы, средства защиты от продвинутых угроз на шлюзе и конечных станциях, проведено обучение персонала и т.д., то злоумышленники используют инструменты из другого арсенала. Основные технические каналы для получения нелегитимного доступа к информации:

- электромагнитные, электрические и индукционные каналы;
- акустические, электроакустические, виброакустические, оптико-электронные (лазерные) и параметрические каналы;
- визуальные каналы;
- материальные каналы.

Электромагнитные каналы используют ПЭМИН, которые всегда существуют при работе компьютерной техники. Перехват ПЭМИН осуществляется в моменты обработки информации, например:

- ввод данных с клавиатуры;
- чтение и запись информации на съемные носители;
- вывод информации на монитор;
- отправка информации в канал связи;
- вывод информации на печатающие устройства и т.д.

Перехват ПЭМИН по цепям электропитания и заземления представлен на рис. 2.

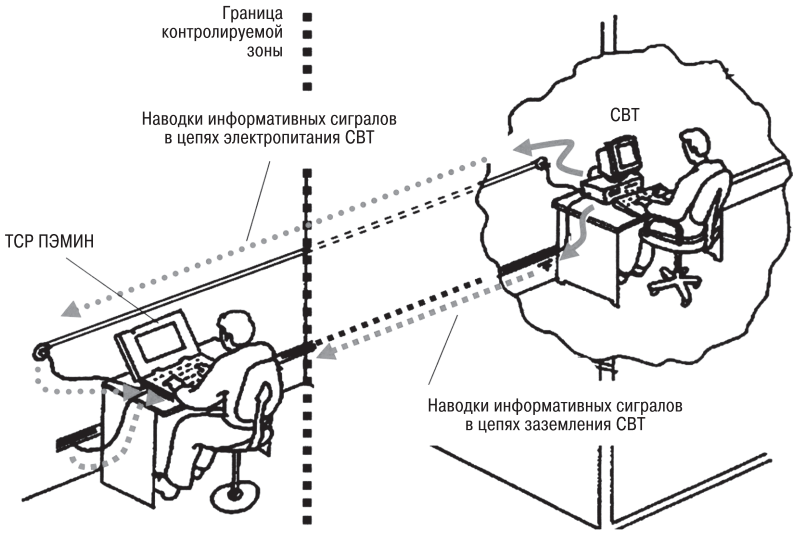

Рис. 2. *Перехват информации с помощью средств разведки ПЭМИН по цепям электропитания и заземления*

Чтобы была понятна актуальность проблемы, достаточно сказать, что мощность электромагнитного излучения у старых мониторов была такой, что съем информации с них был возможен на расстоянии более километра, и с целью блокировки такой незаконной деятельности устанавливались специальные экранирующие сетки. Сейчас расстояние, на котором можно снимать информацию с мониторов, снизилось до нескольких десятков метров. Но из-за большого числа не заглушенных USB-разъемов, записи информации на внешние твердотельные накопители, подключенных устройств аудио вывода, а главное недостаточной осведомленности организаций и людей об этой проблеме, все равно эта проблема остается животрепещущей.

Комплекс для анализа и расшифровки ПЭМИН состоит из антенны, комплекса по обработке сигнала и программного решения по его декодированию, использующего статистические методы для удаления «шума». При идеально настроенной системе и минимальных помехах декодирование электромагнитных сигналов при вводе простой текстовой информации может осуществляться практически, в режиме реального времени.

Бороться с атаками, использующими ПЭМИН, можно используя разнообразное оборудование для генерации электромагнитного шума, заземление проводов, а также виртуальную клавиатуру вместо физической в тех приложениях, где это возможно. Не стоит забывать и о том, что существуют портативные средства радиоразведки, кото-

рые используются в электромагнитных каналах утечки информации, способные перехватывать телефонные переговоры.

Электрические каналы используют непосредственное подключения к кабелям для перехвата информации через специальные согласующие устройства или устройства компенсации падения напряжения для того, чтобы скрыть факт подключения к линиям связи. Индукционные каналы утечки информации, в отличие от электрических, не требуют контакта с линией связи. В данном случае используются специальные датчики, фиксирующие электрические сигналы, возникающие в электромагнитном поле вокруг кабеля.

Следующий вид информации, которую можно перехватывать по техническим каналам связи, это речевая информация. Ее можно улавливать с использованием акустических, электроакустических, виброакустических, оптико-электронных и параметрических каналов. Все эти каналы различаются средой распространения и методами съема информации.

В акустических каналах для съема речевой информации, т.е. сигналов, передаваемых по воздуху, используются специальные направленные микрофоны, соединяемые со звукозаписывающими устройствами и передатчиками. Виброакустические каналы подразумевают использование строительных конструкций, т.е. непосредственно самого помещения, а также труб отопления, вентиляции и других, в которых возникают колебания, вызываемые акустическими сигналами, т.е. речью, регистрируемые соответствующими устройствами.

Для съема информации в таких каналах используются вибродатчики и электронные радиостетоскопы, устанавливаемые в стенах, или с внешней стороны окна. Радиостетоскоп регистрирует колебания и передает информацию на специальный портативный комплекс, где она впоследствии обрабатывается. Для защиты от такой атаки используют комплекс виброакустической защиты, в который включается, в частности, генератор шума, а также системы виброзашумления.

Благодаря возможности преобразования акустических сигналов в электрические существуют электроакустические каналы утечки информации. Под действием акустического поля трансформаторы, катушки индуктивности, электромагниты, находящиеся в офисных устройствах, могут изменять емкость, индуктивность и т.д. Это приводит модуляции токов или появлению ЭДС. С помощью подключения к соединительным линиям специальных усилителей возможен перехват электроакустических колебаний, и в частности, прослушивание разговоров.

Оптико-электронный канал утечки акустической информации подразумевает перехват речевой информации с помощью лазерного зондирования оконных стекол, когда используется зеркальное отражение лазерного луча. При этом в определенных ситуациях, например, когда расстояние до окна не более 50 метров, используется диффузное отражение лазерного луча. Параметрические каналы утечки информа-

ции появились благодаря возможности воздействия высокочастотным сигналом на электронные устройства. С помощью него в помещении, где установлены специальные полуактивные закладные устройства, параметры которых, такие как добротность, меняются по закону изменения акустических сигналов. Для перехвата информации также используется передатчик высокочастотного излучения и приемник.

В визуальных (видовых) каналах утечки данных используется фотографирование информации с экранов, копирование информации и прочие аналогичные методы, которые могут применяться и инсайдерами. Кроме того, надо иметь в виду, что киберпреступниками может быть перехвачено управление системой видеонаблюдения в офисе, что может тоже относится к визуальному каналу утечки. Также, не стоит забывать о возможности установки скрытых, миниатюрных камер и тепловизоров в офисе организации. С помощью методов нелинейной локации возможно обнаруживать все работающие видеокамеры в силу того, что каждая камера имеет определенный спектр побочного излучения.

Серьезным каналом утечки информации является материальный канал. Как ни парадоксально, но мусор, в том числе производственные отходы могут быть источником ценной информации о производимой продукции, а офисный мусор — конфиденциальной информации и коммерческой тайны. Мы очень часто, не задумываясь, выбрасываем в мусорные корзины документы, которые могут быть очень интересны нашим конкурентам и другим третьим лицам. Поэтому не стоит забывать о необходимости использования шредеров. Что касается последних двух каналов, то очень важным элементом защиты являются организационные меры, проведение мероприятий по повышению осведомленности персонала, а также сдерживающие меры, направленные против инсайдеров.

Необходимость проверки оборудования, использующегося при обработке государственной и служебной тайны, а также помещений, в котором данное оборудование установлено, определяется указом президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». В нем говорится, что «... размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях...»

Нормативная база в этой области разрабатывается ФСТЭК России (ранее Гостехкомиссия России), ФСБ России и СВР России. Она за-

трагивает различные виды информации ограниченного доступа, в том числе, и персональные данные. В базовой модели угроз безопасности персональным данным при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 15.02.2008, рассматриваются угрозы, связанные с утечкой по каналам ПЭМИН, речевой и видовой информации.

Есть упоминание об этом и в приказе ФСТЭК от 18.02.2013 № 21 «Об утверждении состава организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также приказе ФСТЭК от 15.07.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». В этих приказах существует мера ЗТС.1. Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам. В информационном сообщении ФСТЭК России от 15.07.2013 № 240/22/2637 сказано, что в качестве методического документа для защиты информации в государственных информационных системах от утечек информации по техническим каналам (17-й Приказ ФСТЭК России) требуется применение все еще остающегося актуальным СТР-К (Специальные требования и рекомендации по технической защите конфиденциальной информации Гостехкомиссии России, принятые решением Коллегии Гостехкомиссии от 02.03.2001 № 7.2).

Для проверки оборудования на наличие скрытых закладных устройств, которые могут использоваться для получения информации по вышеуказанным техническим каналам, а также отсутствия благоприятных факторов для утечки информации по техническим каналам проводятся специальные проверки, обследования и исследования. Этот комплекс мероприятий обязателен к проведению для предприятий, обрабатывающих государственную тайну, но может использоваться и коммерческими компаниями, которые хотят быть уверенными в том, что их информация не может быть получена злоумышленниками по техническим каналам.

Говоря о специальных проверках оборудования, надо сказать, что в основном речь идет об оборудовании иностранного производства, а также отечественного, содержащего иностранные комплектующие. При проведении проверки техническое средство передается в лабораторию, имеющую требуемые лицензии ФСТЭК России и ФСБ России, а также аттестат аккредитации органа по аттестации. В соответствии с программой проверки технического средства проводятся специальные работы, и в случае положительного заключения выдается комплект документов, отправляемый в режимный отдел предприятия, а на само техническое средство наклеивается специальный голографический знак.

Если специальные проверки позволяют найти закладные устройства в технике, то специальные исследования проводятся для выявления возможности передачи информации ограниченного доступа, т.е. конфиденциальной или гостайны, по техническим каналам утечки информации. Техника, например, может проверяться на уровень ПЭМИН и защищенность от утечек по этому каналу, а помещение на наличие акустических, виброакустических и других каналов. Говоря об угрозах утечки информации с помощью ПЭМИН, надо сказать, что есть различные методики анализа защищенности технических средств, основанных на измерении радиуса вокруг испытуемого устройства, и сравнении реального показателя напряженности электромагнитного поля с нормативным. Под радиусом подразумевается та зона, в пределах которой возможен перехват информации посредством ПЭМИН с нужным качеством.

Специальное обследование помещений предназначено для поиска в них закладных шпионских устройств и технических каналов утечки. При этом моделируются действия киберпреступника, и составляется список «жучков» различного действия. Затем с помощью специальных технических средств и осмотра производится обследование помещения для поиска возможных технических каналов, т.е. радиоэфира, вибро- и электроакустических каналов, ПЭМИН, после чего производится анализ и делаются выводы о необходимых мерах по исправлению положения. Результатом такого рода проверок должен являться аттестат помещения или оборудования на соответствие требованиям в области защиты государственной тайны или технической защите конфиденциальной информации на основании СТР-К.

Для похищения информации злоумышленниками используются не только шпионские программы, внедряемые в операционную систему или методы социальной инженерии, но и разнообразные устройства съема информации, использующие технические каналы утечки, например, акустический или ПЭМИН. Поэтому в определенных случаях, например, при создании аккредитованного удостоверяющего центра проводится проверка и аттестация помещений на отсутствие закладных устройств, а также специальная проверка компьютерной техники на отсутствие жучков и устойчивость к утечкам информации через технические каналы.

Вопросы для самопроверки

1. Каким образом злоумышленник может похитить информацию с помощью перехвата ПЭМИН?
2. В чем разница в перехвате информации по акустическому и виброакустическому каналу?
3. Что такое радиостетоскоп?
4. Для чего проводятся специальные проверки оборудования?

6. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Как уже говорилось ранее, цель обеспечения ИБ — это защита конфиденциальности, целостности и доступности информации. Также, мы говорили о подлинности и неотказуемости как о важных свойствах информации, подлежащих защите. Количество технических решений, стоящих на службе у специалистов по ИБ, очень велико — часть из них предназначена для защиты сетевого периметра организаций от внешних нарушителей ИБ, часть для защиты от внутренних нарушителей ИБ.

Возникает вопрос — если шпионское ПО смогло пробраться в локальную сеть и «притаиться», готовясь передавать злоумышленникам конфиденциальную информацию, или нелояльный сотрудник отправил конкуренту ценную информацию, означает ли это, что все рубежи обороны пройдены и информация скомпрометирована? Нет, если, скачав к себе на компьютер искомый файл, злоумышленник увидит «абракадабру» вместо искомого текста. Это делается с помощью средств криптографической защиты информации (СКЗИ).

Криптография — это наука о методах обеспечения конфиденциальности , целостности данных , аутентификации (проверки подлинности авторства или иных свойств объекта) и неотказуемости [6].

Сложно сказать, когда криптография берет свое начало, но по имеющимся данным ей уже более четырех тысяч лет. Как и в любой другой науке, можно проследить ее эволюционное развитие, которое начиналось с моноалфавитных шрифтов, до полиалфавитных, после чего наступила эра использования разнообразных устройств для шифрования. С наступлением эпохи всеобщей компьютеризации, наука пришла к использованию исключительно математических методов.

В настоящее время методы криптографической защиты информации находят свое применение в самых разных областях ИБ: для защиты обладателей прав на цифровой контент с помощью DRM-технологий (*англ.* DRM — Digital Rights Management), для защиты каналов связи с помощью построения виртуальных частных сетей (*англ.* VPN — Virtual Private Network), для подтверждения подлинности сайта с помощью SSL-сертификатов (*англ.* SSL — Secure Sockets Layer) [19].

Как же работает шифрование? Чтобы конфиденциальность и целостность информации не были скомпрометированы, необходимо привести ее определенным образом в нечитаемый вид, и сообщить партнеру алгоритм шифрования, которым вы воспользовались. К примеру, в знаменитом шифре Цезаря буквы сдвигались на три буквы вправо. В этом случае фраза «Привет, мой друг» пишется как «Тулезх, псм жуце». Вы можете отправить эту фразу коллеге, договорившись с ним предварительно, что для шифрования переписки используете шифр Цезаря как самый простой.

Данный шифр относится к шифрам подстановки, т.е. все символы заменяются на другие из алфавита, находящиеся на определенном расстоянии. Безусловно, пользоваться в настоящее время им для ведения переписки и обработки информации ограниченного доступа не стоит, так как при современных вычислительных мощностях взлом такого шифра не является сложным.

Развитием идеи подстановочных шифров стали полиалфавитные шифры, к которым относятся шифр Виженера и шифр Гронсфельда, которые мы и рассмотрим. Если в случае простейших шифров типа шифра Цезаря достаточно просто знать количество символов, на которое осуществлен сдвиг и направление, то в полиалфавитных шифрах уже появляется понятие ключа.

Этот метод является простой формой многоалфавитной замены. Впервые его описал итальянец Джован Баттиста Беллазо (*Giovan Battista Bellaso*) в 1553 году, однако в XIX веке получил имя французского дипломата и криптографа Блеза Виженера (Vigenère; 1523–1596). Шифр Виженера представляет собой матрицу, представленную на рис. 3.

Для того чтобы зашифровать текст, требуется придумать ключевое слово, которое надо повторить столько раз, сколько символов есть в исходном тексте и на пересечении символа исходного текста и соответствующего символа ключевого слова будет символ из шифротекста. Предположим, наш исходный текст такой: *I love my job*. (англ. «Я люблю свою работу»). Пусть ключевое слово «work». В исходном тексте десять символов, значит, ключ будет выглядеть так «workworkwo». Начинаем шифрование текста. Находим пересечение буквы *I* в столбце и буквы *W* в строке, на их пересечении находится буква *D*. В результате мы получаем шифротекст «E zffa ap tkp». Зная ключ и выполняя обратную последовательность действий, очень быстро можно восстановить исходный текст.

На протяжении определенного времени шифр оставался неуязвимым, но по мере развития криптографии и методов анализа шифров, это неуязвимость исчезла, говоря словами А. С. Пушкина, «как сон, как утренний туман». Главный недостаток данного шифра — повторяющийся ключ. Уже в XIX веке были разработаны алгоритмы, связанные с определением длины ключа, и задача взлома

шифра Виженера была успешно решена, причем несколькими специалистами одновременно. Первым это удалось Чарльзу Бэббиджу (*Charles Babbage*; 1791–1871) — английскому математику, изобретателю первой аналитической вычислительной машины — прообраза современной ЭВМ.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рис. 3. *Шифр Виженера*

Другой разновидностью полиалфавитных шифров является шифр Гронсфельда, созданный руководителем первой дешифровальной службы Германии в XVII веке. Шифр можно считать усовершенствованием шифра Цезаря (надежность) и Виженера (скорость). В шифре Гронсфельда ключ является числом, повторяющимся столько раз, чтобы его длина равнялась длине оригинального текста. Для шифрования

текста надо каждый символ заменить на символ, отстоящим от него справа на указанную в ключе соответствующую цифру. Можно также воспользоваться таблицей Гронсфельда.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Исходный текст из предыдущего примера *I love my job* с ключом 1973197319 будет зашифрован в виде шифротекста J vwyf wl mpk. Справедливости ради надо отметить, что и данный шифр скорее является частью истории мировой криптографии, нежели реально действующим в настоящее время, поскольку атаки на него также разработаны очень давно, а от шифра Виженера он скорее отличается не надежностью, а скоростью, опять же в историческом контексте, с использованием современных вычислительных средств любой из этих шифров взламывается очень быстро.

Также надо обратить внимание, что возможна подстановка символов не одиночных символов, а целыми группами, например, так называемыми биграммами, когда подменяются группы по два символа. Надо сказать, что все вышеприведенные шифры являются представителями симметричного шифрования, т.е. ключ для шифрования и дешифрования текста используется один и тот же.

Шифры перестановки относятся также к симметричному шифрованию, но в отличие от подстановочных шифров здесь символы меняются местами по определенному алгоритму, определенному ключом. При этом количество циклов перестановки может быть сколько угодно большим, поэтому и существует разновидности шрифтов перестановки, начиная от шифров одинарной и заканчивая шифрами множественной перестановки.

Для наглядности использование шифров перестановки можно отобразить в виде прямоугольника, разбитого на ячейки, в каждой из которых находится символ. На рис. 4 показан пример шифра перестановки.

Я	И	С	К	Р	Е	Н	Н
Е	Л	Ю	Б	Л	Ю	С	В

О	Ю	Р	А	Б	О	Т	У

Рис. 4. *Пример шифра перестановки*

Можно, например, зашифровать данное сообщение «Я ИСКРЕННЕ ЛЮБЛЮ СВОЮ РАБОТУ» по вертикалям снизу вверх, начиная с первого столбца. Шифротекст будет выглядеть так «ОЕЯЮЛИРЮСАБКБЛРОЮЕТСНУВН». Это называется маршрутная перестановка. Существуют и другие методы перестановки, например, вертикальная перестановка, в которой используется ключ, и т.д.

Кроме того, все симметричные шифры делятся на блочные и поточные. Симметричное шифрование, несмотря на его простоту, скорость работы и меньшую по сравнению с ассиметричным шифрованием длину ключа, имеет и недостатки. Один из ключевых недостатков заключается в том, что ключ передается по открытому каналу связи, и может быть скомпрометирован. Требуется организация защищенного VPN (*англ*. Virtual Private Network — виртуальная частная сеть) канала связи. Кроме того, управление ключами в больших сетях затруднительно. Есть и функциональные ограничения, например, использовать симметричную криптографию для электронной подписи нельзя в связи с тем, что ключ известен каждой стороне.

Как уже говорилось, другой тип шифрования называется асимметричным. Он лишен тех недостатков, которые есть в симметричной криптографии, хотя, безусловно, не лишен своих собственных. Проще всего такой тип шифрования проиллюстрировать ситуацией, когда вы закрываете дверь в квартиру одним ключом, а открываете другим, поскольку первый ключ служит только для закрывания замка. К слову, есть технологии, которые используют сочетание асимметричного и симметричного шифрования, например SSL (англ. Secure Sockets Layer — уровень защищенных сокетов).

Асимметричное шифрование нашло широкое применение в современном мире в инфраструктуре открытых ключей для подтверждения подлинности цифровой личности, т.е. создания электронной подписи, шифрования сообщений, а также в технологии SSH (англ. Secure Shell — безопасная среда).

Основы асимметричной криптографии были заложены американскими криптографами Уитфилдом Диффи (*Whitfield ‘Whit’ Diffie*; р. 1944) и Мартином Хеллманом (*Martin Hellman*; р. 1945), авторами знаменитого алгоритма Диффи — Хеллмана. В асимметричной криптографии используется два ключа: открытый и закрытый, которые связаны друг с другом настолько сложными математическими алгоритмами, что вычислить один ключ на основе другого практически невозможно. Открытый ключ используется для шифрования информации, например, сообщений, а закрытым ключом информация расшифровывается.

Кроме того, открытый ключ используется для проверки электронной подписи его владельца. Для подтверждения подлинности открытого ключа используются электронные сертификаты, но об этом мы поговорим подробнее в разделе 7.

Использование асимметричного шифрования, например, для подписи сообщений и однозначной идентификации отправителя, основано на так называемых односторонних функциях, которые представляют собой математические алгоритмы, позволяющие зашифровать текст, но не дающие возможности его расшифровать. Если кратко описать идею односторонней функции, то речь идет о том, что по известному x можно найти значение функции $f(x)$, а обратная задача — определение x на основе $f(x)$ не решается. Поскольку это делает невозможным практическое применение односторонних функций, то существует «секрет» расшифровки информации. Это некий «y», по значению которого, а также зная $f(x)$, можно вычислить значение «x».

Практически это означает, что получатель информации формирует открытый ключ и закрытый ключ, который и является тем самым секретом, при этом открытый ключ он передает отправителю. Отправитель с помощью открытого ключа шифрует информацию, а расшифровать ее может только тот, у кого есть и открытый и закрытый ключ. Наиболее известными алгоритмами ассиметричного шифрования являются *RSA*, а также алгоритм Диффи-Хеллмана.

Одним из примеров применения односторонней функции без использования секретов является аутентификация в удаленной информационной системе, которая требует ввода паролей для пользователей. Необходимо обезопасить пароль от его компрометации, в первую очередь, запретить хранение пароля в открытом виде на сервере, например, в базе данных. Для этого в базе сохраняется не сам пароль, а результат выполнения функции на основе двух аргументов: имени пользователя и пароля. При вводе имени пользователя и пароля вычисляется функция, и, если имя пользователя и пароля введены правильно, искомое значение функции совпадает с вычисленным при старте сессии и доступ разрешается. При этом обратное вычисление пароля на основе функции не представляется возможным.

Бывают ситуации, когда такая возможность становится необходимостью. Предположим, нам требуется зашифровать слово «Студент». Мы можем взять список студентов вуза, или справочник жителей города, и для каждой буквы случайным образом выбрать человека и его телефонный номер. Пример реализации односторонней функции с «секретом» показан на рис. 5.

