Объекты аудита информационной безопасности и направления их проверки

Objects of Information Security Audit and Directions of Their Verification

УДК 657.6

DOI: 10.12737/1998-0701-2022-8-1-21-31

Л.В. Каширская, д-р экон. наук, профессор Департамента аудита и корпоративной отчетности, Финансовый университет при Правительстве РФ, г. Москва

e-mail: kashirskaya76@mail.ru

Ю.А. Зурнаджьянц, канд. экон. наук, доцент кафедры экономики и управления здравоохранением с курсом последипломного образования, Астраханский государственный медицинский университет

e-mail: julia.zur@yandex.ru

L.V. Kashirskaya, Doctor of Economic Sciences, Professor, Audit and Corporate Reporting Department, Financial University under the Govemment of the Russian Federation, Moscow

e-mail: kashirskaya76@mail.ru

Yu.A. Zurnadzhyants, Candidate of Economic Sciences, Associate Professor, Department of Economics and Health Care Management with Postgraduate Course, Astrakhan State Medical University

e-mail: julia.zur@yandex.ru

Аннотация. *Статья посвящена исследованию объектов аудита информационной безопасности, в состав которых включается информация, хранящаяся и обрабатываемая на предприятии; информационные ресурсы, на которых хранится информация; информационные каналы, по которым передается информация; программное обеспечение, используемое для обработки информации; юридическая и техническая документация по аппаратному и программному обеспечению и средства физической защиты информации, а также характеристике этапов проведения аудита таких объектов. В статье сделан вывод о том, что ввиду непрерывного и динамического развития информационных объектов в компаниях назрела необходимость группировки таких объектов и формирования на ее основе основных элементов аудита информационной безопасности.*

Ключевые слова: экономический контроль, аудит, информационная безопасность, объекты аудита, информация, информационные ресурсы, информационные каналы, программное обеспечение, юридическая и техническая документация, средства физической защиты информации.

Abstract. *The article is devoted to the study of information security audit objects, which include information stored and processed at the enterprise; information resources on which information is stored; information channels through which information is transmitted; software used to process information; legal and technical documentation on hardware and software and means of physical protection of information, as well as the characteristics of the stages of the audit of such objects. The article concludes that in view of the continuous and dynamic development of information objects in companies, there is a need to group such objects and form, on its basis, the main elements of information security audit.*

Keywords: economic control, audit, information security, audit objects, information, information resources, information channels, software, legal and technical documentation, means of physical protection of information.

Сегодня информация все чаще становится инструментом торговли, подрыва деловой репутации, хищения интеллектуальной собственности в виде новых разработок и технологий, в том числе с помощью компьютерных атак, хищений, рейдерских захватов, при этом организаторами этих действий зачастую становятся не только конкуренты, но и сотрудники компании с целью шантажа, продажи, захвата власти. К таким событиям может приводить несоблюдение установленных правил защиты: отсутствие понимания сотрудниками наличия и составляющих конфиденциальной информации и государственной и коммерческой тайны; отсутствие систем автоматизированной защиты данных; хранение документов не должным образом; беспрепятственный доступ к документам случайных лиц или не имеющих на это полномочий; отсутствие защищенных систем хранения и дублирования информации и т.д. Эти проблемные вопросы и определяют область аудита, связанную с выполнением части аудиторского задания в виде аудита информационной безопасности, который на сегодняшний

день становится все более востребованным, а ввиду отсутствия разработок элементов таких проверок, требует их изучения.

В данной статье аудит рассматривается в широком смысле этого понятия как область проверок. В этой связи под аудитом информационной безопасности понимается системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определенными критериями и показателями безопасности.

По объектам проверки аудит информационной безопасности можно классифицировать:

- на информацию, хранящуюся и обрабатываемую на предприятии;
- информационные ресурсы, на которых хранится информация;
- информационные каналы, по которым передается информация;
- программное обеспечение, используемое для обработки информации;
- юридическую и техническую документацию по аппаратному и программному обеспечению;
- средства физической защиты информации.