Исходный текст	Случайная фамилия	Криптотекст
С	Самойлов	3789389

Т	Торопенко	8293049
У	Уваров	1839029
Д	Денисов	4827490
Е	Евтеев	8472047
Н	Носенко	6574829
Т	Тимофеев	3947290

Рис. 5. *Пример реализации односторонней функции с «секретом»*

Таким образом, слово СТУДЕНТ будет выглядеть как 3789389928 3049183902948274908462047657482939472 90. Легитимный получатель сообщения знает об этом справочнике и может расшифровать сообщение. Крайне важным для односторонней функции является ее стойкость к взлому, а также минимальная вероятность возникновения коллизии для хэш-функций, когда мы имеем два различных входных блока данных для одной хэш-функции.

Хэш-функция — это разновидность односторонней функции, при которой массив данных произвольной длины преобразуется в битовую строку фиксированной длины, другими словами, осуществляется хеширование. Хэш-функция является очень популярной для хранения разных данных, например, биометрической информации или паролей. Также, она применяется для выработки электронной подписи, когда подписывается не сообщение, а его хэш.

Криптография является одной из древнейших наук, и издревле люди использовали ее для защиты конфиденциальности, при этом криптографические методы постоянно совершенствовались. Криптографические методы делятся на симметричные и ассиметричные, в зависимости от того, используется ли для шифрования и расшифрования один и тот же или различные ключи. Одним из ключевых понятий в криптографии является хэш-функция, используемая, например, для удостоверения электронной подписи.

Вопросы для самопроверки

1. Что такое шифр Виженера?
2. Чем отличаются шифры подстановки от шифров перестановки?
3. В чем достоинства и недостатки симметричного шифрования?
4. Что такое поточный шифр?

7. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ЭЛЕКТРОННОЙ ПОДПИСИ

Эпоха всеобщей цифровизации принесла с собой новые понятия, одно из которых — цифровая личность. Действительно, одна из ключевых особенностей интернета — это возможность выражать свои мысли анонимно. Фактически это означает, что любой может написать письмо от имени другого человека, написать сообщение на форуме, используя любые имя и фамилию, и проверить — кто это был на самом деле, довольно сложно. А учитывая скорость, с которой распространяется информация по интернету, этой анонимностью пользуются злоумышленники, преследуя, порой, неблаговидные цели.

В мире бизнеса последствия такого рода анонимности также могут быть весьма опасны. Представьте, что вы работаете бухгалтером в торговой компании, и получаете письмо от генерального директора, который в этот момент находится в отпуске с ограниченным доступом к средствам связи. В письме он пишет, что нужно срочно оплатить счет поставщику на большую сумму. Что делать? Телефон директора недоступен. Если в компании не установлена система электронного документооборота, и нет удостоверяющего центра (УЦ), который создает электронную подпись, удостоверяющую вашу цифровую личность, то возможно, став доступным, ваш руководитель будет крайне и неприятно удивлен, поскольку не давал такого распоряжения.

Цифровая личность — это идентификационная информация, позволяющая однозначно определить человека в цифровом пространстве. Важно обратить внимание на то, что признание личности может носить юридический характер, т.е. используемые средства подписания документов принимаются или на территории всей Российской Федерации, или теми сторонами, с которыми об этом имеется соответствующее соглашение. При этом не стоит забывать, что важно также соблюдать условия, при которых обеспечивается отсутствие компрометации электронной подписи, хранимой на специальных токенах,

например, двухфакторная аутентификация на рабочей станции, но об этом чуть позже.

Итак, мы установили, что для того, чтобы электронный документ имел юридическую силу, компания должна иметь или собственный удостоверяющий центр, или, если количество используемых электронных подписей не очень велико, приобретать сертификат электронной подписи. Ключевым законом, регулирующим вопросы, связанные с электронной подписью, является Федеральный закон Российской Федерации от 06.04.2011 № 63 «Об электронной подписи».

Электронная подпись — это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию. Сертификат ключа проверки электронной подписи — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом, либо лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Механизм электронной подписи использует криптосистему с открытым ключом, т.е. асимметричную криптографию, о которой мы говорили выше. С помощью открытого ключа можно проверить подпись владельца. Наиболее распространенным способом организации управления сертификатами ключей является PKI (*англ.* Public Key Infrastracture — инфраструктура открытых ключей) — централизованная модель управления ключами, но существует и децентрализованная модель, которая используется, например, в PGP.

Инфраструктура открытых ключей функционирует так. Есть два ключа — закрытый и открытый. Закрытый ключ известен только его владельцу. Открытый ключ содержится в сертификате, который выпускает удостоверяющий центр, и этот сертификат удостоверяет факт того, что закрытый ключ известен владельцу.

Сертификат открытого ключа содержит такую информацию как открытый ключ владельца сертификата, срок действия сертификата, имя центра сертификации, имя владельца сертификата и цифровую подпись. Именно цифровая подпись гарантирует невозможность подделки сертификата, благодаря использованию односторонних криптографических функций или, по-другому, хэш-функций, о которых мы говорили ранее. Другими словами, цифровая подпись создается как результат криптографической хэш-функции от данных сертификата, зашифрованного закрытым ключом центра сертификации.

У центра сертификации, или удостоверяющего центра, есть свой открытый ключ, с помощью которого любой человек может расшифровать цифровую подпись сертификата, после чего происходит вычисление и сравнение хэшей. Если хэш совпадает, то сертификат действителен,

что является подтверждением того, что открытый ключ принадлежит именно тому, с кем мы предполагаем обмен той или иной информацией. Квалифицированный сертификат электронной подписи является подтверждением ключа проверки электронной подписи соответствующим требованиям, установленным ФЗ-63 и иными правовыми актами. Отметим, что аккредитация удостоверяющего центра — признание уполномоченным федеральным органом соответствия его требованиям ФЗ-63.

В контексте данных определений важно понять, какие виды электронных подписей существуют, суть аккредитации удостоверяющего центра, а также способы и ограничения в применении тех или иных видов электронной подписи. Статья 5 вышеупомянутого федерального закона говорит о том, что все электронные подписи делятся на простую и усиленную. А усиленная электронная подпись, в свою очередь, делится на усиленную квалифицированную и усиленную неквалифицированную электронную подпись. В чем же между ними разница?

Если простая электронная подпись позволяет подтвердить факт ее формирования тем или иным лицом с использованием паролей или кодов, то усиленная подпись позволяет кроме того определить факт внесения изменений в документ после его подписания, т.е. является средством проверки целостности документа. Она создается криптографическим методом с помощью ключа электронной подписи. Разница между неквалифицированной и квалифицированной электронной подписью заключается в том, что открытый ключ квалифицированной электронной подписи находится в квалифицированном сертификате, который выдается аккредитованным удостоверяющим центром УЦ. С точки зрения практического использования, создавать ли свой УЦ и проводить ли процедуру его аккредитации зависит от задач, а также масштабов использования электронной подписи в организации.

Если речь идет о десятках электронных подписей, которые должны быть юридически значимы по всей территории Российской Федерации, то имеет смысл раз в год покупать требуемое количество электронных подписей, заверенных сертификатом одного из крупных аккредитованных в Минкомсвязи РФ. Если количество электронных подписей, которые выдаются сотрудникам, измеряется сотнями, то имеет смысл организовать собственный УЦ.

Если количество контрагентов, с которыми надо организовать юридически значимый электронный документооборот (ЭДО) не очень велико, то достаточно в рамочные договора о поставках товаров внести пункт о том, что используемая неквалифицированная усиленная электронная подпись (ЭП) признается в отношениях между данными организациями юридически значимой. Если же речь идет о сотнях, тысячах ЭП, и при этом в силу обстоятельств или особенностей бизнеса ЭП должна быть квалифицированной, то тогда надо создавать свой УЦ и проводить процедуру его аккредитации.

Заметим, сертификаты электронной подписи записываются на специальные токены или смарт-карты. Одна из проблем с ними в том, что они могут ломаться, и, если речь идет о большом количестве носителей, бизнес-процесс может оказаться под ударом. Альтернативным решением является программно-аппаратные криптографические модули HSM (*англ.* Hardware security module — аппаратный модуль безопасности). Эти устройства, выполняемые в формате одноюнитового сервера, представляют собой новое поколение решений по управлению ЭП. Известны компании, которые отказываются от использования токенов и смарт-карт в пользу централизованного хранения ключей пользователей ЭДО в таких устройствах. Используются они и в облачных сервисах ЭП, предлагаемых рядом крупных УЦ. Среди типовых для HSM функций — создание и хранений ключей администраторов УЦ, формирование и проверка электронной подписи, хеширование данных и т. д. В силу своих возможностей HSM-решения также нашли свое применение в банках при подключении к единой биометрической системе.

Рассмотрим, из каких элементов состоит система электронного документооборота с использованием электронной подписи. Ключевым элементом является удостоверяющий центр, который, как уже говорилось ранее, отвечает за выпуск сертификатов открытых ключей и управление ими. В настоящее время разработаны решения, позволяющие в единой консоли вести учет ключевых носителей различных производителей, а также осуществлять управление сертификатами. В состав УЦ входят центры сертификации и регистрации, автоматизированное рабочее место (АРМ) пользователя, АРМ администратора и АРМ разбора конфликтных ситуаций.

Центр сертификации отвечает за выпуск сертификатов ключей и за управление списком отозванных сертификатов. Центр регистрации ответственен за ведение базы данных пользователей, списка сертификатов и т.д. Также он является интерфейсом для доступа к объектам УЦ. Именно в центр регистрации поступают запросы от АРМ администраторов и обычных пользователей УЦ, а он обеспечивает их обработку.

АРМ администратора центра регистрации — компонент, который позволяет выполнять операции по регистрации пользователей, формировать закрытые ключи и запросы на сертификаты открытых ключей. АРМ разбора конфликтных ситуаций позволяет осуществлять операции по подтверждению подлинности ЭП и устанавливать статус сертификата открытого ключа. АРМ пользователя УЦ — это, как правило, веб-приложение, которое находится в центре регистрации и предназначено для регистрации пользователей, а также формирования ключей и запросов на сертификаты открытых ключей. На рис. 6 представлена типовая схема структуры УЦ.

Важнейшим элементом в организации процесса подписания документов с помощью ЭП служит крипто провайдер — программное

обеспечение, которое выполняет криптографические операции и обеспечивающее функционал авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями. Надо отметить, что существуют USB-токены и смарт-карты, сами являющиеся средством криптографической защиты информации, сертифицированные ФСБ России и являющиеся в этом смысле самодостаточными, не требующими установки на рабочую станцию специализированного ПО.

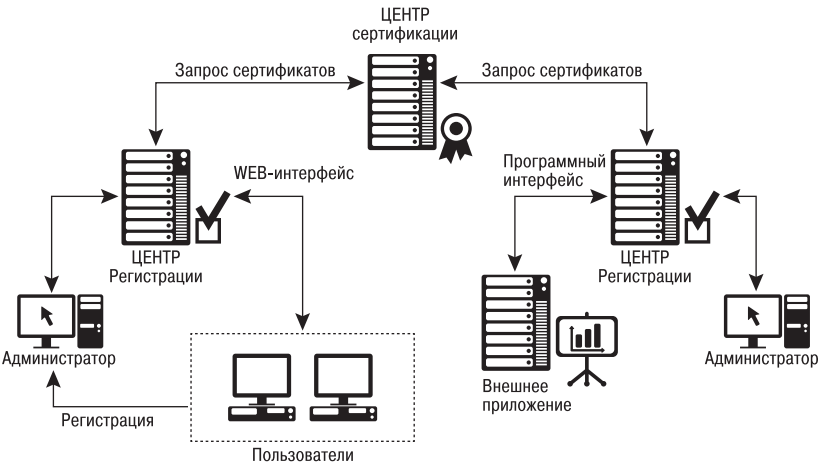

Рис. 6. *Типовая схема структуры УЦ*

Заметим, что токены и смарт-карты могут служить средством двухфакторной аутентификации, например, смарт-карты можно использовать для прохода через турникет (если она содержит RFID-метку), как способ подписания документов, а также для аутентификации в локальной сети по сертификату с вводом ПИН-кода для дополнительного усиления безопасности. В зависимости от стоящих задач необходимо использовать разные виды электронной подписи, которая может быть простой, усиленной, квалифицированной. При большом количестве ЭП активно начинают использоваться HSM-устройства, обеспечивающие полный цикл работы с ЭП, при этом необходимость использования токенов отпадает.

Вопросы для самопроверки

1. В соответствии с каким ФЗ осуществляются действия, связанные с ЭП, на территории РФ?
2. Чем отличается квалифицированная ЭП от усиленной?
3. Какую информацию содержит сертификат открытого ключа?
4. Что такое PKI?

8. УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ ИБ

Одно из ключевых понятий в ИБ — уязвимость — слабое место в информационной системе. Что же скрывается за этим термином? Вспомним известные инциденты в сфере компьютерных преступлений. Вирусы-шифровальщики Wanna Cry, Bad Rabbit, Petya, которые оставили без данных огромное количество людей и компаний, таргетированные атаки на объекты АСУ ТП и крупные финансовые организации.

Во многих случаях зловредное ПО, использованное хакерами, имело возможность функционировать на компьютерах жертв, благодаря одному из видов уязвимостей, а именно ошибкам в операционных системах. Программы могут содержать баги, которые впоследствии устраняются путем обновлений безопасности систем. Но эти обновления, или по-другому, патчи, т.е. программные заплатки, устраняющие уязвимости в ПО, не всегда своевременно выпускаются и моментально устанавливаются. В результате по данным СМИ, только ущерб от вируса WannaCry составил более миллиарда долларов США. Чтобы не допустить шифрования дисков, достаточно было установить критическое обновление Windows, выпущенное компанией Microsoft и устраняющее уязвимость в протоколе SMB (*англ*. Server Message Block).

Одним из основных видов является ошибка в коде системного или прикладного программного обеспечения, для исправления которой требуется установка специального обновления ПО. Говоря о других видах уязвимостей, можно назвать такие как слабый к взлому пароль, излишнее количество привилегированных учетных записей в локальной сети, большое число открытых портов, ошибки конфигураций и многие другие. В Российской Федерации действует ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». Данный национальный стандарт был утвержден приказом Федерального агентства по техническому регулированию и метрологии 19 августа 2015 г., а в ноябре 2018 г. переиздан. Ниже несколько ключевых определений из этого стандарта.

Уязвимость — это недостаток (слабость) программного (программно-технического) средства или информационной системы в целом,

который(ая) может быть использован(а) для реализации угроз безопасности информации.

Угроза безопасности информации — это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Уязвимость кода — это уязвимость, появившаяся в процессе разработки программного обеспечения. Все эти термины мы так или иначе уже обсуждали выше.

В этом же ГОСТе дается определения «организационной уязвимости», которая представляет собой уязвимость, появившуюся в связи с отсутствием организационных мер защиты информации или несоблюдением правил эксплуатации системы защиты информации. Как известно, одними лишь техническими мерами практически невозможно защититься от киберпреступников, которые становятся все более изощренными. Поэтому появилось целое направление, получившее название «security awareness», которое включает в себя целый ряд продуктов, призванных повысить осведомленность сотрудников по вопросам ИБ. Возвращаясь к стандарту, укажем еще одну важную характеристику уязвимости — «степень опасности уязвимости», выражающаяся числом, и определяющая подверженность информационной системы конкретной уязвимости с точки зрения влияния на нарушение свойств безопасности информации, т.е. конфиденциальности, целостности или доступности.

Не все уязвимости одинаково опасны, основной системой оценки уязвимостей является CVSS (англ. Common Vulnerability Scoring System). Эта система была разработана группой экспертов из целого ряда уважаемых компаний, и ей пользуются все основные разработчики сканеров уязвимостей и систем анализа защищенности в России и за рубежом. Более того, база данных уязвимостей ФСТЭК России также использует эту систему [9].

Оценка опасности уязвимости CVSS имеет десятибалльную шкалу и основывается на использовании трех групп метрик: базовых, временных и контекстных. С помощью базовых метрик описываются те характеристики уязвимостей, которые не зависят от того, где они эксплуатируются, а кроме того, никак не связаны с временным фактором.

Если уязвимость может быть эксплуатирована удаленно, то она опаснее той, которая может быть использована только локально. Поэтому, первой из базовых метрик является вектор доступа (англ. Vector access), который и описывает способ эксплуатации уязвимостей: локальный, локально-сетевой, когда уязвимость может быть эксплуатирована удаленно, но из смежных сетей или сетевой.

Следующей базовой метрикой является сложность проведения атаки (англ. Access complexity), где высокий уровень предполагает, что требуется выполнить определенную последовательность действий,

средний — когда уязвимость нельзя отнести к легко эксплуатируемой, но и нельзя отнести к сложно эксплуатируемой, ну и, как вы уже догадались, низкий уровень, когда уязвимость эксплуатируется достаточно просто. Следующей метрикой является метрика аутентификации, которая делится на многократную, если атакующему надо не менее двух раз пройти процедуру аутентификации, однократную, если это требуется сделать только один раз, и нулевую, когда аутентификация не требуется.

Также к базовым метрикам подсчета CVSS относятся метрики воздействия. Метрика воздействия на конфиденциальность делится на нулевое, когда воздействие отсутствует, частичное — если возможно считать часть данных и полное, когда есть полный доступ к данным. Естественно, что чем больше возможный доступ, тем опасней уязвимость. Такая же ситуация с метрикой воздействия на целостность, где выбор есть вариантов, когда уязвимость позволяет изменить часть данных, все данные или воздействие отсутствует, а также метрикой воздействия на доступность, где в зависимости от опасности уязвимость может вызвать полный отказ системы в обслуживании, временный отказ, равно как снижение производительности системы или же воздействие отсутствует.

Для удобства специалистов по ИБ количественные показатели CVSS объединены в группы по уровню опасности уязвимости. Так, уязвимости с оценкой 9–10 соответствуют критическому уровню опасности, 7–8,9 — высокому, 4–6,9 — среднему, 0,1–3,9 — низкому, и ниже 0,1 — информационному уровню, т.е. уязвимостям, которые не несут никакой опасности.

Помимо базовых метрик для расчета оценки уязвимости используются временные и контекстные метрики. Временные метрики связаны с характеристикой времени, и описывают наличие исправлений для уязвимости, которые недоступны или доступны, но представлены в разном виде от временного решения или рекомендаций до официального исправления от разработчика. Также к временным метрикам относится возможность использования уязвимости, которая варьируется от теоретической возможности до высокой, например, если эксплойт, т.е. программа, эксплуатирующая уязвимость присутствует в базе эксплойтов, а также степень достоверность источника, от неподтвержденной до подтвержденной, например, если о наличии уязвимости сообщил сам разработчик ПО.

К контекстным метрикам относятся вероятность нанесения косвенного ущерба (*англ.* CDP — Collateral Damage Potential — вероятность косвенного ущерба), где описываются экономические и технические потери от эксплуатации уязвимости. Она может быть нулевой, низкой, средней, повышенной или высокой. Также, к контекстным метрикам относится плотность целей (*англ.* Target Distribution), кото-

рая может быть нулевой, низкой, средней или высокой. Данная метрика демонстрирует, влияет ли наличие уязвимости только на одну цель или на множество целей.

Каким же образом обеспечить защиту компьютерных сетей и инфраструктуры от уязвимостей? У производителей операционных систем, например, Microsoft есть собственные средства проверки рабочих станций и серверов на наличие уязвимостей. Как правило, инфраструктура организаций представляет собой гетерогенную среду, в которой есть рабочие станции и сервера, как на базе Windows, так и Linux. Помимо этого, присутствует большое число сетевого оборудования, которое также надо проверять на наличие уязвимостей.

Существует специальный класс решений, который называется сканерами безопасности или системами анализа защищенности, позволяющими оперативно отслеживать наличие уязвимостей в сетях и своевременно их устранять. Для проверки исходного кода ПО на уязвимости также существуют специальные сканеры кода, но об этом мы поговорим отдельно. Среди ведущих разработчиков систем анализа защищенности можно выделить такие компании как Tenable, Rapid 7, Positive Technologiess, Qualys. Эти программы проводят инспекцию всей сети, идентифицируют имеющиеся хосты и сканируют их на наличие уязвимостей, отсортировывая их по степени опасности. Данные решения позволяют делать разнообразные аналитические выводы, позволяя определять скорость устранения уязвимостей в различных городах, или на разных объектах инфраструктуры, а также позволяют делать отчеты по соответствию различным стандартам ИБ. Также, некоторые из сканеров уязвимостей имеют сертификат ФСТЭК России, что позволяет их использовать для удовлетворения российских требований по обеспечению безопасности информации.

Заслуживают упоминания сканеры безопасности веб-приложений. Это очень важный класс решений, поскольку понятно, что уязвимости в веб-приложениях банков, операторов связи, интернет-магазинов могут приводит к очень серьезным инцидентам ИБ. Все основные сканеры уязвимости поддерживают сканирование веб-приложений, однако, существуют и специализированные решения, созданные именно для этой цели. Несмотря на то, что количество различных уязвимостей в веб-приложениях достаточно большое, есть список из наиболее опасных векторов таких атак, защиту от которых требуется организовывать в первую очередь. Они находятся в списке OWASP (*англ.* Open Web Application Security Project TOP-10).

На первом месте, как и ранее, находится SQL-инъекция. Это атака, которая использует определенные «дыры» в веб-приложениях для выполнения вредоносного SQL-кода. С помощью использования хранимых процедур, регулярных выражений, подготовленных запросов, ограничения прав на доступ к базам данных можно снизить риски

таких атак, ну а проверить на уязвимости, приводящие к таким атакам, можно с помощью сканеров безопасности.

На втором месте находится Broken Authentication. Атакой киберпреступника может являться в данном случае кража специального идентификатора, который сохраняется в хранилище браузера благодаря использованию *cookies* и который используется браузером при дальнейшем запросе страниц после того, как вы в первый раз произвели авторизацию в приложении и браузер это запомнил. Для защиты от таких атак можно проверять *IP*-адреса сессий, или наличие множества соединений в одной сессии и другими методами.

На третьем месте находится *Sensitive data exposure*, которая переводится как незащищенность критичных данных. При работе с веб-приложениями пользователи зачастую вводят очень важную персональную информацию вроде паспортных данных, номеров банковских карт и т.д. Один из основных способов защиты этих данных — использование сайтов https для шифрования вводимых данных, а также SSL-сертификаты с зеленой полосой, подтверждающие их принадлежности той компании, на чей сайт заходил посетитель.

На четвертом месте расположился такой вектор атаки, как *XML External Entities* (XXE). Это атака, при проведении которой анализируется ввод XML. Это, с одной стороны, не так часто встречающийся вектор, но, тем не менее, очень опасный, так как с помощью него можно похитить важные данные и даже исполнить произвольный код. Чтобы заблокировать такие атаки, надо использовать анализаторы статического кода для поиска XXE или IAST (англ. Interactive Application Security Testing), т.е. интерактивные анализаторы выполнения программ, применять WAF, использовать менее сложные форматы данных, такие как JSON и проверки XSD и т.д.

Среди прочих векторов атак такие как Broken Access Control — ошибка контроля доступа, когда доступ к данным приложения можно получить, например, простым перебором id-пользователя, Security Misconfiguration — небезопасная конфигурация, когда из-за несоблюдения требований ИБ при настройке веб-приложений, например, стоит возможной кража cookie, Cross-Site Scripting — межсайтовый скриптинг — ошибка валидации данных пользователя, позволяющая исполнить произвольный JavaScript в браузере, Insecure Deserialization — небезопасная десериализация, признающаяся одним из серьезнейших современных элементов атак на веб-приложения, особенно, в отношении Java-десериализации и т.д.