В качестве ориентира при проведении аудита информационной безопасности можно представить перечень возможных типичных нарушений, выявляемых при проверке, которые представлены нами в табл. 1.

Рассмотрим основные объекты и присущие им этапы проведения аудита информационной безопасности.

Аудит информации, хранящейся и обрабатываемой на предприятии

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация, в зависимости от категории доступа к ней, подразделяется [1]:

- на общедоступную информацию, к которой относятся общеизвестные сведения и иная информация, доступ к которой не ограничен (перечень сведений, доступ к которым не может быть ограничен, указан в статье 10 упомянутого закона);
- информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В свою очередь, информация ограниченного доступа подразделяется:

- на информацию, отнесенную к государственной или коммерческой тайне. Отнесение

Таблица 1

Перечень типичных нарушений при аудите информационной безопасности

Типичные нарушения
1. Манипулирование информацией (дезинформация, сокрытие и искажение информации)
2. Незаконное копирование, уничтожение, хищение данных и программ, уничтожение носителей информации
3. Хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа
4. Отсутствие утвержденного порядка и требований предоставления пользователям доступа в Интернет, применения электронной почты
5. Запись пароля доступа на мониторе, компьютере и на других близко расположенных предметах
6. Оставленный без присмотра компьютер с открытым доступом к информации компании
7. Не соблюдается режим регулярной смены паролей
8. Потеря переносных персональных устройств (Notebook)
9. Подключение к внешним сетям через модемы, минуя средства защиты (Firewall и другие общие меры безопасности)
10. Подключение к сети предприятия посторонних носителей информации
11. Использование нелицензионного программного обеспечения
12. Отсутствие антивирусных программ, сетевых экранов, файерволов и других средств программной защиты
13. Отсутствие удаленных серверов, защищенных от скачков напряжения, пожаров, рейдерских захватов и воровства

информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне» [2]. Отнесение информации к коммерческой тайне регулируется Федеральным законом «О коммерческой тайне» [3];

- сведения конфиденциального характера. Перечень таких сведений содержится в указе Президента РФ от 06.03.1997 № 188 [4].

Для понимания различия между понятиями «конфиденциальная информация» и «коммерческая тайна» рассмотрим их более детально, что и сделано нами в табл. 2 [5].

На основании вышеизложенного можно предложить основные этапы аудита информации, хранящейся и обрабатываемой на предприятии (рис. 1)

Аудит информационных ресурсов, на которых хранится информация

К таким информационным ресурсам можно отнести (табл. 3):

- серверы;
- файловые и облачные хранилища;
- съемные и переносные устройства для хранения файлов [8].

Таблица 2

Сходство и различие «конфиденциальной информации» и «коммерческой тайны»

Признак	Конфиденциальная информация	Коммерческая тайна
Определение	Сведения, доступ к которым ограничен законом, а их разглашение наказуемо	Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
Нормативное регулирование	Федеральный закон от 27.07. 2006 № 149-ФЗ «Об информации, и информационных технологиях и о защите информации», статья 9 [1] Регламент ФНС России № САЭ-3-13848@ «Об обмене электронными документами» [6]	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [3]
Расхождение понятий	Сведения, неразглашение которых гарантировано законами Российской федерации. При этом они могут быть как коммерческими, так и нет	Может быть не защищена конкретным нормативным актом страны, а установлена в качестве секретной любым лицом или организацией
Сходство понятий	Являются ценным ресурсом для держателей, не все имеют к ним доступ, обладатель тайны считает ее разглашение нарушением. И те, и другие сведения являются предметом получения выгоды для лиц, которые ею владеют	
Перечень сведений, не предусмотренных к засекречиванию	• маркетинговые исследования рынков товаров и услуг; • сведений о технологиях производства и особенностях производственного процесса; • сведения о научных разработках (ноу-хау и проч.); • сведения о деловых партнерах (заказчиках, подрядчиках, поставщиках, торговых агентах, в том числе закупочных ценах и фактах ведения переговоров) и т.д.	• данные в учредительных документах компании, а также ЕГРЮЛ и ЕГРИП; • документы, дающие право заниматься бизнесом; • информация о загрязнении окружающей среды, состоянии противопожарной безопасности и т. д.; • условия труда в компании (численность, состав работников, система оплаты труда, наличие свободных рабочих мест и т.п.); • информация о задолженности по выплате заработной платы и по иным социальным выплатам; • данные о нарушениях законодательства РФ и фактах привлечения к ответственности; • данные о перечне лиц, имеющих право действовать без доверенности от имени компании