Если говорить об уязвимостях в компьютерных сетях как возможных векторов атак злоумышленников, которые находятся вне сети, то важной составляющей является правильная настройка листов доступа на межсетевых экранах, что особенно актуально в случае, если мы имеем дело с большой сетью и, соответственно, большим количеством

межсетевых экранов. В случае отсутствия централизованного аудита конфигураций файрволлов и управления ими, несогласованность действий разных системных администраторов может привести к тому, что к рабочей станции, на которой находятся важные документы, может быть случайно открыт доступ извне по тому или иному порту на всех файрволлах, находящихся между периметром и рабочей станцией.

Для того, чтобы таких проблем не возникало, разработаны специальные решения, позволяющие управлять файрволлами, определять актуальные вектора атак и автоматически приводить конфигурации сетевого оборудования в соответствии с политиками безопасности и стандартами ИБ.

Мы познакомились с понятием «уязвимость», методами их обнаружения и исправления. Слабые пароли, неустановленные обновления безопасности, повышенные привилегии на компьютерах дают возможность злоумышленникам проникнуть в сеть компаний и скомпрометировать информацию. Для борьбы с уязвимостями и эх эксплуатацией следует применять специализированные сканеры безопасности, в том числе, веб-приложений, повышать осведомленность персонала об угрозах ИБ, проводить тестирование на проникновение в локальную сеть.

Вопросы для самопроверки

1. Что такое CVSS?
2. Какие метрики оценки уязвимостей относятся к базовым?
3. Что относится к контекстным метрикам оценки уязвимостей?
4. В чем суть SQL-инъекции?

9. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Сетевая безопасность — это область ИБ, которая включает в себя средства защиты от внешних атак на ресурсы организации. Фактически речь идет о фиксации и блокировании попыток попадания во внутреннюю сеть зловредного трафика, содержащего различные вирусы, сигнатуры, свидетельствующие о попытках проникновения в сеть, сигнатуры «нулевого дня», которые могут стать началом таргетированной атаки на компанию и т.д.

Существуют две технологии защиты периметра сети, которые являются не взаимозаменяемыми, а, скорее, взаимодополняющими. Это МСЭ и шлюзы ИБ, или прокси-сервера с функционалом ИБ. Очень распространены устройства класса *Unified Threat Management*, которые, по сути, являются комбинацией обеих технологий. Заметим, что каждая из технологий претерпела эволюцию, и имеет смысл использовать для различных типов задач или межсетевые экраны нового поколения, или прокси-сервера. В каких случаях используют те или иные решения, мы сейчас и поговорим. Также, в этом разделе коснемся вопросов, связанных с отражением на сетевом уровне атак, использующих уязвимости нулевого дня и социальную инженерию, а также разберем устройства класса NAC (англ. *Network Access Control* — Контроль доступа к сети).

Чтобы понять разницу между МСЭ и прокси-сервером, давайте задумаемся — а какие основные задачи стоят перед администратором сети? Первая — предотвращение несанкционированного доступа к сети извне, вторая — облегчение задач, связанных с доступом к ресурсам в интернете для локальных пользователей с одновременным контролем ИБ, т.е. выполнение роли посредника между пользователем и ресурсом, к которому пользователь хочет получить доступ.

К слову говоря, прокси-сервер может играть и обратную роль, т.е. доступ ко внутренним ресурсам локальной сети для внешних пользователей. Тогда он называется реверс-, или обратный прокси-сервер. Фактически, прокси-сервер был одним из первых типов МСЭ. Среди тех функций, которые выполняет прокси-сервер, кэширование данных, что позволяет ускорять загрузку часто посещаемых ресурсов,

сжатие данных, что дает возможность экономить внешний или внутренний трафик, защиту сети от внешнего доступа, ограничение доступа к внешним ресурсам из локальной сети и т.д.

Большую популярность при решении целого ряда задач, например, защите привилегированных учетных записей получил такой тип прокси-сервера, как прозрачный прокси, когда трафик перенаправляется на прокси-сервер с помощью маршрутизатора, при этом неявно, без изменения настроек интернет-браузера и без специальных программ. Достигается это настройкой перенаправлением трафика с 80 порта на порт прокси-сервера.

Итак, мы определили, что существует три типа прокси-серверов: первый — шлюз, суть которого в том, что никаких изменений в режим диалог между пользователями и сайтами не вносится. Второй — это прямой прокси-сервер, который бывает открытым и внутренним. Разница между ними в том, что внутренние устанавливаются на границе сети и позволяют управлять доступом пользователей к сайтам, а открытые используются для анонимного посещения тех или иных сайтов. Третий тип прокси-серверов — это реверс-прокси. Также прокси-сервер может быть прозрачным, SOCKS-прокси, DNS-прокси, что часто применяется для защиты от DDOS-атак, веб-прокси — эти виды прокси-сервера зависят от конкретной инфраструктуры и способа применения прокси-сервера.

Нельзя не упомянуть и еще об одной тенденции, а именно увеличении в мировом масштабе доли облачных SWG-сервисов (англ. Secure Web Gateway — шлюз безопасного доступа) в общем объеме SWG-контрактов в области, хотя превалирующими пока являются программные и программно-аппаратные решения, устанавливаемы on-premise, т.е. в инфраструктуре заказчиков.

Перечислим функции SWG-решений, которые в большинстве своем присутствуют у основных решений, представленных на рынке:

- блокирование доступа к зараженным сайтам;
- блокирование опасных веб-приложений или конкретных действий в них;
- фильтрация URL-адресов на основе категорий, пользователей, групп и устройств;
- единые политики контроля для приложений и фильтрации URL;
- проверка SSL-трафика с возможностью установки исключений;
- подключение IPS-модулей;
- подключение при проверке трафика облачных сервисов с информацией о новейших угрозах;
- подключение модулей DLP (англ. Data Leak Prevention — предотвращение утечек информации) для контроля утечки конфиденциальной информации;

— сжатие и кэширование данных;
— аппаратное ускорение SSL-трафика;
— построение цепочки прокси-серверов;
— защита и контроль мобильных пользователей;
— настройка ограничений по посещению сайтов в зависимости от времени и пропускной способности;
— фильтрация IM-протоколов;
— разграничение прав доступа к ресурсам с помощью разнообразных механизмов аутентификации и на основании разных параметров: протоколы, порты, членство в группе, тип файла, категория сайта, ключевые слова, расписание и т.д.;
— ограничение скорости по типам трафика;
— возможность блокирования рекламных баннеров;
— наличие десятков отчетов о деятельности пользователей в интернете.

Как мы видим, функционал SWG-решений очень широк, и у этого класса устройств впереди долгая жизнь. Другим классом устройств, призванных обеспечить защиту, являются межсетевые экраны, задачей которых является фильтрация трафика, который проходит через них, по определенным правилам. Это несколько упрощенное определение, вместе с тем, оно отражает суть и принципиальное отличие их от прокси-серверов.

В сетевой модели *OSI* семь уровней, и проще всего описывать все существующие типы МСЭ именно по тому, на каком уровне модели они работают. На канальном уровне работают управляемые коммутаторы. Они работают с MAC-адресами и оперируя ими, могут обрабатывать, в том числе, блокировать те или иные данные. В связи с возможностью компрометации MAC-адресов, т.е. их подмены использование управляемых коммутаторов в качестве решения по обеспечению сетевой безопасности давно стало ненадежным, не говоря уж о том, что уже давно им на смену в контексте обеспечения ИБ пришли более современные решения.

Рассмотрим сетевой уровень модель *OSI*. На этом уровне работают пакетные фильтры, с которых фактически и начинается история межсетевых экранов. Они осуществляют блокировку трафика на основе чтения заголовков пакетов. Работая с протоколами сетевого уровня, некоторые из них также обрабатывают заголовки пакетов протоколов транспортного уровня *TCP/UDP*. Основная проблема пакетных фильтров заключается в опасности пропуска вредоносного кода, если он разделен на сегменты, часть которых выдает себя за легитимный контент. Работают пакетные фильтры достаточно быстро, но им с трудом удается анализировать высокоуровневые протоколы, и они подвержены атакам IP-спуфинга (от *англ*. spoof — мистификация), когда подделывается IP-адрес.

На сеансовом уровне модели *OSI* работают специализированные шлюзы, с помощью которых возводится некая стена с пунктом пропуска трафика. Мы уже говорили ранее о такого рода посредниках — это прокси-сервера.

Чтобы собрать воедино преимущества всех основных типов МСЭ, были придуманы так называемые инспекторы состояния. Они позволяют контролировать передаваемые пакеты на основе определенных правил, сессии на основе таблицы состояний, а также приложения.

Мы подошли к самому новейшему типу межсетевых экранов — МСЭ нового поколения, одной из задач которых является контроль трафика, в том числе, *SSL*-трафика на уровне приложений. Современная парадигма обеспечения безопасности заключается в том, что пользоваться для разрешения или блокировки трафика на основе порта, протокола, *IP*-адреса, уже нельзя, так как вредоносные программы способны использовать большое число самых разных портов, притворяться легитимными и т.д., не говоря уж о том, что весьма актуальным становится вопрос анализа *SSL*-трафика, который фактически сейчас становится основным видом трафика в сети. Необходим детальный анализ работы приложений и пользователей, оценки рисков, связанных с ней, и умного управления трафиком на основе такого анализа. Другими словами, современный МСЭ нового поколения — это устройство, работающее на прикладном уровне, умеющее отличать вредоносные приложения от не вредоносных, независимо от формальных характеристик их работы, таких как порт и протокол, но не только это отличает их.

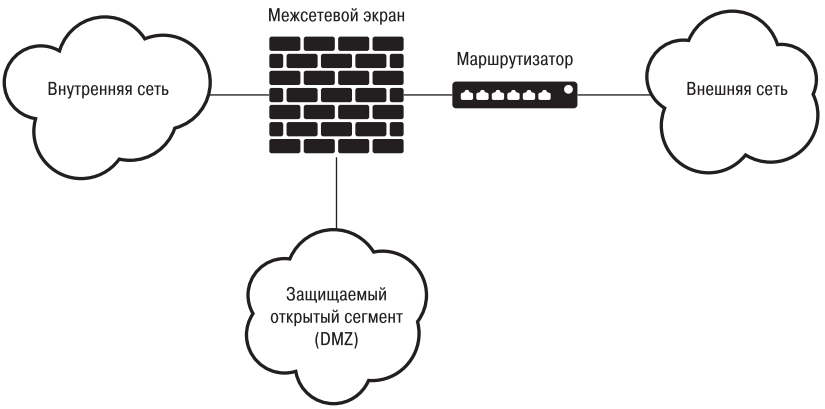

Рис. 7. *Типовая схема работы МСЭ*

Давайте разберемся — какие функции современных межсетевых экранов нового поколения являются ключевыми. Помимо уже упомянутых выше, современные МСЭ должны выполнять сканирование

трафика с возможностью выявления вирусов независимо от портов и протоколов, проводить контроль неизвестного трафика при подключении облачных песочниц (при интеграции с ними), наличие функционала IDS/IPS (*англ.* Intrusion Detection/Prevention System), т.е. детектирования и противостояния вторжениям в сеть, возможность блокировки ботнет трафика, организация удаленного доступа сотрудников посредством VPN или GOST VPN, в случае если этого требует законодательство, поддержка мобильных устройств, реальная производительность устройств при всех включенных модулях безопасности, методы URL-фильтрации, механизмы интеграции с каталогами пользователей, возможность определения утечек информации и т.д. На рис. 7 представлена типовая схема работы МСЭ.

Мы упомянули возможности детектирования вредоносного, но неизвестного трафика. Дело в том, что ключевой опасностью для крупных компаний стали так называемые таргетированные или целевые атаки. Они отличаются тем, что тщательно готовятся, проводятся в несколько стадий, включая предварительную разведку компании и ее инфраструктуры, в том числе средств защиты, используют вредоносный код, который может разрабатываться для атаки на конкретную организацию. Для противодействия таким атакам был разработан несколько классов решений Anti-APT (*англ.* Anti-Advanced Persistent Threat — противодействие целевым атакам), который, включает в себя сетевые сенсоры, «песочницы» для эмулирования рабочей среды и проверки неизвестного трафика, а также специальные программы для рабочих станций, к которым, в частности, относятся решения класса EDR (*англ.* Endpoint Detection & Response), отличающиеся тем, что позволяют не только определять аномальные процессы, происходящие на конечных станциях на основе IOC (*англ.* Indicators of compromise), но и проводить их расследование.

«Песочницы» проверяют веб-трафик и почтовый трафик по другому принципу, нежели это делают межсетевые экраны. Поскольку работают они чаще всего с неизвестным трафиком, то разворачивают данные вложения или открывают ссылки и анализируют поведение файла. Если обнаруживается вредоносная активность, например, попытка зашифровать диск, то такое вложение не доставляется получателю. Справедливости ради заметим, что проверять таким образом весь трафик довольно затруднительно, поэтому в современных Anti-APT решениях есть функционал предварительного анализа трафика по различным базам сигнатур и контента, после которого разворачивается на виртуальных машинах «песочницы».

При выборе «песочницы» имеет смысл руководствоваться следующими критериями — является ли «песочница» кастомизируемой, т.е. поддерживает ли она максимально возможное число операционных систем, где может разворачиваться тестируемый файл, способна ли «песочница» работать с зашифрованным трафиком, доступно ли

YARA-сканирование файлов, важны также разнообразие понимаемых форматов файлов, а также интеграция с SIEM-решениями и т.д.

Еще одним классом решений, который является важным элементом обеспечения сетевой безопасности, является NAC (англ. Network Access Control — контроль доступа к сети). Решения класса NAC — еще один эшелон безопасности корпоративной сети, позволяющие ограничивать или блокировать доступ к внутренним ресурсам локальной сети хостам, не соответствующим определенным политикам безопасности. Необходимость в их появлении была вызвана рядом факторов, среди которых большая загруженность специалистов по ИБ, поэтому очень важно было создать решение, которое будет в автоматическом режиме пресекать возможность появления инцидента за счет отслеживания всех устройств в сети и ограничения их функционирования на основе различных политик безопасности.

С помощью этих решений, которые существуют как в программном, так и аппаратном исполнении, можно вести полный цикл наблюдения и управления подключающимися в сеть устройствами, включая их классификацию и оценку по критериям соответствия политикам безопасности, контроль доступа к сети на основе предыдущего шага, а также интеграцию с другими системами ИБ, например, SIEM, куда можно на автоматической основе отправлять информацию, например, о выявленных уязвимостях.

NAC-решения используют как агентский, так и без агентский подход, и управляют как классическими элементами инфраструктуры, такими как рабочие станции, переносные устройства и с нестандартными, такими как устройств интернета вещей.

В качестве примеров интеграции NAC-решений со сторонними продуктами безопасности можно привести такие как изолирование хостов по команде от EDR-решения или антивирусного продукта. Если с помощью этих решений обнаруживается, например, троян или процесс, говорящий о компрометации учетной записи, то NAC может изолировать соответствующую рабочую станцию. Другим сценарием применения NAC может быть размещение неизвестных хостов в карантин для сканирования на предмет наличия уязвимостей с помощью соответствующей системы анализа защищенности, и предоставление NAC-решением доступа в сеть просканированному хосту на основе результатов сканирования.

Отдельно хочется отметить такой сценарий как подключение к сетям мобильных устройств, когда NAC-решение может проверять наличие на мобильном устройстве агента того или иного EMM-решения (англ. Enterprise Mobility Management) и устанавливать этот агент, если это требуется в соответствии с политиками безопасности, или запрещать определенные действия в сети, если такой агент не установлен. Пример работы NAC показан на рис. 8.

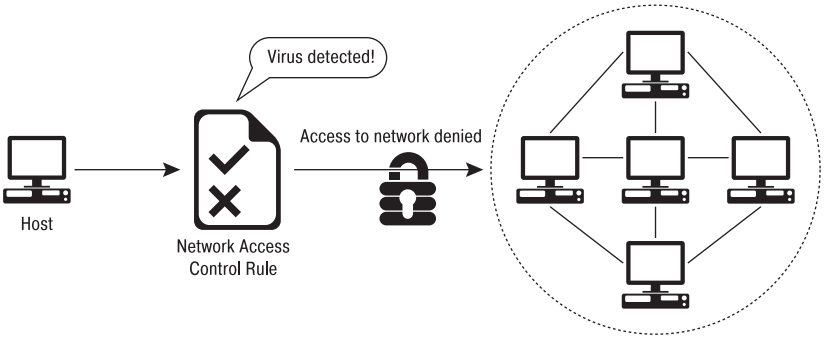

Рис. 8. *Пример работы NAC*

Говоря о безопасности сетей, нельзя обойти вниманием Wi-Fi сети, которые подвержены взлому при небезопасной настройке. Для защиты от атак типа «человек-посередине» применяются специализированные корпоративные решения, которые включают в себя подавление сторонних, не корпоративных, Wi-Fi точек, а также имеют широкие настройки с точки зрения полномочий доступа к сетям для разных групп пользователей, в том числе, с использованием технологии captive portal.

Устройства обеспечения сетевой безопасности, наряду с антивирусами, относятся к базовым решениям ИБ. К основным видам устройств обеспечения сетевой безопасности относятся прокси-сервера, межсетевые экраны (МСЭ), NAC-решения, решения по защите от таргетированных атак и DDOS-атак. Особую важность при внедрении перечисленных решений является их интеграция с другими средствами защиты информации (СЗИ), что позволяет снизить до минимума количество инцидентов ИБ.

Вопросы для самопроверки

1. Чем отличаются МСЭ от прокси-серверов?
2. Для чего применяются «песочницы»?
3. Приведите примеры применения NAC-решений.
4. В чем заключается современная парадигма обеспечения ИБ?

10. БЕЗОПАСНАЯ РАЗРАБОТКА ПРИЛОЖЕНИЙ В ЭПОХУ AGILE

Одной из причин, приводящих к инцидентам ИБ, является наличие ошибок в исходном коде программного обеспечения. Например, распространенная ошибка в реализации первой версии протокола SMB, содержащей эту уязвимость, произвольный код, что послужило причиной большого количества инцидентов с известным шифровальщиком WannaCry. Уязвимость была обнаружена и выпущен патч, но, тем не менее, за то время, пока люди узнали о ней и о необходимости установить патч, было заражено большое число рабочих станций, владельцы которых потеряли свои данные.

В идеале надо создавать код, который не содержит такого рода уязвимостей. Для того, чтобы контролировать качество кода и отслеживать, как минимум, грубые ошибки, а иной раз, и бэкдоры, оставленные самими разработчиками, дающие возможность недокументированного управления ПО, созданы специальные программы — анализаторы кода и исполняемых файлов. В докладе [10] обсуждается развитие систем менеджмента от классического до «Бережливого производства», от «Бережливого» до Agile, которое Ю. Адлер предлагает назвать «Живучим производством» и менеджментом будущего — возможно, «Выживающим производством».

В 1950-е годы Т. Оно теоретически обосновал концепцию *Lean production* («Бережливое производство»), а его коллега С. Синго помог ее практически осуществить. Выделены пять шагов подхода, связанного с «Бережливым производством»: определить, что есть ценность для клиента, организовать поток создания ценности, организовать движение этого потока, создать механизм вытягивания, непрерывно совершенствовать созданную систему («кайдзен»). В монографии [11] говорится о четвертой промышленной революции, начавшейся на пороге тысячелетий и опирающейся на цифровые технологии, искусственный интеллект и обучающиеся машины. Эта революция влияет и на концепцию ИБ.

Как пишет Ю. Адлер: «На рубеже тысячелетий стали проявлять себя новые ценности потребителей. Это стремление приобрести на

рынке не продукцию, и не услугу, и даже не продукцию, завернутую в услугу, а решение проблемы, с которой клиент столкнулся. А мы уже знаем, что смена ценностей неизбежно ведет к глубоким переменам в менеджменте. И действительно, такой подход возник, и мы попробуем сейчас с ним познакомиться. Возник он на Западе и получил название «Agile». Появилось понятие «активное предприятие» (*agile enterprise*) — предприятие, энергично осуществляющее перемены. Активность — это постоянная готовность компании, и ее персонала к переменам, иногда радикальным, в том, что делать и как это делать. Иными словами, активным можно считать такое предприятие, организационная структура и процессы администрирования которого способны быстро и гибко перестраиваться с учетом необходимости действовать в интересах потребителей.

Одна из первых монографий об *Agile* была опубликована в октябре 1994 года [12]. «Живучесть» немыслима без широкого использования информационных технологий, что закреплено в феврале 2001 года в провозглашенном тогда манифесте. В статье [13] рассмотрены возможности применения в строительстве бережливого производства, «живучего» производства и их многочисленных гибридов.

Это особенно актуально сейчас, когда основной методологией разработки у многих компаний является гибкая методология Agile, принципы которой описаны в Agile manifesto, и вот лишь один из них: приветствие изменений требований даже в конце разработки (это может повысить конкурентоспособность полученного продукта). Некоторое возможное пренебрежение документацией на ПО в пользу более конкурентоспособного с точки зрения функционала и сроков выхода на рынок продукта, отсутствие в определенных ситуациях «дорожной карты» разработки проекта, частая смена версий — все это наталкивает на мысль о том, что очень важно встроить процесс анализа кода в сам процесс разработки ПО и управления версиями разрабатываемого продукта.

Переполнение буфера, утечки памяти, переполнение стека, использование неинициализированной переменной, нарушение прав доступа, синтаксические ошибки, и в конце концов, базовые ошибки в написании алгоритма — это далеко не полный перечень ошибок при написании кода ПО, которые могут приводить к проблемам, в том числе, в ИБ, так как фактически могут представлять собой эксплуатируемые уязвимости.

Для поиска ошибок или «закладок» в ПО сканеры кода используют самые разные способы. К ним относятся лексический, семантический и синтаксический анализ, taint-анализ, анализ распространения типов и констант, анализ синонимов и прочие. При этом сканеры анализа кода могут проверять только тот код, который изменился или проверять код ПО от версии к версии с разнообразными системами

управления циклом разработки ПО. Важной особенностью сканеров уязвимости является их возможность не просто показывать ошибки или не декларированные возможности (НДВ) в коде, но и то, как их устранять, по аналогии с описанием уязвимостей CVE в отчетах сканеров безопасности. Еще один ключевой момент это так называемые false positive и false negative — ошибки 1-го и 2-го рода, когда есть риск пропустить ошибку в коде, с одной стороны, и выявить ошибку там, где ее на самом деле нет. Эта проблематика характерна для всех систем ИБ, а решение ее связано с одной из задач математической статистики — проверки простых гипотез.

Для борьбы с ними вендоры-разработчики сканеров кода используют разные решения, в том числе, накапливаемую базу знаний. Эффективным и в то же время наиболее экономичным способом решения могут служить оптимальные статистические критерии вальдовского типа, в свое время примененные автором для статистического регулирования технологических процессов [14].

Сканеры кода ПО приобретаются в интересах служб разработки ПО, которые встраивают их в процесс безопасной разработки кода или в интересах служб ИБ, которые обязаны проверять ПО, используемое в банках, на предмет наличия уязвимостей. Обращаем внимание — ряд нормативных документов в области ИБ, например, в финансовой отрасли прямо указывают на необходимость проверки используемого ПО на наличие уязвимостей и бэкдоров. И здесь возникает интересная ситуация — ведь исходный код программ доступен далеко не всегда. Как же быть?