Окончание табл. **2**

Признак	Конфиденциальная информация	Коммерческая тайна
Перечень сведений, возможный к засекречиванию	• данные, составляющие служебную тайну; • информация, связанная с профессиональной деятельностью гражданина (например, врачебная или адвокатская тайна); • данные, связанные с функционированием коммерческой организации (коммерческая тайна); • информация о тайне следствия и судопроизводства; • данные о частной жизни человека, позволяющие его идентифицировать (персональные данные); • информация о сущности нового изобретения, информация о котором еще не опубликована; • данные о принудительном исполнении судебных и властных актов, а также сведения, содержащиеся в личных делах осужденных граждан [7]	• сведения об условиях заключенных контрактов; • определенные технологические производственные процессы; • разработанные стандарты по существующим бизнес-процессам в компании; • перспективные планы развития компании; • сведения о подготовке и результатах переговоров с деловыми партнерами компании; • сведения о бизнес-идеях и результаты их исследований; • сведения о внешнем и внутреннем финансировании; • сведения о мероприятиях налогового планирования и о налоговых рисках
Ответственность за разглашение информации	Ответственность за утечку конфиденциальных сведений предусмотрена в законах, регламентирующих разные их виды. Уголовное наказание предусмотрено за разглашение государственной тайны — тюремный срок от 3 до 7 лет или ограничение в праве на определенную деятельность до 3 лет [7]	За разглашение коммерческой тайны законом предусмотрено: • административное наказание — выговор, увольнение, штраф до 1,5 млн рублей; • уголовная ответственность — лишение свободы до 7 лет [7]

Этапы аудита информации, хранящейся и обрабатываемой на предприятии

1 этап	Сбор и систематизация данных об информации, которая возникает, хранится и передается внутри компании. Установить, структурирована ли эта информация на информацию, которая может находиться в открытом доступе и информацию, составляющую коммерческую тайну и конфиденциальную информацию; есть ли в обработке информация, содержащая служебную и государственную тайну. Выяснить составлены ли регламенты по ее хранению и обработке, соответствующие действующему законодательству
2 этап	Проверка возможности утечки информации «через человеческий фактор», в том числе путем сопоставления штатного расписания компании и схемы структурирования информации в целях выявления того, не получает ли кто-либо из сотрудников доступ к информации, которая не является для него необходимой
3 этап	Систематизация на основе понимания возможности и необходимости доступа сотрудников к информации, подлежащей охране, и правомерности предоставления доступа к этой информации в соответствии с занимаемой сотрудником должностью
4 этап	Проверка порядка систематизации, классификации и порядка обработки потоков информации, составляющей коммерческую тайну и конфиденциальную информацию
5 этап	Исследование информации, требующей особого контроля, в целях выявления возможности ее попадания на информационные ресурсы открытого доступа путем сопоставления схемы обработки информации со схемой ИТ-инфраструктуры предприятия (хранится в отделе информационных технологий)

Рис. 1. Этапы аудита информации, хранящейся и обрабатываемой на предприятии

Доступ к информационным ресурсам, на которых хранится информация, может осуществляться в целях:

- скачивания информации, как правило, для получения коммерческих секретов;
- проникновения к информации с целью ее уничтожения, как правило, для нарушения нормальной работы компании;
- порчи или подмены информации, как правило, для внесения изменений или введения новых данных.

Основные этапы аудита информационных ресурсов, на которых хранится информация, представлены нами на рис. 2.