Существуют два основных вида анализа программного обеспечения на наличие уязвимостей — статический SAST, т.е. анализ исходного кода и динамический DAST, когда анализируется программа в процессе ее выполнения. В большинстве случаев предпочтителен статический анализ, но и у динамического есть свои преимущества. Также, есть сканеры кода, обладающие функционалом декомпиляции уже готовых приложений, некоторые из них могут производить декомпиляцию приложений, написанных, под Android и на лету находит ошибки в коде. С точки зрения ИБ такая функция полезна, но не стоит забывать о том, что такого рода действия могут трактоваться как нарушение лицензионных соглашений разработчиков ПО с пользователями, которые, как правило, не допускают декомпиляцию. Погрешности в определении ошибок в коде при работе с автоматически декомпилированным приложением всегда выше, чем когда код предоставлен разработчиком самостоятельно.

Итак, как мы уже выяснили, в идеале необходимо использовать и статический и динамический анализ приложений. Определим ситуации, когда динамический анализ приложений более эффективен и дополняет преимущества статического анализа кода. Очень хороший

пример привел Андрей Карпов — разработчик сканера статического анализа кода PVS-Studio в своей статье [15].

Например, у нас есть функция, которая выглядит так:

```
void OutstandingIssue(const char *strCount)
{ unsigned nCount;
sscanf_s(strCount, «%u», &nCount);
int array;
memset(array, 0, nCount * sizeof(int));}
```

С помощью статического анализатора кода выяснить, может ли быть выход за границу массива или нет, крайне затруднительно, а особенно если строка, конвертирующаяся в число, читается из файла. И даже если строка формируется где-то в другой функции, а не в файле, задача практически не решаемая, так как надо понять, в какой последовательности будет выполняться код, какие значения будут принимать переменные, возможно ли переполнение и т.д. Чем дальше от места вычисления значения осуществляется его использование, тем сложнее анализ. Если же между местом формирования строки и местом ее использования вызывается несколько функций, то в связи количеством возможных ветвлений и значений переменных, сложность анализатора и количество требуемых ему ресурсов увеличивается многократно.

А если бы задачу решил динамический анализатор приложений, то ему достаточно увидеть, что после массива затирается маркер, т.е. произошел выход за границы массива. И все — задача решена. Можно найти задачи, решаемые с помощью именно статического анализа, но при этом абсолютно неподвластные динамическому анализу. В упомянутой выше статье Андрея Карпова приведен противоположный пример. Рассмотрим еще один кусок кода:

```
const unsigned char stopSgn[2] = {0x04, 0x66};
....
if (memcmp(stopSgn, answer, sizeof(stopSgn) != 0))
return ERR_UNRECOGNIZED_ANSWER;
```

С точки зрения динамического анализа проблем никаких нет — просто сравнивается часть буфера, а ситуаций, когда функция memcmp () сравнивает только часть буфера, немало. А статический анализатор кода увидит проблему в этом куске кода, которая заключается в том, что количество сравниваемых байт, вероятно, вычисляется не совсем корректно. А причина в том, что скобка поставлена не в том месте и статический анализатор увидит проблему и просигнализирует о ней. Так что, в идеале для анализа корректности кода следует использовать

оба вида анализа. При выборе сканера статического анализа кода имеет смысл обращать внимание на количество поддерживаемых языков программирования, скорость работы, интеграция с системами управления версий ПО, возможность визуализации графов выполнения анализируемого кода и т.д.

Особое место в ряду сканеров анализа кода занимают сканеры ERP-систем и учетных систем, в том числе, SAP и 1С. Ошибки в коде этих решений могут приводить к самым разным инцидентам ИБ, включая кражу финансовой информации и персональных данных, модификацию финансовой отчетности, кражу информации о клиентах и поставщиках, ложные транзакции и т.д. Решения данного класса позволяют определить наличие уязвимостей, найти ошибки конфигураций, определить превышение допустимых полномочий, например Segregation of Duties — недопустимое совмещение служебных обязанностей, провести оценку соответствия стандартам ИБ и дать соответствующие рекомендации. По сути — это уже не просто сканеры кода или приложений, а полноценные решения по всестороннему анализу безопасности ERP-систем.

Также нельзя обойти вниманием такой важный класс решений как сканеры кода веб-приложений. Статистика ведущих пен тестеров мира говорит о том, что в большинстве случаев веб-приложения содержат уязвимости, которое позволяют злоумышленникам проводить атаки на них. С помощью уязвимостей киберпреступники могут похищать данные пользователей, содержащиеся в cookie-файлах, заражать рабочие станции посетителей таких сайтов вредоносным ПО и т.д.

Особое внимание имеет смысл обратить на веб-приложения банков, которые зачастую содержат уязвимости высокой степени риска в связи с повышенной сложностью их логики, на веб-приложения государственных организаций, которые также содержат уязвимости, с помощью которых возможно проведение атак на посетителей сайтов, а также веб-приложения интернет-магазинов, которые содержат уязвимости, которые могут приводить к отказу в обслуживании. Современные сканеры кода веб-приложений содержат как статический анализ кода, так и динамический и при этом могут интегрироваться с WAF (англ. Web Application Firewall — файрволл веб-приложений) для обеспечения безопасности приложений. Некоторые из сканеров кода веб-приложений поддерживают возможность генерации эксплойтов на лету, что позволяет протестировать реальную опасность уязвимостей, и загружают готовый патч для исправления в WAF, который создает соответствующее правило для блокировки атаки.

Несмотря на то что сканеры анализа кода веб-приложений — это мощный инструмент, который можно использовать как в собственной инфраструктуре, так и по модели SaaS, сам по себе браузер также предоставляет определенные возможности по анализу кода приложений,

конечно, более ограниченные, но, тем не менее, мы их рассмотрим. Как известно, все браузеры снабжены определенными средствами разработчиков, которые доступны, например, по команде F12 в окне браузера. Для использования браузера для анализа кода также желательно иметь установленный редактор кода и интегрированные среды разработки, а также инструменты типа NodeJS, интерпретаторы Python и т.д.

Встроенные средства разработчика в браузере полезны тем, что, например, увидев пустую страницу и нажав на Ctrl+U, Вы увидите, что код на странице присутствует, просто не отображается в виде HTML, в связи с тем, что не все тэги показывают контент на страницах. Это очень полезное наблюдение с точки зрения безопасности. В скрытых от глаз данных могут содержаться URL на внутренние ресурсы, «скрытый» frame с формой входа и т.д. Более того, размер frame может быть настолько маленьким, что Вы можете зайти на сайт и вообще его не увидеть. При этом одновременно на Ваш компьютер может загружаться вредоносное ПО.

Если мы рассмотрим браузер Chrome, то в панели Source можно увидеть очень много интересной информации, а именно ресурсы, загруженные <iframe>, <script> или другими тэгами. Также, существует возможность поиска функции в коде, что может также быть полезно с точки зрения ИБ. Полезной также является вкладка Elements и другие, которые также дают возможность серьезного анализа HTML и Java.Script кода. Помимо перечисленного, инструменты браузера можно использовать для того, чтобы понимать — сохраняет ли вебсайт что-то на стороне посетителя сайта. Также, крайне полезной является вкладка Приложение в тех же инструментах разработчика, с помощью которой можно даже проверять — возможно ли выдать себя за другого пользователя с помощью изменения маркера сессии.

Анализ кода ПО является очень важной частью обеспечения ИБ в связи с тем, что разработчики пишут не идеальный код. Он может содержать непредумышленные ошибки или закладки. И то, и другое представляет собой опасность с точки зрения компрометации информации, обрабатываемой приложениями. Для поиска уязвимостей в приложениях существуют специальные анализаторы кода, статические и динамические. В связи с важностью этой задачи, необходимость анализа безопасности приложений прописана в нормативных актах, например, Банка России.

Вопросы для самопроверки

1. Чем отличается статический анализатор кода от динамического?
2. На что необходимо обращать внимание при выборе анализатора кода?
3. Для чего нужны средства разработчика, встроенные в браузер?
4. Приведите примеры ошибок при написании кода ПО.

11. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Говорить о том, что мобильные устройства, телефоны и планшеты, давно вошли в нашу жизнь, став частью и профессиональной деятельности, смысла не имеет, это давно уже стало данностью. А вот о том, каким образом защищать данные на мобильных устройствах, мы и поговорим в этой главе.

Что же угрожает корпоративной информации, обрабатываемой на мобильных устройствах. Есть три основные составляющие в обеспечении безопасности информации: конфиденциальность, целостность и доступность. Особенность мобильных устройств, связанная с тем, что мы постоянно берем их с собой, обуславливает и специфические проблемы ИБ. Первое, что приходит на ум — это то, что мобильное устройство можно потерять, и информация может попасть в руки тех, для кого она не предназначалась. Соответственно, у нас сразу компрометируется конфиденциальность и доступность информации. С точки зрения источника угрозы здесь фигурируют два основных потенциальных нарушителя — внешние злоумышленники, получившие физический доступ к устройству или установившие на устройство зловредное ПО и получившие над ним контроль, а с другой стороны, это могут быть нелояльные сотрудники.

Есть понимание того, что, если на мобильном телефоне сотрудника обрабатывается чувствительная корпоративная информация, требуется предпринимать меры по обеспечению ее защиты. При этом мы сталкиваемся с такой особенностью — как право собственности и ограничениями на управление мобильными устройствами со стороны компаний. Суть проблемы в том, что в большинстве компаний сотрудники пользуются личными устройствами, на которых обрабатывается и личная и корпоративная информация. Законодательно компании довольно серьезно ограничены с точки зрения установки на мобильные телефоны и планшеты сотрудников какого-либо ПО.

Существует концепция BYOD (*англ.* Bring Your Own Device — принеси свое собственное устройств). Она подразумевает использование

личных устройств сотрудников, но с применением корпоративной политики безопасности, которая подразумевает установку специального ПО на данные устройства. Регламентироваться установка такого ПО может с помощью дополнительного соглашения к трудовому договору. Кроме того, одним из вариантов решения проблемы является концепция COPE (англ. Corporate Owned, Personally Enabled — «корпоративные устройства, настройкой и обслуживанием которых сотрудник занимается самостоятельно»), когда устройства выдаются сотрудникам вместе с корпоративной сим-картой. В этом случае у работодателя, как говорится, развязаны руки. Другое дело, что, так как в любом случае у работодателя будет определенный доступ к личной информации сотрудника, т.е. их персональным данным, цели, порядок такой обработки и состав обрабатываемых персональных данных необходимо донести до него в письменном виде.

Так или иначе, необходимо защищать информацию, когда она находится непосредственно на мобильном устройстве, или же в процессе ее передачи с мобильного устройства по каналам связи. И в том, и в другом случае на помощь приходят специальные решения класса EMM (*англ. Enterprise Mobility Management* — управление корпоративной мобильностью). В дополнение к ним желательно использовать антивирусные решения для мобильных устройств и VPN-клиенты отечественных разработчиков. Заметим, что большинство EMM-решений включают в себя VPN-модуль, но это не сертифицированные решения, поэтому следует оценивать применимость тех или иных нормативных актов к защите, обрабатываемой на мобильных устройствах информации, например, в области защиты персональных данных, и при необходимости использовать отечественные VPN-клиенты для мобильных устройств.

EMM-решения представляют собой клиент-серверные приложения с агентом, устанавливаемым на мобильные устройства, серверная часть которых, как правило, состоит из двух основных частей: сервер управления политиками безопасности и прокси-сервер, который на основе получения данных с сервера управления политиками может блокировать для тех или иных пользователей те или иные виды трафика.

Все задачи по обеспечению ИБ на мобильных устройствах можно разделить на несколько типов:

— отделить корпоративную информацию от личной и защитить ее с помощью, например, криптографических средств;
— управлять полномочиями пользователей на мобильных устройствах, т.е. запрещать или блокировать доступ к тем или иным функциям приложений или к тому или иному контенту;
— обеспечить защиту информации в процессе ее передачи с мобильного устройства.

Первая задача решается с помощью криптоконтейнера, виртуальной машины, разворачиваемой на мобильной ОС (операционная система), доступ к которой организовывается с помощью пароля, ПИН-кода или при вводе биометрических данных. Все корпоративные данные, хранимые внутри криптоконтейнера, зашифрованы штатными средствами ОС и доступны лишь авторизованному владельцу мобильного устройства. В случае если злоумышленник получит доступ к мобильному устройству, данные будут бесполезны для него, так как расшифровывать их с учетом длины ключа и новейших алгоритмов шифрования будет, практически, невозможно. Кроме того, у администратора системы ИБ всегда есть возможность нажатием одной кнопки превратить мобильное устройство в «кирпич», т.е., как минимум, стереть всю информацию, а как максимум, лишить его всех функций для предотвращения перепродажи устройства на черном рынке.

Вторая задача решается с помощью интеграции прокси-сервера и сервера управления политиками с инфраструктурой управления пользователями на основе Active Directory или другого каталога пользователей. Третья задача решается с помощью встроенных в EMM-решения VPN-модулей, а также с помощью описанной выше интеграцией прокси-сервера и сервера управления политиками ИБ. Решения класса EMM содержат в себе следующие основные функциональные модули:

- прокси-сервер, т.е. шлюз, функцией которого является управление, шифрование и защита трафика между мобильным устройством и внутренними ресурсами организаций;
- магазин приложений, с помощью которого можно управлять как собственными программами, разработанными программистами тех или иных компаний, или же приложениями вендоров;
- защищенный почтовый клиент, с помощью которого обеспечиваются повышенные функции безопасности электронной почты;
- защищенный менеджер файлов для организации надежного и безопасного доступа с различным уровнем полномочий в различных хранилищах, включая облачные;
- защищенный браузер для доступа к внутренним ресурсам компании;
- VPN-клиент.

Ряд EMM-продуктов имеют так называемую технологию «обертывания» сторонних приложений самого разного функционала, т.е. с помощью не очень сложной процедуры позволяют сделать так, что эти приложения могут автоматически настраиваться для разных групп пользователей с различными полномочиями, а также автоматически контейнеризироваться, что означает автоматическое шифрование данных. Владелец мобильного устройства, а также офицер безопасности

могут быть уверены, что данные такие «обернутых» приложений надежно защищены с помощью криптографических средств.

Обратим внимание на еще ряд функций EMM-решений, некоторые из которых уже упоминались в этом разделе. Первой из этих функций является защита от фишинга. Фишинг — это одна из очень серьезных проблем в области киберпреступности, поскольку она использует социальную инженерию. В любой момент времени человеку может прийти сообщение из банка о том, что у него просрочен кредит, или о необходимости смены пароля, или о выписанном штрафе, или о полученном наследстве. В письме будет содержаться ссылка или вложение.

В результате открытия ссылки или файла, пользователь не знакомый с элементарными правилами цифровой гигиены, или автоматически загрузит на свое устройство вредоносный код или собственноручно передаст злоумышленникам важную информацию о себе. Ряд EMM-решений содержат функционал, позволяющий блокировать такие попытки на основе контентного анализа и соединения с репутационными базами, в которых уже перечислены индикаторы компрометации подобных ссылок или вложений.

Вторая проблема — это так называемый jailbraik, когда пользователь пытается с помощью установки нелегитимной прошивки ОС получить административный доступ к устройству. Решение и этой проблемы в EMM-решениях, отслеживающих такую попытку и, во-первых, сообщают об этом офицеру безопасности, а во-вторых, блокируют такому сотруднику, практически, весь функционал. Ну и еще одной функцией, о которой хочется напомнить, является «антивор». При потере устройства, во-первых, есть возможность удаления всей ценной информации на устройстве без возможности восстановления, а во-вторых, такие решения позволяют отследить устройство, делать тайные фотоснимки, активировать тревожные сигналы и т.д.

Стоит также упомянуть о разнице между Android и iOS. Если iOS изначально создавалась как закрытая ОС для устройств одной компании, то Android — это открытая система. Среди элементов обеспечения ИБ на мобильных устройствах, контролировать которые можно централизованно с помощью EMM-решений, установка приложений из Google Play или корпоративного магазина приложений, о чем упоминалось выше, что само по себе может обеспечить более высокий уровень доверия к устанавливаемым приложениям, а также настройка списка разрешений для приложений, например, отключение геолокации, запрашиваемой приложениями. Не стоит забывать и о возможностях таких решений с точки зрения аутентификации, например, по сертификатам и применения технологий единого входа SSO (*англ.* Single Sign-On — технология единого входа).

С точки зрения интеграции в инфраструктуру EMM-решения позволяют применять ту или иную политику ИБ в зависимости от под-

ключения к конкретным Wi-Fi сетям, геолокационной информации и т.д. Чтобы подчеркнуть важность EMM-решений, опишем лишь некоторые из современных угроз ИБ, нивелировать которые можно с их помощью.

Программы-шифровальщики. Они являются бедой как для обычных компьютеров, так и для мобильных устройств. Но если на мобильном устройстве установлен входящий в комплект поставки EMM-решения криптоконтейнер, то даже при попадании шифровальщика на мобильное устройство, корпоративным данным ничего не угрожает. Кроме того, за счет применения политик ИБ, пользователь мобильного устройства с меньшей вероятностью загрузит себе вредоносное ПО.

Еще одной бедой являются ботнеты (*англ.* botnet, произошло от слов *robot* и *network*), сети зараженных компьютеров, в которые попадают устройства, на которых не установлены современные СЗИ. Устройство, ставшее не по своей воле частью ботнета, может или использоваться как вычислительный ресурс, или выполнять вредоносные функции. EMM-решения могут ограничивать скачивание приложений из Интернета, и тем самым обезопасить телефон от скачивания опасного и вредного ПО.

Вспомним и о такой проблеме как взлом NFC. Интернет пестрит случаями взломов методом «bump and defect» и кражей денежных средств и ценной информации пользователей из-за уязвимостей протокола NFC. EMM-решения позволяют управлять функционалом мобильных устройств, в том числе, функциями Wi-Fi, Bluetooth и NFC и при необходимости отключать их. Обратной стороной медали является необходимость контроля утечки информации с мобильных устройств. Основным классом решений, которые позволяют предотвращать утечку информации ограниченного доступа, являются DLP-решения. Однако большинство разработчиков таких систем обходят стороной мобильные устройства и мобильные операционные системы. Думается, виной тому то, что устройства принадлежат лично сотрудникам, и слежка за тем, что происходит на них может трактоваться как прямое нарушение законодательства, в том числе, даже определенных статей Конституции Российской Федерации, например, о праве на неприкосновенность частной жизни.

Попытки разработать такие решения предпринимались. В некоторых случаях компании разрабатывали специальные мобильные устройства с повышенной степенью защищенности от утечек информации, но они не стали популярными. Видимо, EMM-решения можно использовать и для предотвращения утечек информации. Например, при использовании почтовых клиентов можно запретить пересылку вложений через личные почтовые ящики, если вложение пришло на корпоративный ящик. Можно использовать и возможности прокси-серверов, которые, как уже говорилось, поставляются в комплекте

EMM-решений для контроля и, в том числе, блокировки передачи той или иной информации с мобильного устройства.

Защита информации на мобильных устройствах представляется крайне важной задачей, так как информация давно вышла за периметр классической локальной сети. Для защиты такой информации созданы решения класса EMM, позволяющие управлять правами пользователей на мобильных устройствах. Кроме того, они дают возможность шифровать корпоративную информацию на телефонах и планшетах, а также в процессе ее передачи другим людям.

Вопросы для самопроверки

1. Каковы основные угрозы для информации, обрабатываемой на мобильных устройствах?
2. Что такое криптоконтейнер?
3. Чем BYOD отличается от COPE?
4. Что такое “jailbreak”?

12. ЗАЩИТА ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА И ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

В компаниях обрабатывается большое количество информации ограниченного доступа, перечень тайн, существующих в рамках российского законодательства, достаточно большой. Согласно указу Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» существуют следующие виды тайн: персональные данные, сведения, составляющие тайну следствия и судопроизводства, служебная тайна, профессиональная тайна, например, врачебная, нотариальная, адвокатская тайна, коммерческая тайна, данные об изобретениях до момента публикации информации о них, сведения из личных дел осужденных, а также о принудительном исполнении судебных актов или актов других органов за исключений общедоступных по закону сведений.

Федеральный закон от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации» в п. 2 ст. 9 говорит, что «Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами». Вопросам защиты информации в этом федеральном законе отведен п. 4 ст. 16: «Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации».

Ниже рассмотрим две темы: список организационных и технических мер, которые надо предпринимать для зашиты информации ограниченного доступа, и вопросы, связанные коммерческой тайной. Говоря об утечках информации из организаций, надо сказать, что они бывают умышленные и случайные. И проводя работу по повышению уровня системы ИБ, важно предпринимать меры по предотвращению и тех и других.

Сложно представить, но для большей наглядности предположим, что один из конструкторов-проектировщиков автомобиля послал своему приятелю — инженеру из другой компании, пусть даже не конкурирующей, чертеж будущего автомобиля для независимой оценки. При этом никаких криминальных идей о продаже чертежа в голове у инженера не было. Если в компании установлена система DLP, то она обнаружит это и подаст сигнал офицеру безопасности и бедному инженеру придется оправдываться за свои действия. Данный пример в очередной раз показывает необходимость внедрения в организациях программ повышения осведомленности по вопросам ИБ, но мы сейчас не об этом.

Меры по защите информации ограниченного доступа должны, как мы уже говорили выше, включать и организационные и технические меры. К организационным относятся проведение обучений по основам ИБ для сотрудников, в частности, по работе с информацией ограниченного доступа, подписание соглашений о неразглашении информации с сотрудниками и внедрение интерактивных решений по повышению осведомленности по вопросам ИБ. Также, важным является проведение процессов классификации информации, оценки ее стоимости на основе интервьюирования ключевых владельцев информации, рисков компрометации и т.д.

Технические меры подразумевают внедрение двух основных классов решений — DLP-систем, предотвращающих утечки информации из компании, программ по ИТ-аудиту и систем класса Data Access Governance, позволяющих проводить аудит действий в сети, определять, кто и какие действия с файлами совершал, находить чувствительную к компрометации информацию в файлах, а также автоматизировать регламенты по предоставлению пользователям прав, в первую очередь, на файловые ресурсы, но не только. Также, мы немного коснемся темы контроля за перемещением файлов на основе меток безопасности. Возвращаясь к упомянутым выше системам, можно сказать, что, фактически, DLP и DAG системы являются взаимодополняющими и в комплексе позволяют эффективно защищать чувствительную к потере конфиденциальности информацию. Правда, стоит оговориться, что DAG-системы

являются наиболее эффективными при наличии классификатора, т.е. механизма, позволяющего анализировать содержимое файлов и на основе определять типы информации, содержащейся в файлах: персональные данные, информация о платежных картах, медицинская информация и т.д.

К слову говоря, в ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» есть термин «утечка информации», которая определена как «неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и получения защищаемой информации иностранными разведками».

DLP-системы способны определить попытку передать ту или чувствительную информацию или с помощью установки специального агента на рабочую станцию или на уровне сетевого перехвата, в том числе, благодаря интеграции с прокси-серверами по протоколу iCap. Несмотря на то, что перехват на уровне периметра сети дает широкие возможности с точки зрения контроля за утечками информации, есть те каналы передачи информации, контролировать которые невозможно без установки специального приложения на рабочую станцию.

К ним относятся распечатка документов на принтер, передача файлов на съемные носители, общение в мессенджерах, установленных на рабочей станции. Установка агентов также очень важна, поскольку преобладающую долю в общем объеме трафика начинает играть шифрованный трафик, и без использования агентов на конечных устройствах анализировать информацию в этом трафике крайне затруднительно.