Аудит информационных каналов, по которым передается информация

К основным информационным каналам, по которым передается информация, относятся:

- сети;
- узлы маршрутизации;
- шлюзы;
- коммуникационное оборудование провайдера (при наличии).

Таблица 3

Основные информационные ресурсы, на которых хранится информация

Понятие	Определение
Облачные и файловые хранилища	Хранилища пользовательских и других файлов; удаленные игровые сервисы; антивирусные службы; средства обработки информации на основе веб-интерфейса
Сервер	Выделенный или специализированный компьютер для выполнения сервисного программного обеспечения (в том числе серверов тех или иных задач)
Съемное и переносное устройство для хранения файлов	Средство хранения и переноса информации с одного компьютера на другие. В качестве носителей информации чаще всего выступают оптические диски (CD, DVD, Blu-Ray), флеш-накопители (флешки) и внешние жесткие диски

Этапы аудита информационных ресурсов, на которых хранится информация

1 этап	Систематизация перечня съемных и переносных устройств для хранения файлов и определение того, какого рода информация (открытая или информация, подлежащая особой охране) может на них оказаться, а также являются ли они возможными каналами утечки информации
2 этап	Проверка вариативности доступа пользователей к информационным ресурсам, доступа к ним пользователей с правами, которые для выполнения их работы избыточны, путем сопоставления списка съемных и переносных устройств для хранения файлов и информации, которая хранится на этих устройствах, со штатным расписанием и списком логинов пользователей, взятых из операционных систем, обеспечивающих функционирование информационных ресурсов [8]
3 этап	Проверка соответствия паролей пользователей и администраторов требованиям безопасности (наличие традиционного стандарта кодирования пароля – определенная длина, использование минимум одной цифры, одной заглавной буквы, специального символа
4 этап	Проверка использования облачных сервисов только для открытой информации, а не для информации, подлежащей охране, для которой необходимо использовать собственные серверы компании
5 этап	Проверка возможности использования специализированного программного обеспечения, фиксирующего все действия пользователя при обработке информации на информационном ресурсе, возможности формирования отчетных данных о произведенных пользователем действиях

Рис. 2. Этапы аудита информационных ресурсов, на которых хранится информация

Приведем основные понятия, используемые в рамках формирования этапов аудита информационных каналов, по которым передается информация (табл. 4).

С использованием приведенных понятий опишем основные этапы аудита информационных каналов, по которым передается информация (рис. 3).

Аудит программного обеспечения, используемого для обработки информации

В целом программные средства обработки информации — это инструментальные наборы, применяемые в компьютерном оборудовании для обработки текстовых, графических и других информационных данных. К программному обеспечению, используемому для обработки информации, относятся:

- системное программное обеспечение;
- инструменты технологических методик программирования;
- пакеты прикладного программного обеспечения.

Учитывая составляющие данного направления проверки, можно предложить этапы аудита программного обеспечения, представленные на рис. 4.

Аудит юридической и технической документации по аппаратному и программному обеспечению

Заметим, что согласно части IV Гражданского кодекса Российской Федерации программы для ЭВМ и базы данных включены в перечень результатов интеллектуальной деятельности (интеллектуальной собственности), которым предоставлена правовая охрана (статья 1225 ГК РФ) [9]. Интеллектуальные права включают в себя «исключительное право», являющееся имущественным правом, а также личные неимущественные права и иные права (в предусмотренных ГК РФ случаях).

Интеллектуальные права на программы для ЭВМ и базы данных входят в сферу авторского права и охраняются законом как литературные произведения (ст. 1261 ГК РФ) [9]. Поэтому интеллектуальные права на программы для ЭВМ и базы данных называют еще и «авторскими правами», а сам результат интеллектуальной деятельности (программное обеспечение) — «произведениями». Обладатель исключительного права именуется «правообладателем».