Надо сказать, что многие решения по обеспечению сетевой безопасности, которые разбирались ранее, содержат некоторый функционал DLP-систем, но, безусловно, специализированные решения в этой области намного более функциональны, и если принято решение о внедрении соответствующих технических мер, то, конечно, надо делать ставку на специально созданное для этих задач решение.

Выбирая DLP-систему, стоит обратить внимание на следующие основные критерии. В первую очередь, на количество контролируемых каналов утечки информации: электронная почта, веб, мессенджеры, съемные носители и т.д. Есть DLP-системы, которые способны только детектировать утечку информации, а есть, которые способны работать в режиме блокировки. И здесь мы сталкиваемся, наверное, с главной задачей при внедрении DLP-систем — точность настройки правил срабатывания.

Если используются правила «из коробки», количество ложных срабатываний может быть настолько большим, что способно па-

рализовать работу компании. Поэтому к работе DLP-систем в режиме блокировки передачи информации необходимо относиться внимательно и не злоупотреблять этим режимом. Ряд DLP-систем для улучшения качества работы поддерживает технологию UEBA (*англ.* User and Entity Behaviour Analytics — поведенческий анализ), которая, в определенном смысле, добавляет искусственный интеллект в процесс поиска, вводя в него понятия контекста в отношении конкретного сотрудника, и определяя аномалии по целому ряду признаков.

Среди других критериев выбора DLP-систем можно отметить скорость работы, определяемая ее особенностями взаимодействия с СУБД, аналитические возможности, в том числе, позволяющие выявлять взаимосвязи сотрудников друг с другом и т.д. Различие в подходах хостовых и шлюзовых DLP лучше всего видны на рис. 9 и 10.

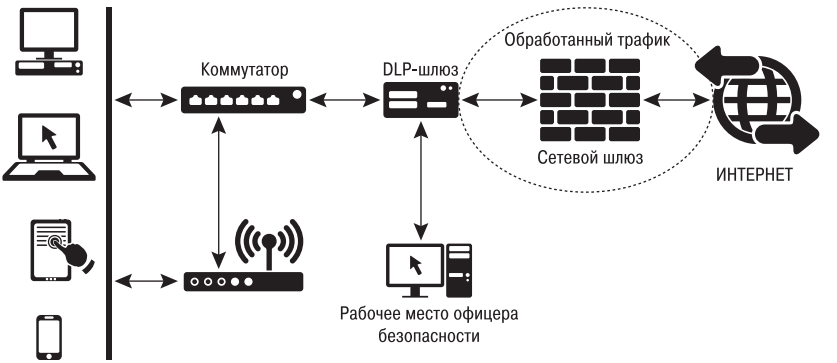

Рис. 9. *Принцип работы шлюзовой DLP-системы*

Рис. 10. *Принцип работы хостовой DLP-системы*

Теперь рассмотрим другой класс решений под названием Data Access Governance (Управление доступом к неструктурированным данным). Мы уже говорили, что эти решения позволяют дополнять защиту от утечек информации благодаря тому, что, во-первых, выстраивается и автоматизируется механизм согласования доступа сотрудников к файловым хранилищам, а в-вторых, обеспечивается ведение непрерывного аудита за действиями пользователей в сети, и, в том числе, сигнализирование о попытках получения доступа к файлам, которые не должны быть доступны тому или иному сотруднику, исходя из его полномочий.

Действительно, безопасность неструктурированных данных — это очень серьезная проблема, поскольку в случайно забытых на том или ином файловом ресурсе, облачном хранилище или папках MS Exchange документах может содержаться очень важная информация, раскрытие которой нанесет компании существенный вред, при этом именно неструктурированные данные являются, по показателю объема, основными данными в компаниях.

Благодаря DAG-решениям можно решить задачи контроля действий пользователей в сети, анализировать доступ к критичным данным, в том числе, на основе классификатора, получать оперативную информацию о том, кто и к каким файловым ресурсам имеет доступ, и что не менее важно, автоматизировать процесс получения доступа пользователей к тем или иным ресурсам компании. Отдельно, хочется упомянуть, что решения класса DAG также способны анализировать изменение прав пользователей в Active Directory.

Еще одним способом защищать безопасность файлов и предотвращать утечки информации, является использование меток. Использование меток относится к мандатной системе управления доступом. Метка, установленная с помощью одного из программных продуктов в этой области, в файл, позволяет определить тип секретности информации, содержащейся в том или ином файле, и в зависимости от этого определить перечень доступных для тех или иных пользователей действий, например, только чтение, или чтение и редактирование, или отправка информации вовне и т.д.

Одним из видов информации ограниченного доступа, который защищается федеральным законодательством, является коммерческая тайна. Для определения прав и обязанностей субъектов при работе с ней был разработан и принят Федеральный закон от 29.07.2004 98-ФЗ «О коммерческой тайне».

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или иных возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую тайну.

Информация, составляющая коммерческую тайну, — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе, о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которой у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Для привлечения к ответственности сотрудников, разгласивших коммерческую тайну, надо ввести на предприятии режим коммерческой тайны, в том числе, проставить грифы Коммерческая тайна на документах и указать на них же правообладателя. Это, далеко, не полный перечень тех мероприятий, которые требуется провести.

Проект по установлению режима коммерческой тайны начинается с обследования организации, в ходе которого анализируются внутренние нормативные документы, которые регламентируют обработку конфиденциальной информации и обеспечения ИБ. Определяется шкала, в соответствии с которой будет оцениваться ценность информации с точки зрения ее конфиденциальности, целостности и доступности.

На этом же этапе формируются методики для оценки рисков ИБ, проводится выявление критичных информационных активов с оценкой их ценности, выявляются внедренные меры защиты, обследуется сетевая инфраструктура и собирается информация о конфигурации информационных систем. Результатом является отчет об обследовании, содержащий, в частности, реестр информационных активов с указанием их ценности и оценку рисков ИБ.

На втором этапе разрабатывается необходимая организационно-распорядительная документация, в которую входят Положение о коммерческой тайне, включающее стандарт определения принадлежности информационных активов к коммерческой тайне, перечень сведений составляющих коммерческую тайну, дополнения в трудовые договора и должностные инструкции, регламенты управления доступом, регистрации событий ИБ и действий работников при утечке информации, составляющей коммерческую тайну.

Обязанность организаций защищать информацию ограниченного доступа предусмотрена действующим законодательством, в частности, 149-ФЗ. Особое место среди тайн, подлежащих защите, занимает коммерческая тайна — информация, дающая организации преимущество в силу ее незнания другими организациями. Для ее защиты на предприятиях вводится режим коммерческой тайны и внедряются DLP-системы, которые, впрочем, подойдут для защиты от инсайдеров любой ценной для предприятия информации.

Вопросы для самопроверки

1. Что оператор информационной системы обязан сделать для защиты информации в соответствии со 149-ФЗ?
2. Какие виды DLP-систем существуют?
3. Что входит в понятие «управление защитой неструктурированных данных»?
4. Из каких шагов состоит проект по внедрению режима коммерческой тайны?

13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРОИЗВОДСТВЕ И В УПРАВЛЕНИИ КАЧЕСТВОМ

Задача обеспечения ИБ, и так являясь одной из важнейших в организациях, в случае, если речь идет о безопасности промышленного производства, становится архиважной. Можно вспомнить достаточное количество примеров, когда атаки на промышленные предприятия приводили, если не к фатальным, то уж точно, весьма неприятным последствиям. Так, кибератака с использованием вируса Stuxnet на завод по обогащению урана в иранском городе Натанза привела к выходу из строя 1369 центрифуг.

Также, как и в целом в отрасли ИБ все нормативные документы в области безопасности АСУ ТП (автоматизированные системы управления технологическими процессами) можно разделить на обязательные к исполнению федеральные законы и подзаконные акты, а также российские и международные стандарты. Полный их перечень приведен в Приложении 4.

Выделим приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», а также Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконные акты. Что касается стандартов, то, в первую очередь, имеет смысл обратить внимание на ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008) «Защищенность (кибербезопасность) промышленного процесса измерения и управления».

Все меры по защите АСУ ТП можно поделить на два больших блока — выполнение требований законодательства и внедрение решений по защите АСУ ТП, которые не входят в перечень обязательных, но вместе с тем от этого не ставших менее полезными. Определим основ-

ные угрозы безопасности АСУ ТП, которые можно считать актуальными. К ним можно отнести:

- эксплуатацию уязвимостей в инфраструктуре АСУ ТП, результатом которого может стать несанкционированное проникновение и подключение к АСУ ТП;
- внедрение вредоносного ПО в системы управления АСУ ТП;
- сетевые атаки, включая попытки вторжения в АСУ ТП;
- использование возможных закладок в ПО и оборудовании.

Нельзя упускать из вида, что устранение уязвимостей в АСУ ТП не идентично аналогичному процессу в классической корпоративной инфраструктуре. В связи с работой многих систем в круглосуточном режиме и их критической важностью многие уязвимости могут оставаться неисправленными в течение многих месяцев, так как даже сканирование средствами безопасности не разрешается в связи с тем, что, теоретически, они могут нарушить нормальную работу АСУ ТП систем. С целью поиска уязвимостей в SCADA системах ряд разработчиков сканеров безопасности выпустили специальные снифферы — перехватчики-анализаторы трафика, которые позволяют находить уязвимости в программном обеспечении путем анализа заголовков пакетов.

Например, определяя версии ПО — есть ли для соответствующего программного решения обновление на сайте разработчика. Таким образом, частично отпадает необходимость активного сканирования тех или иных хостов. Другая проблема заключается в том, что производители программируемых логических контроллеров могут не выпускать прошивки, устраняющие уязвимости, например, в связи с тем, что устройства сняты с производства и поддержки. Для того, чтобы понять на какие элементы АСУ ТП, в первую очередь, направлены атаки киберпреступников, необходимо понять, каким образом разделена АСУ ТП. Принято выделять три основных уровня:

- верхний уровень, на котором осуществляется визуализация, диспетчеризация и сбор данных. На данном уровне функционируют MES, SCADA и ERP системы;
- средний уровень, где основным элементом являются программируемые логические контроллеры, дающие команды исполнительным механизмам на основе данных от датчиков и команд верхнего уровня;
- нижний уровень, где работают различные виды контрольно-измерительного оборудования типа датчиков и исполнительных механизмов.

Наиболее громкими инцидентами, говорящими о многообразии векторов атак на объекты АСУ ТП, можно назвать атаку на Thyssen Krupp в 2014 г., когда благодаря перехвату контроля над компьютером, управлявшим доменной печью, был установлен зловред, который заставил печь перегреться и выйти из строя, а также слу-

чай с нелояльным к компании ранее уволенным из нее инженером Maroochy Water Service, получившим удаленный доступ через направленную антенну и в течение трех месяцев сливавшим неочищенные сточные воды, управляя помпами. Еще одним примером может быть инцидент, когда один из инженеров установил беспроводную сеть в центре дамбы, завел на нее исполнительные устройства и снимал информацию о работоспособности систем, не выходя из диспетчерской. А радиус действия точки выходил за пределы контролируемой зоны. Не стоит лишний раз говорить, что инциденты, особенно первые два, нанесли ущерб компаниям, как финансовый, так и репутационный.

Практика показывает, что защищать от атак надо элементы, работающие на всех уровнях АСУ ТП, на верхнем, среднем и нижнем. В качестве примеров защиты на верхнем уровне АСУ ТП можно привести использование так называемых датадиодов, которые обеспечивают одностороннее сетевое взаимодействие, обеспечив блокировку зловредного трафика из корпоративной сети в сеть АСУ ТП, представленную на рис. 11.

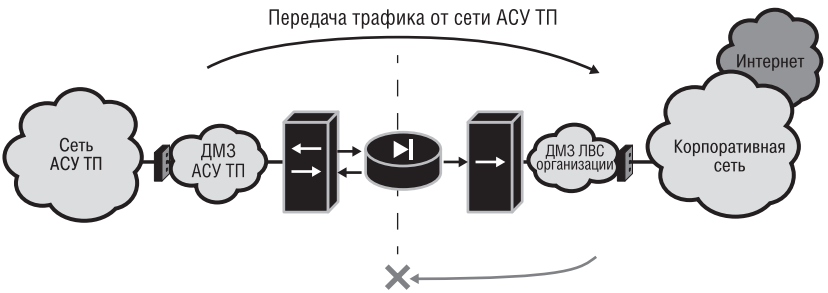

Рис. 11. *Схема работы датадиода*

Переходя к среднему уровню АСУ ТП, можно отметить, что зачастую для защиты от атак на контроллеры внедряются специализированные межсетевые экраны, предназначенные для защиты АСУ ТП, т.е. которые понимают все основные протоколы АСУ ТП, например, MODBUS, DNP3, CIP и другие, а также имеют обновляемую базу специализированных сигнатур вторжений в сети АСУ ТП. Что касается нижнего уровня АСУ ТП, то безопасность обеспечивается физической и логической изоляцией. В определенных архитектурных решениях также возможно применение специализированных решений по защите от вторжений.

Важным элементом защиты АСУ ТП является система управления инцидентами ИБ, включающая систему мониторинга трафика. Такие решения позволяют осуществлять инвентаризацию сетевых активов АСУ ТП, выявлять попытки неавторизованного управления системами АСУ ТП, обнаруживать и предотвращать кибератаки на АСУ ТП,

а также помогают в расследовании инцидентов кибербезопасности в АСУ ТП.

Примером такого решения может служить PT ISIM от Positive Technologies, схема которого представлена на рис. 12.

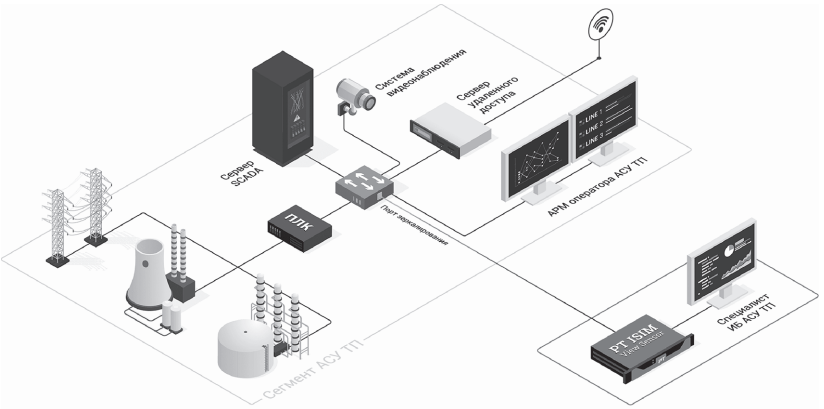

Рис. 12. *Схема работы PT ISIM*

Общий перечень мер защиты может включать в себя межсетевые экраны и системы защиты от вторжений, DLP-систему, антивирусное решение, средства анализа защищенности и сканеры кода ПО, средства криптографической защиты каналов связи, средства аутентификации, а также решения по обеспечению доверенной загрузки и средства контроля съемных носителей.

Основным нормативным актом, на который необходимо ориентироваться предприятиям при защите АСУ ТП, является приказ ФСТЭК России от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

В приказе содержится четкое понимание алгоритма действий при организации защиты объектов АСУ ТП. После принятия решения о необходимости защиты в АСУ ТП, требуется:

- провести классификацию АСУ по требованиям защиты информации;
- определить угрозы безопасности информации и разработать модель угроз;
- определить требования к системе защиты АСУ ТП;
- внедрить соответствующие организационные и технические меры.

Класс защищенности АСУ выбирается отдельно для каждого уровня и каждой системы, и может быть от К1 до К3, где К3 — самый низкий класс, а К1 — самый высокий.

Определяется класс защищенности АСУ на основании уровня значимости (критичности) обрабатываемой в АСУ информации, а уровень значимости (УЗ) определяется степенью возможного ущерба от нарушения целостности, конфиденциальности и доступности информации, из-за чего возможно вмешательство в работу АСУ или нарушение ее работы.

УЗ определяется следующим образом:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) х (конфиденциальность, степень ущерба)].

При этом степень ущерба определяется заказчиком или оператором самостоятельно, и варьируется от высокой, где последствием компрометации свойств безопасности может быть чрезвычайная ситуация, средней, если масштаб инцидента носит региональный или межмуниципальный характер, или низкой, если инцидент носит муниципальный (локальный) характер. При этом оцениваются возможные социальные, политические, экономические, военные или иные последствия.

Также нужно обратить внимание, что последствия инцидента могут рассматриваться не обязательно с точки зрения компрометации всех трех свойств безопасности, достаточно, компрометации двух из них. Если хотя бы для одного из свойств безопасности определена высокая степень ущерба, то речь идет о УЗ1. При средней степени ущерба — присваивается УЗ2. Если для всех свойств безопасности определена низкая степень ущерба, то устанавливается УЗ3. Если в АСУ обрабатывается несколько видов информации с разным уровнем значимости, то итоговый уровень устанавливается по наивысшему значению степени ущерба. УЗ соответствует классу защищенности АСУ, т.е. УЗ1 соответствует К1, УЗ2 — К2 и УЗ3 — К3.

Выбор мер защиты определяется по приложению № 2 к этому же приказу на основании класса защищенности АСУ ТП. Важным этапом в развитии законодательства в области защиты промышленных предприятий стало принятие Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры», о нем мы поговорим в отдельной главе. Наконец, обратим внимание на опубликованный в 2018 году стандарт безопасности АСУ ТП ISA/IEC 62443. Он был разработан комитетом ISA99 и является основой для управления уязвимостями в АСУ ТП. В частности, в нем описываются технические требования к кибербезопасности элементов АСУ ТП, в том числе, встраиваемых устройств, сетевых компонент, компонент хоста и приложений. В стандарте описаны функции безопасности, которые дают возможность элементам АСУ ТП без использования тех или иных контрмер отражать угрозы безопасности.

Защита АСУ ТП на предприятиях осуществляется на основе сочетания требований Приказа ФСТЭК России № 31, а также ряда других нормативных актов и стандартов, например, ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008). Учитывая три уровня управления АСУ ТП, важно предусмотреть внедрение СЗИ на всех этих уровнях. В дополнение к тем СЗИ, которые предусмотрены Приказом ФСТЭК № 31, важно обеспечить сегментацию сети, отделение сети АСУ ТП от корпоративной с помощью датадиодов, а также внедрение средств анализа сетевых аномалий.

Вопросы для самопроверки

1. Назовите основные угрозы безопасности АСУ ТП.
2. Как осуществляется проект по приведению защиты АСУ ТП в соответствии с Приказом ФСТЭК России № 31?
3. Как определяется уровень значимости информации, обрабатываемой в АСУ ТП?
4. Какие средства защиты применяются на среднем уровне АСУ ТП?

14. ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В течение достаточно долгого времени в качестве критически важных с точки зрения кибербезопасности объектов выступали предприятия энергетической отрасли и промышленные предприятия с опасными производствами, успешная атака на которые может привести к печальным последствиям. Все изменилось в 2017 г., когда вышел Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры», который существенно расширил интерпретацию критической инфраструктуры и отнес к ней не только промышленные и потенциально опасные производственные предприятия. В законе введены термины.

Критическая информационная инфраструктура (КИИ) — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры (КИИ) — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Под субъектами КИИ имеются ввиду предприятия, работающие в самых разных отраслях, атака на которые может также привести к негативным последствиям для граждан. В ст. 2 говорится о ГОССОПКе (Государственной системе обнаружения, предотвращения и ликвидации компьютерных атак). Здесь имеет смысл акцентировать внимание на том, что все предприятия, которые относятся к субъектам КИИ обязаны подключиться к ГОССОПКе и передавать в НКЦКИ (Национальный координационный центр по компьютерным инцидентам) информацию об инцидентах. С целью облегчения этой работы созданы специализированные порталы, которые получают информацию из SIEM-решений, а также от сотрудников службы ИБ или SOC (англ. Security Operations Center — Центр мониторинга и реагирования на инциденты ИБ) и передают информацию в НКЦКИ.

Защита объектов КИИ осуществляется в соответствии со ст. 5 на основе присвоения им категорий значимости, исходя из факторов социальной, политической, экономической, экологической значимости или значимости для выполнения государственного оборонного заказа. Что же подразумевается под каждой значимостью.

Социальная значимость подразумевает возможный ущерб жизни и здоровью людей вследствие возможного нарушения функционирования социальных объектов, транспортной инфраструктуры или сетей связи или максимальном времени отсутствия возможности получения госуслуги.

Политическая значимость означает ущерб Российской Федерации в вопросах внутренней и внешней политики. Экономическая значимость подразумевает возможный ущерб, причем как прямой, так и косвенный, субъектам КИИ или бюджетам РФ. Экологическая значимость выражается в оценке возможного ущерба окружающей среде.

Ну и последняя — значимость объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка предполагает оценку возможного увеличения сроков выпуска продукции, снижения производительности или функционирования информационных систем, работающих в области обеспечения обороны страны.

Перечислим ряд нормативных актов, которые надо использовать в работе при приведении предприятия в соответствии с требованиями закона № 187-ФЗ. В первую очередь, речь идет о Постановлении Правительства Российской Федерации № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Все объекты КИИ делятся на значимые и незначимые. Значимые — это те, которым в соответствии с вышеупомянутым постановлением присвоена одна из трех категорий значимости, где первая — наибо-

лее высокая, где возможный ущерб максимален, а третья — наиболее низкая. Те работы, которые субъект КИИ должен провести по защите информации, регламентируется рядом приказов ФСТЭК России. Приказом ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» устанавливаются цели функционирования систем безопасности, требования к структурному подразделению по обеспечению безопасности, требования к программным и программно-аппаратным средствам, обеспечивающим безопасность значимых объектов КИИ, а также требования к составу организационно-распорядительной документации и функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ.

Одной из обязанностей субъекта КИИ — составить перечень объектов КИИ, провести их категорирование и отправить во ФСТЭК России эти сведения. Форма направления таких сведений регламентируется Приказом ФСТЭК России от 22.12.2017 № 236. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Такие сведения должны содержать информацию:

— об объекте КИИ, в том числе его адресе, назначении, сфере деятельности, архитектуре и назначении;
— о субъекте КИИ, включая данные о наименовании, адресе, должности и ФИО руководителя, структурном подразделении, отвечающем за безопасность значимых объектов КИИ;
— о взаимодействии объекта КИИ с сетями электросвязи, в том числе, такие данные как категория сети электросвязи, наименование оператора связи, способ взаимодействия с сетью (проводной, беспроводной);
— о лице, эксплуатирующем объект КИИ, включая информацию о наименовании юрлица или ИП, адрес, элемент объекта, который эксплуатируется;
— о программных и программно-аппаратных средствах, которые используются на объекте КИИ, в том числе, наименования компьютеров, серверов, сетевого, технологического оборудования, наименования общесистемного и прикладного ПО, список применяемых средств защиты, в том числе, информацию о сертификатах соответствия, функции безопасности, встроенные в ПО;
— об угрозах безопасности информации и категориях нарушителей (внешний, внутренний), включая информацию о возмож-

ностях нарушителя по реализации угроз в части его знаний и мотивации, или обоснование невозможности нарушителем реализовать те или иные угрозы ИБ, а также основных угрозах безопасности информации или обоснование их неактуальности;
- возможных последствиях инцидентов, в том числе, о возможном ущербе, и типах инцидентов, в том числе, в результате таргетированных атак (НСД, утечка данных, отказ в обслуживании), нарушение функционирования технических средств и т.д.;
- категории значимости объекта КИИ, в том числе, полученных значений по каждому из показателей критериев значимости с обоснованием или информацией о неприменимости показателя к объекту с обоснованием;
- организационных и технических мерах, применяемых для обеспечения безопасности значимых объектов КИИ. Под организационными мерами подразумеваются установление контролируемой зоны, контроль физического доступа к объекту, разработка организационно-распорядительной документации. Технические меры включают, в частности, управление доступом, идентификацию и аутентификацию, ограничение программной среды, антивирусную защиту и другие меры.