Таблица 4

Основные понятия и информационные каналы, по которым передается информация

Понятие	Определение
Сеть	Сеть, основной задачей которой является передача данных, в которой продуктом генерирования, переработки, хранения и использования является информация
Узлы маршрутизации	Точки сети с несколькими интерфейсами, каждый из которых имеет свой MAC-адрес и IP-адрес, по которым проходит маршрут следования информации в сетях связи
Шлюзы	Маршрутизатор или какое-либо программное обеспечение, которое позволяет двум и более независимым сетям с разными протоколами обмениваться между собой данными (дает возможность узлу из локальной сети выйти в глобальную паутину)
Коммуникационное оборудование	Специальное техническое устройство, через которое осуществляется передача данных для определенных или общих пользователей (линии связи, коммутаторы, адаптеры)
SSL-соединение (Secure Sockets Layer) или уровень защищенных сокетов)	Протокол шифрования, который позволяет кодировать данные для более безопасного обмена, т.е. обеспечивает зашифрованное соединение между человеком и используемым сайтом
VPN (Virtual Private Network) или виртуальная частная сеть)	Обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети (например Интернет)
Bluetooth или Wireless (Wi-Fi)	Технология беспроводной передачи данных

Этапы аудита информационным каналам, по которым передается информация	
1 этап	Сбор и систематизация списка информационных каналов (сетей, узлов маршрутизации, шлюзов и т.д.), по которым передается информация [8]
2 этап	Проверка использования шифрованного SSL-соединение с применением действующих сертификатов, а также логина и пароля, соответствующего требованиям безопасности, при передаче информации, подлежащей охране. Анализ использования при передаче информации, подлежащей охране, шлюзов, установленных на территории предприятия, но контролируемых провайдером, предоставляющим услуги связи в нешифрованном виде [8]
3 этап	Проверка допустимости использования эфирных (не кабельных) каналов связи, таких как Bluetooth или Wireless (Wi-Fi). Беспроводная сеть должна быть закрытой, т.е. подключение новых устройств в эту сеть не должно выполняться в автоматическом режиме, даже если новому пользователю известен пароль сети — администратор должен добавлять новые устройства вручную. Использовать публичные беспроводные сети (кафе, ресторанов, гостиниц и т.д.) без организации специализированного канала связи нельзя. Допускаются только внутрикорпоративные беспроводные сети
4 этап	Проверка регулярности обновления программного обеспечения шлюзов/маршрутизаторов; обновления списков вредоносных сайтов; соответствия паролей административных учетных записей, используемых для управления шлюзами/маршрутизаторами, критериям безопасности

Рис. 3. Этапы аудита информационных каналов, по которым передается информация

Часть IV Гражданского Кодекса Российской Федерации вводит два основных вида договоров по распоряжению исключительным правом [9]:

- договор об отчуждении исключительного права;
- договор о предоставлении другому лицу права использования соответствующего результата интеллектуальной деятельности в установленных договором пределах (лицензионный договор). При этом заключение лицензионного договора не влечет за собой переход исключительного права к лицензиату (п. 1. ст. 1233 ГК РФ).

Аппаратное и программное обеспечение разнообразно и в зависимости от сущности правоотношений возможны несколько вариантов их документальной фиксации, так оформляются следующие договора:

- договор на продажу готового программного обеспечения (при покупке созданной ранее программы у автора);
- договор поставки программного обеспечения (при необходимости доставки до места установки готовой лицензионной программы);
- договор на создание сайта (при разработке интерфейса, контента, функционала интернет-площадки для продвижения продукта компании);
- договор технической поддержки программного обеспечения (при устранении поломки и проведении профилактических работ специалистом для нормального функционирования программного обеспечения);
- договор на разработку мобильного приложения (при разработке приложения для продажи через мобильные устройства).

Согласно российскому законодательству лицензионный договор является правоустанавливающим документом, достаточным для подтверждения правомерности использования программы для ЭВМ. Однако, зачастую требуется наличие документов, подтверждающих передачу прав на программы для ЭВМ (акта приема-передачи) и оплату (счет, счет-фактура на приобретенные программы для ЭВМ) (табл. 5).