Если говорить о конкретных мерах защиты информации для значимых объектов КИИ, то сразу имеет смысл сослаться на приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ Российской Федерации», который как раз и устанавливает состав мер по обеспечению безопасности для значимых объектов КИИ на основе категории значимости, определяемой, как мы указывали выше, с помощью постановления Правительства Российской Федерации № 127. Одновременно с принятием закона № 187-ФЗ были внесены изменения и в УК РФ и УПК РФ. В ст. 274.1 УК РФ предусмотрена ответственность за нарушения в области КИИ.

Для того, чтобы понять является ли организация субъектом КИИ, можно воспользоваться формальными признаками ОКВЭД, УСТАВ или имеющиеся лицензии, или проанализировать процессы в организации и как следствие, те информационные системы, которые работают в указанных в законе сферах.

Проект по приведению процессов и систем в соответствии с требованиями законодательства о КИИ состоит из обследования объектов, моделирования угроз безопасности, категорирования объектов КИИ, после чего внедряются соответствующие меры защиты.

Резюмируя вышесказанное, субъекты КИИ — организации, владеющие информационными системами в ряде отраслей, например, в банковской сфере, энергетике, медицине и других. Для защиты КИИ

необходимо определить перечень объектов, категории значимости, а также внедрить меры по защите информации в соответствии с Приказом ФСТЭК России от 25.12.2017 № 239.

Вопросы для самопроверки

1. Что такое КИИ?
2. В соответствии с каким нормативным документом предприятия осуществляют отправку информации об объектах КИИ в надзорный орган?
3. Чем отличаются значимые объекты КИИ от незначимых?
4. Что такое Госсопка?

15. ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Когда мы говорим об угрозах ИБ, мы всегда подразумеваем, что те или иные угрозы могут реализоваться, а могут не реализоваться. Другими словами, мы оцениваем риски ИБ. Это нужно для того, чтобы понять, что защищать в первую очередь. Риск — это вероятность того, что угроза может воспользоваться уязвимостью на том или ином хосте, в результате чего будет скомпрометирована целостность, доступность или конфиденциальность и организация понесет ущерб. Основной международный стандарт в области ИБ ISO-27001 основан на оценке рисков, и будем использовать, в том числе, положения данного стандарта при описании подхода по оценке рисков ИБ.

В первую очередь при оценке рисков необходимо определить ценность информации, понять ее жизненный цикл — как она появляется, обрабатывается, удаляется и т.д. Другими словами, имеет смысл начать с формирования реестра информационных активов. Составляя такой реестр, необходимо указывать и описывать элементы инфраструктуры, такие как оборудование, ПО, каналы связи, облачные сервис, неразрывно связанные с обработкой той или иной информации. Следующий элемент в описании рисков ИБ — модель угроз или сценарий их реализации, что, в классической интерпретации, является сочетанием трех элементов: актив — уязвимость — угроза.

Примером риска может служить риск утечки коммерческой тайны, например, рецепта продукта в связи с отсутствием, внедренной в компании DLP-системы. Уязвимостью в данном случае является отсутствие средства защиты, информационным активом — рецепт продукта, угрозой — потеря конфиденциальности рецепта. Задачей является выяснить вероятность риска и последствия от его реализации.

У каждого риска должен быть владелец, т.е. тот, кто несет ответственность за обработку риска и размер остаточного риска, т.е. приемлемого для организации уровня риска, снизить до которого первоначальный размер риска помогают организационные и технические меры. Зачастую владельцем риска, если мы говорим об

информационном активе, является представитель того бизнес-подразделения, который отвечает за этот информационный актив, т.е., в частности, за производство или обработку этой информации или получение ее от контрагентов организации. В случае ИТ-активов, к которым относятся информационные системы, то владельцем скорее будет отдел ИТ.

Существует два основных подхода к оценке рисков — количественный и качественный. Как следует, из названия в первом случае — мы оцениваем ущерб и вероятность некими значениями, а во втором — с помощью неких описательных характеристик, например, оценивая возможный ущерб как высокий, средний, низкий, а вероятность такими характеристиками, как вероятно, маловероятно, крайне невероятно. В очень упрощенном виде оценки рисков представлены в табл. 1.

Таблица 1

Таблица оценки рисков ИБ

Вероятность	Ущерб		
	Низкий	Средний	Высокий
Вероятно	Низкий риск	Средний риск	Высокий риск
Невероятно	Низкий риск	Средний риск	Средний риск
Крайне невероятно	Низкий риск	Низкий риск	Средний риск

Каждая компания определяет шкалу, по которой оценивается отнесение ущерба к одной из категорий, но в любом случае качественная оценка проще, чем количественная, а с точки зрения обоснования затрат на внедрение решений количественная оценка лучше. Примером высокого ущерба от инцидентов ИБ относится существенная потеря клиентской базы, или финансовые потери, допустим, более 5 млн руб., средний — когда скорость обслуживания клиентов снизится на 10–15%, или финансовые потери в случае реализации такого риска прогнозируются на уровне от 1 млн руб. до 5 млн руб. Примером низкого ущерба могут стать не влияющие на работу перебои в работе, или финансовые потери не более 1 млн руб.

Для анализа вероятности надо принимать во внимание тот факт — насколько часто возникали подобные инциденты в прошлом. Кроме того, важно понимать уязвимость активов в отношении рассматриваемых рисков — насколько они могут быть интересны для злоумышленников, или подвержены сбоям. Вероятность оценивается на основе статистических данных. Низкая вероятность — если такие инциденты не происходили никогда, или происходили крайне редко, среднюю — если инциденты уже случались, или же есть потенциал для их появления, и высокую — когда инциденты случались регулярно. Но, ко-

нечно, для максимально точного расчет используется исключительно количественный анализ рисков.

Алгоритм процесса анализа рисков можно расписать следующим образом:

1. Определить ценность актива с точки зрения прибыли от актива, стоимости поддержки, стоимости восстановления и т.д.

2. Определить потенциальные потери от компрометации конфиденциальности, целостности или доступности. На данном шаге также необходимо рассчитать ущерб от единичного инцидента SLE (англ. Single Loss Expactancy) для всех активов и угроз.

3. Проанализировать угрозы с учетом их вероятности и рассчитать среднюю частоту реализации той или иной угрозы (ARO — Annualized Rate of Occurrence).

4. Рассчитать общие годовые потери на каждый вид угрозы, объединив расчет вероятности и возможного ущерба. Основным расчетным значением здесь является ALE — Annualized Loss Expectancy, и для его расчета нам потребуются ранее полученные данные.

При количественном анализе рисков ИБ формула SLE выглядит так:

$$\text{SLE} = \text{Ценность актива} \times \text{Фактор воздействия}.$$

Фактор воздействия — это процент ущерба от угрозы, т.е. часть стоимости, которую потеряет актив при реализации угрозы. Например, стоимость актива составляет 10 млн руб. В случае DDOS-атаки на сайт ущерб может составить 20% от стоимости актива, включая упущенную прибыль. Процент посчитан, исходя из максимального времени простоя сайта. Таким образом, максимальный ущерб может составить 2 млн руб.

Итак, значение SLE определено, теперь можно рассчитать ARO (среднегодовая частота возникновения инцидентов), т.е. расчет ожидаемой частоты реализации угрозы в год. Он рассчитывается в диапазоне от 0, когда инциденты определенного типа за время существования компании не были зафиксированы и выше. Например, двойка означает, что в среднем два раза в год случаются инциденты. Для описанного выше примера представим, что инцидент, связанный с атакой на сайт, случался в среднем раз в 2 года, т.е. ARO = 0,5. В данном случае ALE = 2 млн руб. * 0,5 = 1 млн руб. Ожидаемый среднегодовой ущерб равен 1 млн руб. Планируя применение защитных мер, имеет смысл исходить из их стоимости, которая не должна превышать ожидаемого ущерба от реализации угрозы, в данном случае, не более 1 млн руб.

Есть инциденты, которые очевидны, например, DDOS-атака, а утечки конфиденциальной информации из организации при отсутствии внедренной DLP-системы пропустить можно. Поэтому, в слу-

чае если в организации не накоплена статистика по реализации угроз того или иного типа, т.е. по числу инцидентов, то это не значит, что инцидентов не было, организация просто могла их не заметить. Имеет смысл в любом случае провести оценку активов, посчитать риски компрометации конфиденциальности, целостности и доступности, по крайней мере, для наиболее критичных активов и внедрить соответствующие организационные и технические меры.

Некоторые законодательные акты напрямую требуют от организаций проведения оценки рисков ИБ и внедрения мер по защите информации на основе такой оценки. Примером может являться Общий регламент ЕС по защите данных — GDPR. Все риски поделены по размеру потенциального ущерба и по вероятности реализации угрозы на четыре зоны. Обработку персональных данных при наличии рисков, которые находятся в так называемой красной зоне, т.е. с высокой возможной степенью ущерба для компрометации персональных данных физических лиц с высокой степенью вероятности, проводить запрещено. Для таких рисков рекомендуется внедрение организационных и технических мер по их уменьшении и перевода этих рисков в другие зоны, где описаны менее критичные риски, с меньшей вероятностью угрозы или меньшим ущербом.

Каким образом получить информацию об информационных активах и ИТ-активах? Конечно, у владельцев соответствующих бизнес-процессов, к которым эти активы относятся. Именно интервьюирование этих специалистов может дать информацию о том, какие активы наибольшим образом влияют на их бизнес-процессы, и о том, какой ущерб понесет организация при компрометации свойств безопасности этих активов. В сочетании с информацией от ИТ-подразделения о частоте, с которой происходят те или иные инциденты, можно провести оценку рисков ИБ. После того как все риски проанализированы, необходимо составить их реестр, сопоставить с принятыми в компании критериями и обработать в порядке приоритета критичности. Обрабатывать риски можно четырьмя основными способами.

1. Снижение риска, позволяющее уменьшить его вероятность или ущерб от возможного инцидента, за счет внедрения организационных и технических мер.

2. Исключение риска, позволяющее не допускать появления ситуации, при которой риск возникает. Примером, иллюстрирующим этот способ, может быть уменьшение вероятности компрометации критичной информации при передаче по каналам связи между двумя офисами компании в Москве за счет введения запрета на использование каналов связи и передачи такой информации только специализированной курьерской службой.

3. Передача риска может подразумевать страхование рисков ИБ или же передачу их по какому-либо договору, например, на хранение

персональных данных клиентов в защищенном облаке специализированной компании.

4. Принятие риска, которое говорит о том, что компания понимает последствия, но не возражает против того, чтобы он был в существующем виде. Такой способ применяется в случае, например, если стоимость его обработки слишком велика.

Обработка рисков — это всегда сочетание различных способов. Защитные меры могут носить организационный или технический характер. Методик оценки рисков ИБ очень много — это и Octave, и NIST SP800-30, и ГОСТ Р ИСО/МЭК 27005-2010 и многие другие, при этом не существует единого мнения о том — какая же методика является оптимальной. В большинстве случаев подход, связанный с идентификацией активов, оценкой угроз и рисков, так или иначе находится в основе методик, разница заключается в глубине и освещению тех или иных аспектов оценки рисков ИБ.

Для автоматизации процесса управления рисками и не только был разработан специальный класс решений SGRC (Security Governance Risk, Compliance).

Системы данного класса как правило, содержат расширенный функционал, который также позволяет управлять инцидентами ИБ и имеет целый ряд дополнительных функций. Касаемо управления рисками, то при выборе решений имеет смысл обращать внимание на следующие параметры.

Модели оценки рисков ИБ, которые используются в том или ином решении — Octave, ALE, методика Банка России и т.д. При этом существенную роль играет наличие возможности применения собственной методики. Другой критерий связан с использованием количественного или качественного подхода к оценке рисков. Способность решений данного класса давать оценку остаточных рисков и устанавливать размер риск-аппетита также достаточно важна. Не стоит забывать и о формировании плана обработки рисков и плана их снижения, аналитических возможностях отслеживания изменения уровня рисков по временной шкале. Из того, что также может быть достаточно важным для SGRC систем стоит упомянуть о функционале workflow, дающем возможность организовать процессный подход на базе SGRC-решения к оценке, обработке и контролю уровня рисков.

С учетом того, что основным стандартом для организаций по оценки рисков является ISO 31000, имеет смысл узнать о том, а поддерживает ли та или иная система оценку рисков на основе данного стандарта. Это может быть достаточно важно, поскольку оценка рисков ИБ может быть в организации частью оценки бизнес-рисков и осуществляться под контролем соответствующего подразделения, которое использует этот стандарт. Стоит упомянуть, что подход к процессу управления рисками, используемый в ISO 27001 и в ISO 31000,

очень похожи, поэтому не должно возникнуть каких-либо сложностей.

Оценка рисков ИБ — это базовый процесс в обеспечении ИБ, в частности, на основе стандарта ISO 27001. Для обеспечения правильной оценки рисков важно провести классификацию активов, определить их стоимость, оценить вероятность компрометации конфиденциальности, целостности и доступности, и на основе этого создать реестр рисков, который позволит выстроить приоритеты при организации мероприятий по защите информации.

Вопросы для самопроверки

1. Что такое SLE?
2. Назовите способы обработки рисков ИБ.
3. Как называется класс решений, предназначенных для автоматизации процесса управления рисками ИБ?
4. Какой стандарт оценки рисков является основным?

16. СТАНДАРТ ISO 27001 И СПОСОБЫ ЕГО ВНЕДРЕНИЯ

Многие организации внедряют защитные меры для уменьшения рисков ИБ. При этом у специалистов по ИБ, определяющих список мер, может существовать собственное мнение о принимаемых мерах. Влияет на это и позиция топ-менеджеров организаций, выделяющих бюджеты. Возникает вопрос — насколько можно быть уверенным, что меры, принимаемые по защите информации организацией-контрагентом достаточны? Ответ простой — можно в какой-то степени быть в этом уверенным, если организация прошла сертификацию на соответствие стандарту ISO 27001.

Данный стандарт содержит требования к внедрению, сопровождению и непрерывному совершенствованию системы управления ИБ и является основным в серии. Стоит обратить внимание также на стандарт ISO 27002, который является хранилищем лучших практик по обеспечению ИБ. В ISO 27004 описываются процедуры мониторинга эффективности процессов управления ИБ, в ISO 27005 говорится об управлении рисками ИБ, в ISO 27035 даны основы управления инцидентами ИБ. Перечень защитных мер, которые могут быть внедрены в организациях для приведения СУИБ в соответствии со стандартом, содержится в приложении к нему.

Известный принцип Шухарта-Деминга Plan — Do — Check — Act нашел свое применение и в ИБ, где процесс управления ИБ состоит из создания, внедрения, поддержки, непрерывного совершенствования СУИБ. Суть применения цикла в ИБ показана на рис. 13.

Требования к ИБ исходят от заинтересованных сторон, при этом эти стороны могут быть как внешними, например, клиенты, поставщики, регуляторы, или внутренними, коими являются акционеры. На этапе Plan определяются область и границы применения СУИБ, выделяются процессы управления ИБ, которые должны быть внедрены, задачи, ставящиеся перед ней и ресурсы, которые требуются для выполнения задач, составляется план реализации целей. Кроме этого, на этом этапе осуществляется анализ и оценка рисков ИБ, что помогает расставить приоритеты в выборе мер защиты на основе оценки

вероятности и размера ущерба от киберугроз для тех или иных активов компании. После того как риски проанализированы составляется перечень мероприятий по обработке рисков, включая организационные и технические меры, необходимые для приведения рисков к приемлемому остаточному уровню.

Рис. 13. *Использование цикла PDCA при управлении ИБ*

На этапе Do осуществляется выполнение запланированных процессов управления ИБ, внедряются необходимые защитные меры. На этапе Check проверяется факт того, что процессы работают именно так как запланировано. Осуществляется обратная связь с заинтересованными сторонами для подтверждения, что их требования. Выделяются процессы, связанные с проверкой ИБ, т.е. внутренний или внешний аудит, мониторинг эффективности ИБ с помощью метрик или KPI или анализ СУИБ со стороны руководства. Целью этапа является нахождение отклонений в работе СУИБ и зон для совершенствования ее. На этапе Act внедряются меры по ее совершенствованию, т.е. корректирующие действия, или же совершенствуем структуру управления СУИБ, в целом. И описанный процесс является повторяющимся и непрерывным для повышения зрелости СУИБ, ее непрерывного совершенствования и соответствия меняющемуся ландшафту угроз ИБ.

При управлении жизненным циклом СУИБ в соответствии с процессным подходом и Циклом Шухарта-Деминга, можно использовать следующее соотнесение разделов стандарта и этапов Цикла:

Plan — 4. Контекст организации, 5. Руководящая роль, 6. Планирование, 7. Поддержка.

Do — 8. Операционная деятельность.

Check — 9. Оценка состояния.

Act — 10. Улучшение.

ISO 27001 — стандарт, устанавливающий требования к процессам управления ИБ. И при строительстве СУИБ, в первую очередь, имеет смысл определить ее границы, поскольку в любой компании есть критичные с точки зрения компрометации свойств безопасности бизнес-процессы и требования раздела 4. Контекст организации как раз и говорят о необходимости определения того, в каком виде СУИБ принесет наибольшую пользу организации. С этой точки зрения необходимо начать с определения внешних и внутренних факторов, влияющих на организацию и ее цели, а также на построение СУИБ. После этого надо определить внешние и внутренние заинтересованные стороны, например, клиенты, партнеры, регуляторы, персонал и т.д. Для каждой из сторон определяются специфические для нее требования к СУИБ.

В случае регуляторов это выполнение требований нормативных актов, в случае клиентов или сотрудников — обязательства о защите персональных данных и т.д. После этого анализа делаются выводы о том, в каких областях и для каких процессов внедрение СУИБ будет наиболее эффективно. Далее готовится документ «Область действия системы менеджмента ИБ», который содержит список наиболее критичных для компании бизнес-процессов, на которые распространяется СУИБ, а также границы процессов, где они осуществляются. Также разрабатывается обоснование важности описанной области деятельности для компании, включая все внутренние и внешние факторы в отношении описанных бизнес-процессов и заинтересованные стороны с их требованиями к СУИБ.

Одно из ключевых мест в стандарте отведено роли руководства компаний. Ведь СУИБ — это часть общей системы менеджмента компании и затрагивает все уровни управления, т.е. стратегический, тактический и операционный. Поскольку внедрение СУИБ затрагивает, как правило, большое число бизнес-процессов и подразделений компании, то руководство компании, имеющее необходимые полномочия, может влиять на эффективное внедрение СУИБ и взаимодействие всех подразделений.

Руководство должно демонстрировать приверженность идее внедрения СУИБ через разные системы мотивации, изменение уровня ответственности за результаты управления ИБ, создание политик ИБ, обеспечение и назначение полномочий в области управления ИБ и т.д. Должен быть назначен куратор из состава совета директоров, который будет отвечать за внедрение СУИБ или создан Комитет по ИБ, в состав которого входят представители ИБ, ИТ, бизнес-подразделений и службы внутреннего контроля. Он нужен для решения стратегических и тактических вопросов, касающихся функционирования СУИБ, мер по непрерывному улучшению СУИБ. Также должна быть разработана политика ИБ, понятная всем заинтересованным сторонам. Для подготовки такого документа можно использовать систему менеджмента качества, включая Политику в области менеджмента качества.

За всеми процессами СУИБ должны быть закреплены ответственные с соответствующими обязанностями и необходимыми полномочиями. На этапе планирования СУИБ осуществляется самый важный процесс с точки зрения построения СУИБ — анализируются риски ИБ, а также определяются цели ИБ и планы по их достижению. Управление рисками ИБ — основа управления ИБ, на основе которой разрабатываются процессы управления и внедряются необходимые защитные меры. Цель управления рисками — оценить вероятность и потенциальный ущерб от реализации угроз ИБ.

При управлении рисками необходимо учитывать контекст организации, т.е. применимые внутренние и внешние факторы, заинтересованные стороны, требования к определению рисков со стороны заинтересованных сторон, которые сами могут являться источником рисков. Процесс оценки рисков строится для выявления вероятности компрометации конфиденциальности, целостности и доступности информации в рамках области деятельности СУИБ. Для каждого риска должен быть определен владелец, отвечающий за обработку риска и его остаточный уровень. Приемлемый уровень риска определяется руководством компании с учетом предложений ответственных лиц, проводящих соответствующий анализ рисков ИБ. Для рисков, превышающих приемлемый уровень, разрабатываются мероприятия по их обработке.

На стадии Act внедряется план обработки рисков, а на стадии Check при проведении повторного анализа рисков осуществляется анализ того, привели ли внедренные меры к снижению рисков до приемлемого уровня, после чего на стадии Do осуществляется улучшение СУИБ, и внедрение дополнительных мер, или совершенствование внедренных мер для приведения рисков ИБ к приемлемому уровню.

Для поддержания и эксплуатации эффективной СУИБ требуется ряд важных составляющих. Одна из них — это различные типы ресурсов, включая кадровые и финансовые. Обеспечение внедрения СУИБ требуемыми ресурсами задача руководства. Но простого выделения ресурсов недостаточно. С точки зрения кадровых ресурсов, выделяемых для процессов обеспечения СУИБ, надо оценивать их компетенции с точки зрения ИБ и достаточны ли они для выполнения работы. Важно также проведение мероприятий по повышению осведомленности в вопросах ИБ, включая доведение до заинтересованных сторон положений Политики ИБ и правил ИБ. Кроме того, важно понимать — как должен происходить обмен информацией, что можно передавать, а что нельзя?

Особое место здесь занимает документированная информация с описанием требований к управлению организационно-распорядительной документацией в рамках СУИБ, хранению, поддержанию, архивированию свидетельств выполнения процессов СУИБ. Условно можно поделить документированную информацию на документацию,

имеющую жизненный цикл, и которая может корректироваться. Операционная деятельность в стандарте включает требования по обеспечению документооборота, организации управления изменениями, реагирования не незапланированные события и управления аутсорсинговыми организациями. Здесь же устанавливаются требования к периодичности выполнения оценки рисков ИБ. Как правило, организации управляют рисками на ежегодной основе. Если требуется, на этапе контроля изменений, могут применяться элементы оценки рисков ИБ, чтобы спрогнозировать как изменения влияют на организацию и СУИБ.

Все предложенные мероприятия по управлению рисками должны проверяться на соответствие приложению А стандарта, в котором описаны процессы операционного уровня управления ИБ. Практическая реализация требований приложения А описана в стандарте ISO 27002. После оценки рисков разрабатывается «Положение о применимости механизмов контроля», который, де факто, является паспортом СУИБ, представляющий собой таблицу с перечислением всех мер с указанием возможности применимости.

На стадии Check основным является раздел 9. Оценка состояния, где речь идет о необходимости мониторинга, измерения, анализа и оценки работы СУИБ для того, чтобы быть уверенными в том, что СУИБ и ее отдельные процессы работают так, как было запланировано и приносят необходимую и запланированную отдачу. Для решения этих задач существует три основных процесса.

Первый — это оценка эффективности процессов и мер обеспечения ИБ с использованием количественных способов оценки достигнутых. Обязательным здесь является определение метрик, временных интервалов измерения, ответственных за проведение измерений, способов их проведения, ответственных за анализ результатов измерений, а также определение списка мер, которые принимаются при отклонении показателей от целевых значений.

Второй — процесс внутреннего аудита, который должен проводиться с заданной периодичностью для обеспечения контроля соответствия СУИБ требованиям стандарта, требованиям заинтересованных сторон. Должна создаваться программа аудита, чтобы определить — какие аудиты должны проводиться, когда, кем, а также какие результаты аудита должны быть предоставлены. Для проведения аудита надо выбирать компетентных специалистов, при этом важно сохранение принципа независимости, т.е. внутренний аудитор не можем проверять свою деятельность или деятельность своего руководителя. Результаты аудита должны документироваться.

Третий процесс оценки эффективности СУИБ — анализ СУИБ со стороны руководства, которое должно участвовать в пересмотре СУИБ в определенные интервалы времени для подтверждения ее актуаль-

ности и эффективности. Результаты оценки должны фиксироваться в виде решений руководства.

В случае если в процессе функционирования СУИБ возникают отклонения или несоответствия, надо вырабатывать мероприятия по их устранению. При возникновении несоответствий, как правило, есть основная причина, отчего это произошло. Цель по работе с несоответствиями — найти эту причину и внедрить меры для предотвращения возникновения подобных несоответствий в будущем. Организация должна вести процесс по управлению несоответствиями, чтобы вовремя узнавать о них, передавать информацию специалистам, анализировать и принимать меры. Можно вести классификацию критичности несоответствий для обеспечения своевременной реакции на них.

Необходимо различать корректирующее действие, т.е. мероприятие, направленное на устранение коренных причин выявленных несоответствий и коррекцию, т.е. устранение единичного проявления несоответствия. Например, коррекцией может быть административное взыскание сотруднику, хранящему пароль на бумажке рядом с монитором, а корректирующим действием переход на биометрическую аутентификацию и отказ от паролей, которых может быть очень много, и пользователи их просто не запоминают. После внедрения корректирующих действий проводится контроль того, насколько они были эффективны, и устранили ли они причину несоответствия. Другими словами, с помощью корректирующих действий обеспечивается непрерывное совершенствование СУИБ.

Термин СУИБ трактуется в соответствии со стандартом ISO 27000 как система управления информационной безопасностью — часть общей системы менеджмента организации, основанная на оценке бизнес-рисков в цикле создания, внедрения, поддержания и улучшения ИБ в организации. СУИБ должна удовлетворять ожиданиям заинтересованных сторон, чтобы повысить доверие с их стороны. У СУИБ должен быть владелец — обладающий необходимым уровнем полномочий один из руководителей организации, чтобы проводить необходимые изменения на всех уровнях управления. СУИБ должна быть применимой и адекватной в контексте вида деятельности организации и интегрирована в бизнес для максимальной эффективности.

Все системы менеджмента по своей структуре одинаковы, и хорошей практикой является их интеграция между собой. СУИБ не реализуется только «на бумаге», а должна помогать контролировать процессы СУИБ и не создавать излишние бюрократические требования. При этом стандарт допускает подстраивание тех или иных механизмов под бизнес-процессы организации.

Разберем этапы внедрения СУИБ. На этапе Plan создается СУИБ с учетом требований организации по ИБ, требований заинтересованных сторон, целей и задач бизнеса. При этом важно понять насколько

на текущий момент СУИБ соответствует ISO 27001, как ИБ может помочь целям бизнеса. Сравнив текущее состояние ИБ с требованиями ISO 27001, можно понять несоответствия и составлять план-график проекта по внедрению СУИБ, определить ресурсы, человеческие, финансовые и материальные, утвердить план у руководства для повышения статуса и более широких возможностей привлечения ресурсов. На этапе Do происходит внедрение и эксплуатация СУИБ с помощью созданных на предыдущем этапе процессов, политик и защитных мер. На этапе Check осуществляется мониторинг и пересмотр процессов с помощью описанных выше методов, и при выявлении несоответствий на этапе Act производим необходимую корректировку для улучшения СУИБ.

Говоря о требованиях к СУИБ, важно понять, каким образом определить внешние и внутренние факторы, относящиеся к целям организации, например, изменения законодательства по ИБ, в том числе, специфические отраслевые и как осуществлять мониторинг этих изменений. СУИБ должна иметь процесс для идентификации и непрерывного мониторинга требований к СУИБ, чтобы в любой момент времени организация понимала — каким требованиям она должна соответствовать и соответствует ли.

Это может делаться с помощью реестра законодательных и договорных требований с указанием применимости к компании или к конкретным подразделениям или областям деятельности, после чего реестр поддерживается в актуальном состоянии, включая регулярную оценку соответствия организации этим требованиям. Напомним, что для эффективной работы СУИБ очень важно определить владельцев всех процессов, включая бизнес-процессы и процессы СУИБ. Это помогает процессам коммуникации и повышению эффективности процессов.

В любой момент времени важно понимать, насколько далеко организация находится от той системы СУИБ, к которой она идет. Помогает в этом, в том числе, разработка документации. Поэтому важно определить тот оптимальный объем документации. Документированная информация делится на документы и записи. Объем документации по СУИБ зависит от размера организации, ее структуры, отраслевой принадлежности, компетенции персонала. ISO 27001 требует наличия определенных документов и управления ими, т.е. создания, изменения, согласования, утверждения и распространения их. Жестких требований к документам в стандарте нет, но есть понимание того, какие документы должны быть.

Это Политика ИБ, отвечающая на вопрос — что должно быть сделано, Руководство СУИБ, описывающее структуру управления СУИБ и ее отдельные процессы, после этого идут процедуры, регламенты, стандарты, т.е. отвечающие на вопрос — как должно быть сделано.

Наконец, поддерживающая информация — инструкции, методички повышению осведомленности, и на самом нижнем уровне находятся записи, позволяющие понять — работает ли система так как она спроектирована — акты, протоколы и т.д.

Одной из составляющих процесса управления ИБ является определение текущего статуса СУИБ и направления развития. Это осуществляется с помощью интервьюирования владельцев бизнес-процессов, оценки результатов предыдущих внутренних и внешних аудитов, анализа инцидентов, недостатков систем. С помощью этого разрабатываются корректирующие действия по совершенствованию СУИБ. Это называется GAP-анализ, т.е. анализ позволяющий посмотреть на СУИБ «как есть» и сравнить с тем «как должно быть».

После GAP-анализа надо провести планирование проекта по внедрению СУИБ. Это будет включать в себя назначение ответственных, планирование сроков выполнения проекта с учетом декомпозиции до конкретных задач и выделение требуемых ресурсов. Одним из факторов успеха проекта является назначение менеджера проекта, который будет контролировать сроки выполнения проекта и все остальные аспекты, включая ресурсы, а также осуществлять мониторинг эффективности взаимодействия всех вовлеченных в проект бизнес-подразделений.

После появления плана проекта и его утверждения, высшее руководство должно распространить план по внутренним заинтересованным сторонам. Важно определить — кто должен быть в курсе этого плана, или его отдельных частей. В самом начале проекта важно определить контекст организации, в том числе, как неоднократно говорилось, внешние и внутренние факторы, влияющие на организации, которые у каждого предприятия свои. Кроме того, организация должна понимать свои цели, согласованные с ожиданиями заинтересованных сторон, имеющих отношение к СУИБ. Кроме того, компания должна определить взаимодействие и зависимости между видами деятельности и деятельность других организаций, которые могут повлиять на ИБ, например, аутсорсеров и их влияние на ИБ организации.

Один из важных документов СУИБ — Политика ИБ, которая соответствует целям организации, поскольку ИБ, являясь поддерживающим механизмом, должна помогать в реализации целей компании. Политика должна включать в себя цели ИБ, которые должны быть измеримыми, обязательства по соблюдению применимых требований по соблюдению ИБ и постоянному улучшению СУИБ. Политика ИБ должна быть доступна сотрудникам организации, и более того, должны предприниматься меры по ее распространению и ознакомлению с ней заинтересованных сторон и сотрудников организации. Политика ИБ должна быть утверждена высшим руководством компании и рассматриваться как самый главный документ в документации

СУИБ. Для политика должен быть установлен периметр пересмотра в соответствии с изменениями целей бизнеса и прочими изменениями в компании.

Для эффективного функционирования СУИБ высшим руководством должны быть распределены ответственные за реализацию тех или иных процессов ИБ, у которых также должен быть достаточный уровень полномочий для полноценного выполнения своих обязанностей. Еще раз подчеркнем важность формирования целей ИБ на всех уровнях управления, включая план их достижения и способ оценки результатов. Цели должны быть документированы с фиксацией того — что будет сделано, какие ресурсы потребуются, кто будет ответственным и как будут оцениваться результаты. И повторим, что цели должны быть измеримы, основаны на результатах оценки рисков и должны быть согласованы с политикой ИБ.

С точки зрения человеческих ресурсов крайне важно понимать тот список компетенций, которые должны быть у участников СУИБ и регулярно его оценивать. При оценках ниже требуемой направлять персонал на соответствующее обучение. Это требование относится, в том числе, и к руководителю проекта внедрения СУИБ. Каждый сотрудник, входящий в область деятельности СУИБ, должен быть ознакомлен с Политикой ИБ, должен знать свою роль и обязанности в СУИБ, и знать о последствиях несоблюдения требований ИБ.

В рамках мониторинга эффективности функционирования ИБ необходимо получить ответ на вопрос, что именно подлежит оценке и измерению, и оценивать как процессы СУИБ, так и сами защитные меры. Метод оценки должен давать воспроизводимые результаты, не зависящие от конкретных людей, дающий объективную оценку. Компания определяет периодичность мониторинга, ответственных за его проведение и оценку результатов. Это может потребовать создания отдельного процесса мониторинга эффективности ИБ.

При создании метрик надо учитывать три важных момента. Метрика должна быть измеримой и значимой, т.е. важность измерения метрики не должна поддаваться сомнению. Сотрудник, к которому приписывается метрика, например, владелец процесса, должен иметь возможность влиять на ее значение. Для понимания отклонений процессов должны быть целевые и пороговые значения у метрик. Целевое — желаемое значение, пороговое — значение, которое говорит о том, что с процессом что-то не так.

При управлении проектам полезным является метод восемь дисциплин решения проблем (8D). Он используется для определения, корректировки и устранения проблем и является полезным для совершенствования процессов. Подход эффективен при решении различных ситуаций при внедрении СУИБ. Метод предполагает следующие этапы:

D0: План. Планируйте решение проблемы и определите предпосылки/условия возникновения проблемы.

D1. Использование команды. Создайте команду людей со знанием продукта/процесса.

D2. Определите и опишите проблему. Определите проблему путем ее идентификации в количественных терминах: кто, где, когда, почему, как и сколько (5W2H) для проблемы.

D3. Разработайте промежуточный план сдерживания; Реализуйте и проверьте промежуточные действия. Определите и реализуйте задерживающие действия для изоляции проблемы от клиентов.

D4. Определите, идентифицируйте и проверьте основополагающую причину и точки избегания. Определите все применимые причины, из-за которых появилась проблема. Идентифицируйте, почему проблема не была замечена во время возникновения. Все причины должны быть проверены и доказаны, что не определяется во время мозгового штурма. Можно использовать метод «Пять почему» или диаграмму Исикавы для сопоставления причин против эффектов или выявленной проблемы.

D5. Выберете и проверьте долговременные исправления для проблемы/несоответствия. Через предварительные производственные программы количественно убедитесь, что выбранные коррекции решат проблему для клиента (убедитесь, что коррекция действительно решит проблему).

D6. Реализуйте и проверьте корректирующие действия. Определите и реализуйте лучшие корректирующие действия.

D7. Предпримите профилактические/превентивные меры. Измените системы управления, операционные системы, практики и процедуры для предотвращения повторения этой или похожей проблемы.

D8. Поздравьте Вашу команду. Признайте коллективные усилия команды. Команда должна быть формально отблагодарена от имени организации.

В 1979 г. Союз японских ученых и инженеров (*JUSE — Union of Japanese Scientists and Engineers*) собрал воедино семь достаточно простых методов контроля качества [16]. По мнению одного из творцов «Японского экономического чуда» К. Исикавы: «Основываясь на опыте своей деятельности, могу сказать, что 95% всех проблем фирмы могут быть решены с помощью этих семи принципов. Они просты, однако без них невозможно овладеть более трудными методами» [17]. Одним из этих методов является схема Исикавы — инструмент, обеспечивающий системный подход к определению фактических причин возникновения проблемы, который, по нашему мнению, может быть использован при построении СУИБ.

Схема Исикавы (из-за формы ее часто называют «рыбьей костью» или «рыбьим скелетом») дает наглядное представление не только о со-

вокупности тех факторов, которые влияют на изучаемый объект, но и о причинно-следственных связях. При построении схемы Исикавы к центральной стрелке, отображающей объект анализа, подводят первичные стрелки — главные факторы, влияющие на объект, затем к каждой из них стрелки, изображающие вторичные факторы и т.д. до тех пор, пока на схеме не будут упомянуты все факторы, оказывающие заметное влияние на объект анализа. Каждая из стрелок, нанесенных на схему, представляет собой, в зависимости от ее положения, либо причину, либо следствие.

Трудность применения схемы Исикавы в такой постановке в том, что информация для ее построения собирается из всех доступных источников, выявляются и фиксируются все факторы. В результате часто получается громоздкая диаграмма, которая недостаточно четко структурирована, а потому не позволяет делать выводы. Поэтому рекомендуется при определении первичных факторов использовать мнемонический прием (от греч. *mnemonikon* — искусство запоминания) 5*m* (иногда 4*m* и 6*m*), определяя процесс формирования качества как взаимодействие 5*m:* m*aterial* (материал), m*achine* (оборудование), m*an* (исполнитель), m*ethod* (метод), m*easuring* (измерения) [20].

Рекомендуется также объединить «рыбий скелет» с методологией «пять почему?» или «очистка лука», позволяющей проанализировать проблему постепенно, «раздевая» ее с помощью последовательно задаваемых вопросов до тех пор, пока не будут выяснены ее причины. Обычно для этого достаточно найти ответ на «пять почему?». Метод «Пять почему?» был предложен в 1970-х гг. Сакиши Тойода — основателем компании Тойота. Метод не ставит целью выявить виновника, но позволяет найти причины возникновения проблемы. Пример использования схемы Исикавы при построении СУИБ показан на рис. 14.

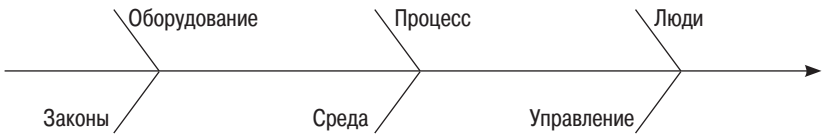

Рис. 14. *Использование схемы Исикавы при построении СУИБ*

С помощью схемы Исикавы можно исследовать все возможные причины проблемы, включая расследования, проведение опросов и т.п. Алгоритм работы с помощью Диаграммы Исикавы следующий.

1. Определите проблему. Выпишете в деталях точную проблему, с которой столкнулись. Определите, кто вовлечен, что представляет собой проблема, когда и где она возникла. Напишите проблему в квадрате с правой стороны. Проведите горизонтальную линию из квадрата через весь лист. Такое расположение выглядит как голова и позвоночник рыбы, что дает пространство для развития идей.

2. Разработайте основные влияющие факторы. Определите факторы, которые поспособствовали появлению проблемы. Нарисуйте линию от позвоночника для каждого фактора и подпишите ее. Это могут быть люди, вовлеченные в проблему, системы, среда, материалы, внешние факторы и пр. Постарайтесь написать как можно больше факторов. Если вы пытаетесь решить проблему с группой, то это подходящее время для мозгового штурма. Используя аналогию «Рыбья кость», факторы, которые вы выявите, могут выглядеть как кости рыбы.

3. Определите вероятные причины. Для каждого из факторов, которые вы рассмотрели на второй стадии, проведите мозговой штурм для определения возможных причин проблемы, которые связаны с факторами. Изобразите их мелкими линиями, исходящими из «костей» рыбы. Когда причина слишком большая или комплексная, лучше всего разбить ее на подпункты. Покажите их как линии, исходящие из линии причины.

4. Проанализируйте вашу диаграмму. На этом этапе у вас должна быть диаграмма, показывающая все возможные причины вашей проблемы. В зависимости от сложности и важности проблемы теперь вы можете исследовать наиболее вероятные причины с помощью расследований и опросов, что позволит проверить правильность оценки.

Схема Исикавы позволяет стимулировать творческое мышление, представить взаимосвязь между причинами и сопоставить их относительную важность. Она обладает рядом достоинств:

— позволяет графически отобразить взаимосвязь исследуемой проблемы и причин, влияющих на эту проблему;
— дает возможность провести содержательный анализ цепочки взаимосвязанных причин, воздействующих на проблему;
— удобна для применения и понимания персоналом. Для работы со схемой Исикавы не требуется высокая квалификация сотрудников, и нет необходимости проводить длительное обучение.

Стандарт ISO 27001 является основным стандартом в области ИБ. Сертификат соответствия данному стандарту является подтверждением зрелости СУИБ организации, улучшает репутацию компаний на международных рынках. Для соответствия стандарту ISO 27001 логичным шагом будет применение Цикла Шухарта-Деминга, позволяющего регулярно пересматривать и улучшать СУИБ, что является одним из требований стандарта.

Вопросы для самопроверки

1. В чем суть цикла Шухарта-Деминга?
2. Что такое СУИБ?
3. Что должен содержать документ «Политика ИБ»?
4. Опишите метод 8D и диаграмму Исикавы.

ЗАКЛЮЧЕНИЕ

Мы рассмотрели основные угрозы информационной безопасности и защиту от них. Защита информации в Российской Федерации осуществляется в соответствии с целым рядом законодательных актов, регулирующих вопросы защиты персональных данных, банковских транзакций, электронной подписи и другие аспекты.

Для защиты информации в организациях необходимо обеспечивать внедрение целого ряда мер. Среди них выделяют превентивные меры, решения для мониторинга и управления инцидентами, сдерживающие и детективные меры.

Для того чтобы выстраивание СУИБ носило системный характер, выстраивать ее надо в соответствии со стандартом ISO 27001. Это позволит использовать лучшие практики построения СУИБ, а также получить сертификат соответствия, который существенно улучшит репутацию компанию при взаимодействии с международными контрагентами.

В связи с большим количеством угроз ИБ внедрение СЗИ надо производить на основе оценки рисков. Это дает возможность понять, какие информационные системы требуют защиты в первую очередь, и грамотно распорядиться инвестициями в ИБ.

СУИБ — живой организм, который нуждается в постоянном пересмотре и улучшении. Для управления СУИБ рекомендуется использовать цикл Деминга, позволяющий организовать оптимальный процесс соответствия СУИБ актуальным угрозам ИБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Клименко И. С.* Информационная безопасность и защита информации. Модели и методы управления: монография. М.: ИНФРА-М, 2020. 178 с.
2. *Козьминых С. И.* Обеспечение комплексной защиты объектов информатизации: учебное пособие для студентов высших учебных заведений, обучающихся по направлению «Информационная безопасность», квалификация (степень) «магистр». М.: ЮНИТИ, 2020. 543 с.
3. *Сычев Ю. Н.* Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие для учебных заведений, реализующих программу среднего профессионального образования по укрупненной группе специальностей 10.02.00 «Информационная безопасность». М.: ИНФРА-М, 2020. 221 с.
4. *Бабаш А. В.* Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие. М.: РИОР: ИНФРА-М, 2019. 235 с.
5. *Бубнов А. А.*, *Пржегорлинский В. Н.*, *Савинкин О. А.* Основы информационной безопасности: учебник для студентов, обучающихся по специальностям укрупненной группы специальностей среднего профессионального образования «Информационная безопасность». 2-е изд., стер. М.: Академия, 2019. 253 с.
6. *Марков А. С.*, *Дорофеев А. В.*, *Барабанов А. В.*, *Цирлов В. А.* Семь безопасных информационных технологий. М.: ДМК-Пресс, 2017. 224 с.
7. *Кондратьев Э. В.*, *Адлер Ю. П.* Эффективность TWI по-русски: точки синергии // Методы менеджмента качества. 2019. № 2. С. 44–47.
8. *Адлер Ю. П.*, *Кондратьев Э. В.* Эффективность TWI по-русски: 5 полезных изменений // Методы менеджмента качества. 2019. № 7. С. 56–61.
9. *Трещев И. А.* Анализ защищенности распределенных информационных систем. Для студентов технических специальностей. Litres, 2018. 100 с.
10. *Адлер Ю.* От Lean до Agile и далее, без остановок // Proceedings /8th DQM International Conference Life cycle engineering and management. Editor Ljubisha Papic. Prijevor, Serbia, 2017, p. 3–13.
11. *Шваб К.* Четвертая промышленная революция. М.: Эксмо, 2018. 285 с.

12. Goldman, S. L., *Nagel R. N.*, *Preiss K.* Agile Competitors and Virtual Organizations: Strategies for Enriching the Customer. New York: Van Nostrand Reinhold, 1994. 414 p.
13. *Оуэн Р.*, *Коскела Л.*, *Гильерме Х.*, *Кудиньогу Р.* Применимо ли живучее управление в строительстве? // Менеджмент качества. 2008. № 4. С. 382–394; 2009. № 1. С. 18–24.
14. *Гродзенский Я. С.* Применение оптимальных статистических последовательных критериев для контроля технологических процессов // Метрология. 2009. № 5. С. 3–9.
15. *Карпов А.* Статический и динамический анализ кода. https://www.viva64.com/ru/b/0248/
16. *Гродзенский С. Я.*, *Гродзенский Я. С.*, *Чесалин А. Н.* Средства и методы управления Качеством: учебное пособие. М.: Проспект, 2019. 128 с.
17. *Исикава К.* Японские методы управления качеством: сокр. пер. с англ. М.: Экономика, 1988. 256 с.
18. *Родичев Ю. А.* Нормативная база и стандарты в области информационной безопасности: учебное пособие: третье поколение. СПб.: Питер, 2018. 254 с.
19. *Фомичев В. М.*, *Мельников Д. А.* Криптографические методы защиты информации: в 2 ч. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: Юрайт, 2017. 209 с.
20. *Гродзенский С. Я.* Управление качеством: учебник. 2-е изд. перераб. и доп. М.: Проспект, 2018. 320 с.

Приложение 1

ВИДЫ ИНФОРМАЦИИ, ТРЕБУЮЩЕЙ ЗАЩИТЫ

№	Вид информации	Содержимое	Нормативный акт	Ответственность за разглашение
1	Информация, составляющая коммерческую тайну	Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны	98-ФЗ «О коммерческой тайне»	183 УК РФ, 81 ТК РФ
2	Банковская тайна (тайна банковских вкладов)	Сведения об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией	ФЗ 395-1 «О банках и банковской деятельности», Статья 857 ГК РФ, Таможенный кодекс РФ, ФЗ «О реструктуризации кредитных организаций»	183 УК РФ, 81 ТК РФ
3	Служебная тайна	Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами	Указ Президента от 06.03.1997 № 188, 139 ГК РФ, ФЗ «Об основах государственной службы Российской Федерации», Постановление Правительства РФ от 03.11.1994 № 1233	81 ТК РФ

4	Тайна кредитной истории	Информация, которая характеризует исполнение заемщиком принятых на себя обязательств по договорам займа (кредита) и хранится в бюро кредитных историй	218-ФЗ «О кредитных историях»	81 ТК РФ
5	Тайна страхования	Сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также имущественном положении этих лиц	946 ГК РФ, от 29.11.2010 № 326-ФЗ, от 24.07.2009 № 212-ФЗ, от 24.07.1998 № 125-ФЗ.	81 ТК РФ
6	Тайна завещания	Сведения, касающиеся содержания завещания, его совершения, изменения или отмены	1123 ГК РФ	81 ТК РФ
7	Налоговая тайна	Любые, полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике (за рядом исключений)	146-ФЗ «Налоговый кодекс РФ»	183 УК РФ, 81 ТК РФ
8	Тайна усыновления ребенка	Это право, охраняемое законом, на сохранение интересов как усыновленного ребенка, так и его усыновителей, подразумевающее запрет на разглашение любой информации об определении ребенка в приемную семью	223-ФЗ «Семейный кодекс РФ»	155 УК РФ, 81 ТК РФ
9	Врачебная тайна	Сведения о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья. Информация о факте обращения за медицинской	117-ФЗ «О психиатрической помощи и гарантиях прав граждан при ее оказании» Основы законодательства РФ об охране здоровья граждан (Статья 61)	81 ТК РФ 151 ГК РФ, 1064 ГК РФ, 137 УК РФ, 81 ТК РФ

Продолжение табл.

№	Вид информации	Содержимое	Нормативный акт	Ответственность за разглашение
		помощью, состоянии здоровья гражданина, диагнозе заболевания, иные сведения, полученные при обследовании и лечении гражданина, а также сведения о проведенных искусственном оплодотворении эмбриона, а также о личности донора		
10	Медицинская тайна	Результаты обследования лица, вступающего в брак	223-ФЗ «Семейный кодекс РФ»	81 ТК РФ
11	Сведения о доноре и реципиенте	Врачебная тайна	4180-1-ФЗ «О трансплантации органов и (или) тканей человека»	81 ТК РФ
12	Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений		176-ФЗ «О почтовой связи», 126-ФЗ «О связи», Статья 13 УПК РФ	138 УК РФ, 81 ТК РФ
13	Тайна частной жизни (личная тайна)	Личная и семейная тайна	Конституция РФ (Статья 23), 150 ГК РФ	137 УК РФ, 81 ТК РФ
14	Аудиторская тайна	Любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг (за рядом исключений)	307-ФЗ «Об аудиторской деятельности»	81 ТК РФ

15	Тайна судопроизводства (тайна следствия)		241 УПК РФ, 10 ГПК РФ, 11 АПК РФ, 166 УПК РФ, Указ Президента от 06.03.1997 № 188, от 10.06.2008 № 76-ФЗ	81 ТК РФ
16	Адвокатская тайна (она же тайна судебного представительства)	Любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	63-ФЗ «Об адвокатской деятельности и адвокатуре в РФ»	81 ТК РФ
17	Тайна нотариальных действий (относится к профессиональной тайне)	— содержание нотариального действия; — информация о лицах, в отношении которых совершено нотариальное действие; — сам факт обращения к нотариусу или отсутствие его; — документы, истребованные нотариусом;	«Основы законодательства РФ о нотариате», от 05.07.2010 № 154-ФЗ	81 ТК РФ
18	Профессиональная тайна		Указ Президента РФ от 06.03.1997 № 188	81 ТК РФ
19	Персональные данные		143-ФЗ «Об актах гражданского состояния», 152-ФЗ «О персональных данных», 242-ФЗ «О государственной геномной регистрации в РФ»	13.11 КОАП РФ, 137 УК РФ, 81 ТК РФ
20	Тайна исповеди		125-ФЗ «О свободе совести и о религиозных объединениях»	

Продолжение табл.

№	Вид информации	Содержимое	Нормативный акт	Ответственность за разглашение
21	Государственная тайна		ФЗ 5485-1 «О государственной тайне», Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»	81 статья ТК РФ, 283 статья УК РФ
22	Семейная тайна		23 и 38 Статьи Конституции РФ, 150 Статья ГК РФ	137 статья УК РФ, 81 статья ТК РФ
23	Тайна голосования		51-ФЗ «О выборах депутатов Государственной думы Федерального Собрания РФ», 19-ФЗ «О выборах Президента РФ», 67-ФЗ «Об основных гарантиях избирательного права и права на участие в референдуме граждан РФ»	141 статья УК РФ, 81 статья ТК РФ
24	Секрет производства (ноу-хау)		1465 ГК РФ	183 статья УК РФ, 81 статья ТК РФ
25	Тайна предварительного следствия		139 УПК РФ, ФЗ 2202-1 «О прокуратуре РФ»	310 статья УК РФ, 81 статья ТК РФ

26	Тайна сведений о мерах безопасности в отношении судьи и иных участников		311 статья УК РФ	311 статья УК РФ, 81 статья ТК РФ
27	Тайна сведений о мерах безопасности в отношении должностного лица правоохранительного органа или контролирующего органа		320 статья УК РФ, 17.13 статья КОАП	320 статья УК РФ, 17.13 статья КОАП, 81 статья УК РФ
28	Сведения о сущности изобретения, полезной модели или промышленного образца до их официальной публикации		147 статья УК РФ, 7.12 статья КОАП	147 статья УК РФ, 7.12 Статья КОАП, 81 статья ТК РФ

Продолжение табл.

№	Вид информации	Содержимое	Нормативный акт	Ответственность за разглашение
29	Журналистская тайна		2124-1-ФЗ «О средствах массовой информации»	144 статья УК РФ, 29 статья Конституции РФ, 81 Статья ТК РФ
30	Тайна вероисповедания	Сведения об отношении к религии, к исповеданию или отказу от исповедания религии, об участии или не участии в богослужениях, других религиозных обрядах и церемониях, о деятельности в религиозных объединениях, об обучении религии	125-ФЗ «О свободе совести и о религиозных объединениях», 152-ФЗ	148 статья УК РФ, 81 статья ТК РФ
31	Тайна сведений о военнослужащих внутренних войск МВД России	Сведения о местах дислокации или о передислокации соединений и воинских частей внутренних войск, а также сведения о военнослужащих внутренних войск, принимавших участие в пресечении деятельности вооруженных преступников, незаконных вооруженных формирований и иных организованных преступных групп, а также сведений о членах их семей	27-ФЗ «О внутренних войсках МВД РФ»	81 ТК РФ, 283 статья УК РФ
32	Тайна сведений личного характера, ставших известными работникам учреждений	Профессиональная тайна	122-ФЗ «О социальном обслуживании граждан пожилого возраста и инвалидов», 152-ФЗ	81 статья ТК РФ

33	Тайна ценных бумаг	Любая не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу своего служебного положения, трудовых обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг	224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты РФ»	
34	Военная тайна	Гостайна или Служебная тайна Вооруженных Сил РФ		
35	Тайна сведений о лицах, внедренных в организованные преступные группы, штатных негласных сотрудников органов, осуществляющих оперативно-розыскную деятельность		76-ФЗ «О статусе военнослужащих», Устав внутренней службы Вооруженных Сил РФ, 144-ФЗ «Об оперативно-розыскной деятельности»	81 статья ТК РФ, 283 статья УК РФ
36	Тайна совещания судей	Суждения, имевшие место при обсуждении и постановлении приговора	298 УПК РФ	81 ТК РФ

Окончание табл.

№	Вид информации	Содержимое	Нормативный акт	Ответственность за разглашение
37	Тайна совещания присяжных судей	Суждения, имевшие место во время совещания	341 УПК РФ	81 ТК РФ
38	Дактилоскопическая тайна	Информация об особенностях строения папиллярных узоров пальцев рук человека и о его личности (охраняется в режиме служебной тайны	128-ФЗ «О государственной дактилоскопической регистрации в РФ», 152-ФЗ	81 ТК РФ
46	Депутатская тайна		3-ФЗ «О статусе депутата Совета Федерации и статусе депутата Государственной Думы Федерального Собрания РФ», статья 56 УПК РФ	81 ТК РФ

Приложение 2

НАЦИОНАЛЬНЫЕ СТАНДАРТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Обозначение	Наименование на русском языке
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
ГОСТ Р 50922-2006	Защита информации. Основные термины и определения
ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство
ГОСТ Р 51275-2006	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
ГОСТ Р 51583-2014	Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
ГОСТ Р 52069.0-2013	Защита информации. Система стандартов. Основные положения
ГОСТ Р 52447-2005	Защита информации. Техника защиты информации. Номенклатура показателей качества
ГОСТ Р 52448-2005	Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения
ГОСТ Р 52633.0-2006	Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации
ГОСТ Р 52633.1-2009	Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
ГОСТ Р 52633.2-2010	Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
ГОСТ Р 52633.3-2011	Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора
ГОСТ Р 52633.4-2011	Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия – код доступа

Продолжение табл.

Обозначение	Наименование на русском языке
ГОСТ Р 52633.5-2011	Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа
ГОСТ Р 52633.6-2012	Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой»
ГОСТ Р 52863-2007	Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования
ГОСТ Р 53109-2008	Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности
ГОСТ Р 53110-2008	Система обеспечения информационной безопасности сети связи общего пользования. Общие положения
ГОСТ Р 53111-2008	Устойчивость функционирования сети связи общего пользования. Требования и методы проверки
ГОСТ Р 53112-2008	Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний
ГОСТ Р 53113.1-2008	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения
ГОСТ Р 53113.2-2009	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов
ГОСТ Р 53114-2008	Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
ГОСТ Р 53115-2008	Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства
ГОСТ Р 53131-2008	Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения

ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы
ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия
ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия
ГОСТ Р 56045-2014	Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью
ГОСТ Р 56093-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования
ГОСТ Р 56103-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения
ГОСТ Р 56115-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования
ГОСТ Р ИСО/МЭК 13335-1-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
ГОСТ Р ИСО/МЭК ТО 13335-5-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

Окончание табл.

Обозначение	Наименование на русском языке
ГОСТ Р ИСО/МЭК 15408-1-2012	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ГОСТ Р ИСО/МЭК 15408-2-2013	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности
ГОСТ Р ИСО/МЭК 15408-3-2013	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности
ГОСТ Р ИСО/МЭК ТО 15446-2008	Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности
ГОСТ Р ИСО/МЭК ТО 18044-2007	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
ГОСТ Р ИСО/МЭК 18045-2013	Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК ТО 19791-2008	Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
ГОСТ Р ИСО/МЭК 21827-2010	Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса
ГОСТ Р ИСО/МЭК 27000-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ГОСТ Р ИСО/МЭК 27001-2006	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ГОСТ Р ИСО/МЭК 27002-2012	Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности
ГОСТ Р ИСО/МЭК 27003-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27004-2011	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
ГОСТ Р ИСО/МЭК 27005-2010	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
ГОСТ Р ИСО/МЭК 27006-2008	Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности
ГОСТ Р ИСО/МЭК 27007-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности
ГОСТ Р ИСО/МЭК 27013-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1
ГОСТ Р ИСО/МЭК 27033-1-2011	Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
ГОСТ Р ИСО/МЭК 27033-3-2014	Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления
ГОСТ Р ИСО/МЭК 27034-1-2014	Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия
ГОСТ Р ИСО/МЭК 27037-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме
ГОСТ Р ИСО/МЭК 29100-2013	Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности
Рекомендации по стандартизации Р 50.1.050-2004	Защита информации. Система обеспечения качества техники защиты информации. Общие положения
Рекомендации по стандартизации Р 50.1.053-2005	Информационные технологии. Основные термины и определения в области технической защиты информации
Рекомендации по стандартизации Р 50.1.056-2005	Техническая защита информации. Основные термины и определения

Приложение 3

НОРМАТИВНЫЕ АКТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральные законы

- Конституция Российской Федерации (1993)
- Закон РФ «О безопасности» от 05.03.1992 № 2446-1
- Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (с изм. и доп., вступающими в силу с 15.12.2007)
- ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
- ФЗ РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ
- ФЗ РФ «О персональных данных» от 27.07.2006 № 152-ФЗ
- ФЗ «О техническом регулировании» от 27.12.2002 № 184-ФЗ
- ФЗ РФ «Об обеспечении единства измерений» от 26.06.2008 № 102-ФЗ
- ФЗ РФ «Электронной цифровой подписи» от 10.01.2002 № 1-ФЗ
- ФЗ РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ
- ФЗ РФ «О связи» от 07.07.2003 № 126-ФЗ
- ФЗ «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ
- ФЗ «Об органах Федеральной Службы Безопасности в Российской Федерации» 03.04.1995 № 40-ФЗ (СЗ РФ. 1995. № 15. Ст. 1269)
- ФЗ «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

1. «Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 № К 1274) (Совет безопасности РФ)

2. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

3. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам»)

4. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Зарегистрировано в Минюсте России 06.09.2018 № 52108) (Кодекс)

5. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Критическая информационная инфраструктура

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

2. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 № 803) (Совет безопасности РФ)

3. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

4. Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

5. Постановление Правительства РФ от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»

6. Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (Зарегистрировано в Минюсте России 30.06.2014 № 32919)

7. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации (Зарегистрировано в Минюсте России 08.02.2018 № 49966)

8. Приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 28.12.2017 № 49500)

9. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (Зарегистрировано в Минюсте России 22.02.2018 № 50118)

10. Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (Зарегистрировано в Минюсте России 13.04.2018 № 50753)

11. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 09.08.2018) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 26.03.2018 № 50524)

12. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК России от 04.05.2018 № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации»

13. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК России от 24.08.2018 № 240/25/3752 «По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Приложение 4

ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Федеральные законы

— Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
— Федеральный закон от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии» http://zlonov.ru/wp-content/uploads/Федеральный-закон-от-21.11.1995-170-ФЗ-Об-использовании-атомной-энергии.pdf http://base.garant.ru/10105506/ http://docs.cntd.ru/document/9014484 http://www.consultant.ru/document/cons_doc_LAW_148639/ http://pravo.gov.ru/proxy/ips/?docbody=&nd=102038289
— Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов» http://zlonov.ru/wp-content/uploads/Федеральный-закон-от-21.07.1997-116-ФЗ-О-промышленной-безопасности-опасных-производственных-объектов.pdf http://base.garant.ru/11900785/ http://docs.cntd.ru/document/9046058 http://www.consultant.ru/document/cons_doc_LAW_173548/ http://pravo.gov.ru/proxy/ips/?docbody=&nd=102048376
— Федеральный закон от 21.07.1997 № 117-ФЗ «О безопасности гидротехнических сооружений» http://zlonov.ru/wp-content/uploads/Федеральный-закон-от-21.07.1997-117-ФЗ-О-безопасности-гидротехнических-сооружений.pdf http://base.garant.ru/12100061/ http://docs.cntd.ru/document/9046062 http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=law;n=156787 http://pravo.gov.ru/proxy/ips/?docbody=&nd=102048349
— Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» http://zlonov.ru/wp-content/uploads/Федеральный-закон-от-9-февраля-2007-г.--16-ФЗ-О-транспортной-безопасности.pdf http://base.garant.ru/12151931 http://docs.cntd.ru/document/902027326 http://www.consultant.ru/document/cons_doc_LAW_158524/ http://pravo.gov.ru/proxy/ips/?docbody=&nd=102111823
— Федеральный закон от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» http://zlonov.ru/wp-content/uploads/Федеральный-закон-от-21-июля-2011-г.-256-ФЗ-О-безопасности-объектов-топливно-энергетического-комплекса.pdf http://base.garant.ru/12188188/ http://docs.cntd.ru/document/902290768 http://www.consultant.

ru/document/cons_doc_LAW_169797/ http://pravo.gov.ru/proxy/ips/?docbody=&nd=102149573

— Федеральный закон от 21.07.2011 № 257-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения безопасности объектов топливно-энергетического комплекса» http://zlonov.ru/wp-content/uploads/Федеральный-закон-от-21.07.2011-г.-257-ФЗ-О-внесении-изменений-в-отдельные-законодательные-акты-РФ.pdf http://base.garant.ru/12188189/ http://docs.cntd.ru/document/902290765 http://www.consultant.ru/document/cons_doc_LAW_153485/ http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102149574
— Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»

Указы Президента РФ

— Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» http://zlonov.ru/wp-content/uploads/Указ-Президента-РФ-от-12.05.2009--537-О-Стратегии-национальной-безопасности-Российской-Федерации-до-2020-года.pdf http://base.garant.ru/195521/ http://docs.cntd.ru/document/902156214 http://www.consultant.ru/document/cons_doc_LAW_165072/ http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631
— Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года (утв. Президентом РФ 15.11.2011, Пр-3400) http://zlonov.ru/wp-content/uploads/Основы-государственной-политики-в-области-обеспечения-безопасности-населения-РФ-и-защищенности-КВО-и-ПОО.pdf http://www.garant.ru/products/ipo/prime/doc/70041358/ http://docs.cntd.ru/document/499055777 http://www.consultant.ru/document/cons_doc_LAW_174322/
— Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)» http://zlonov.ru/wp-content/uploads/Указ-Президента-РФ-от-15.01.2013-31с-О-создании-ГосСОПКА.pdf http://www.garant.ru/products/ipo/prime/doc/70199068/ http://docs.cntd.ru/document/902392496 http://www.consultant.ru/document/cons_doc_LAW_140909/ http://pravo.gov.ru:8080/page.aspx?35023

— Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013, Пр-1753) http://zlonov.ru/wp-content/uploads/Основы-государственной-политики-РФ-в-области-международной-ИБ-на-период-до-2020-года.pdf

Документы Правительства РФ

— Распоряжение Правительства РФ от 27.08.2005 № 1314-р «Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры РФ и опасных грузов»
— Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры и их значений» http://zlonov.ru/wp-content/uploads/Распоряжение-Правительства-РФ-от-27.08.2005-1314-р-Об-одобрении-Концепции-федеральной-системы-мониторинга-КВО.pdf http://iv.garant.ru/document?id=88549 http://docs.cntd.ru/document/901945388
— Постановление Правительства РФ от 21.05.2007 № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера» http://zlonov.ru/wp-content/uploads/Постановление-Правительства-РФ-от-21.05.2007-304-О-классификации-чрезвычайных-ситуаций-природного-и-техногенного-характера.pdf http://base.garant.ru/12153609/ http://docs.cntd.ru/document/902043525 http://www.consultant.ru/document/cons_doc_LAW_114211/
— Постановление Правительства РФ от 22.12.2011 № 1107 «О порядке формирования и ведения реестра объектов топливно-энергетического комплекса» http://zlonov.ru/wp-content/uploads/Постановление-Правительства-РФ-от-22.12.2011-1107-О-порядке-формирования-и-ведения-реестра-объектов-ТЭК.pdf http://base.garant.ru/70120040/ http://docs.cntd.ru/document/902321164 http://www.consultant.ru/document/cons_doc_LAW_124278/
— Постановление Правительства РФ от 05.05.2012 № 459 «Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса, порядке его проведения и критериях категорирования» http://zlonov.ru/wp-content/uploads/Постановление-Правительства-РФ-от-05.05.2012-

459-Об-утверждении-Положения-об-исходных-данных-для-проведения-категорирования-объекта-ТЭК.pdf http://base.garant.ru/70173868/ http://docs.cntd.ru/document/902346050 http://www.consultant.ru/document/cons_doc_LAW_129654/

— Постановление Правительства РФ от 05.05.2012 № 460 «Об утверждении Правил актуализации паспорта безопасности объекта топливно-энергетического комплекса» http://zlonov.ru/wp-content/uploads/Постановление-Правительства-РФ-от-05.05.2012-460-Об-утверждении-Правил-актуализации-паспорта-безопасности-объекта-ТЭК.pdf http://base.garant.ru/70172076/ http://docs.cntd.ru/document/902345684 http://www.consultant.ru/document/cons_doc_LAW_178341/
— Постановление Правительства Российской Федерации от 02.10.2013 № Р861 «Об утверждении Правил информирования субъектами топливно-энергетического комплекса об угрозах совершения и о совершении актов незаконного вмешательства на объектах топливно-энергетического комплекса» http://zlonov.ru/wp-content/uploads/Постановление-Правительства-РФ-от-02.10.2013-861-Об-утверждении-Правил-информирования-субъектами-ТЭК.pdf http://ivo.garant.ru/document?id=70364138 http://docs.cntd.ru/document/499047629 http://www.consultant.ru/document/cons_doc_LAW_152677/ http://pravo.gov.ru/proxy/ips/?docbody=&nd=102168052

Документы Совета Федерации и Совета Безопасности

— Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012, 803) http://zlonov.ru/wp-content/uploads/Основные-направления-госполитики-в-области-обеспечения-безопасности-АСУ-ПиТП-КВО.pdf

Документы ФСТЭК

— Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
— Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объек-

тов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

- Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
- Приказ ФСТЭК России от 25.12.2107 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
- Информационное сообщение ФСТЭК России от 25.07.2014 № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 “Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды”»
- Информационное сообщение ФСТЭК России от 24.08.2018 № 240/25/3752 по вопросам предоставления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
- Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период (утв. ФСТЭК России 23.04.2011) http://zlonov.ru/wp-content/uploads/Методические-рекомендации-по-формированию-аналитического-прогноза-по-укомплектованию-подразделений.pdf http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=119625

Министерство энергетики

- Приказ Министерства энергетики РФ от 13.12.2011 № 587 «Об утверждении перечня работ, непосредственно связанных с обеспечением безопасности объектов топливно-энергетического

комплекса» http://zlonov.ru/wp-content/uploads/Приказ-Минэнерго-РФ-от-13.12.2011-587-Об-утверждении-перечня-работ-непосредственно-связанных-с-обеспечением-безопасности-объектов-ТЭК.pdf http://ivo.garant.ru/document?id=70032916&byPara=1&sub=1 http://docs.cntd.ru/document/902320371 http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=125336;div=LAW

— Приказ Министерства энергетики РФ от 10.02.2012 № Р48 «Об утверждении методических рекомендаций по включению объектов топливно-энергетического комплекса в перечень объектов, подлежащих категорированию» http://zlonov.ru/wp-content/uploads/Приказ-Минэнерго-РФ-от-10.02.2012-48-Об-утверждении-методических-рекомендаций-по-включению-объектов-ТЭК-в-перечень.pdf http://base.garant.ru/70184568/ http://www.consultant.ru/document/cons_doc_LAW_137344/

ГОСТы

— ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008) «Защищенность (кибербезопасность) промышленного процесса измерения и управления»
— ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»
— ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее — ГОСТ Р 51624)
— ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения»

Международные стандарты

— ISO 27000 Серия международных стандартов по ИБ
— IEC 62210 Power system control and associated communications — Data and communication security
— IEC 62351 Power systems management and associated information exchange — Data and communications security — Part 3: Communication network and system security — Profiles including TCP/IP
— IEEE 1402 Guide for electric power substations physical and electronic security
— Семейство отраслевых стандартов NERC
— Семейство стандартов NIST

ОГЛАВЛЕНИЕ