Приобретение программного обеспечения в коробке (в том числе дисков) сопровождается, как правило, либо договором купли-продажи, либо договором поставки. В таком случае условия лицензионного договора содержатся либо на диске, либо на упаковке программы для ЭВМ. Дополнительными доку-

Этапы аудита программного обеспечения, используемого для обработки информации	
1 этап	Сбор и систематизация списка программного обеспечения, используемого для обработки информации. Выяснение того, какого рода информация фиксируется и обрабатывается при помощи программного обеспечения. Выявление нелицензионного программного обеспечения, наличия и использования антивирусных приложений, регулярности и своевременности их обновления. Выявление используемого программного обеспечения шлюзов, регулярности и своевременности обновления базы данных вредоносных сайтов, которые подлежат блокировке
2 этап	Проверка информации о регулярности обнаружения уязвимостей в операционных системах, системах управления базами данных, системах файловых хранилищ и т.д. Проверка возможности использования специальных программных комплексов для обнаружения «дыр» и «черных ходов» в аппаратном и программном обеспечении: тестирование средства защиты с выводом обнаруженных уязвимостей [8]
3 этап	Контроль соответствия паролей пользователей и администраторов требованиям безопасности в случае входа в программный продукт по паролю, а также проверка их осмысленности
4 этап	Проверка отдельного программного обеспечения на соответствие внутренней архитектуре продуктов организации согласно международным стандартам
5 этап	Проверка возможности в компании моделирования искусственно созданных критических ситуаций, а также ситуаций прорыва информационной безопасности, имитационного моделирования с помощью средств Excel и VBA вероятностных ошибок и нарушений в работе определенного программного обеспечения
6 этап	Проверка возможности периодической установки максимально возможной нагрузки на системы, отвечающие за информационную безопасность и возможности удаленного управления информационной безопасностью
7 этап	Проверка возможности использования специализированного программного обеспечения, фиксирующего все действия пользователя при обработке информации на информационном ресурсе. К числу такого программного обеспечения относится StaffCop Enterprise, позволяющий фиксировать абсолютно все действия пользователя на информационном ресурсе, связанные с получением и обработкой информации. Действия пользователя могут быть представлены в виде журнала событий, который потом может быть проанализирован администраторами или аудиторами

Рис. 4. Этапы аудита программного обеспечения, используемого для обработки информации

ментами для подтверждения приобретения экземпляров программ для ЭВМ являются счет-фактура и товарная накладная.

Правоустанавливающими документами, подтверждающими правомерность использования предустановленных программ, являются: договор купли-продажи (договор поставки), счет-фактура и накладная, где отдельной строкой должно быть выделено предустановленное программное обеспечение, сертификат подлинности, который наклеивается на корпус системы.

Техническая документация является составляющей проекта по созданию, внедрению, сопровождению, модернизации и ликвидации информационной системы на всем протяжении жизненного цикла.

Основным назначением технической документации является обеспечение эффективных процедур разработки и использования информационной системы как программного продукта, а также организация обмена между разработчиками и пользователями информационных систем.

Можно выделить следующие функции технической документации [11]:

- дает описание возможностей системы;
- обеспечивает фиксацию принятых и реализованных проектных решений;

Таблица 5

Основная юридическая документация по аппаратному и программному обеспечению

Наименование документа	Описание документа
Лицензионный договор	Соглашение, в силу которого одна сторона — правообладатель исключительного права на ПО (Лицензиар) предоставляет или обязуется предоставить другой стороне (Лицензиату) право использования ПО в предусмотренном договором пределах (статьи 1235, 1286 ГК РФ)
Акт приема-передачи (программного обеспечения)	Документ, подтверждающий факт передачи прав использования программ для ЭВМ от правообладателя к пользователю. Акт приема-передачи может быть приложением к лицензионному договору. Существуют случаи, когда в самом лицензионном договоре фиксируется дата передачи прав использования программ для ЭВМ, при таких условиях акт приема-передачи не составляется
Счет-фактура (на приобретенное программное обеспечение)	Документ, который служит для покупателя основанием принять к вычету НДС, предъявленный продавцом товаров (работ, услуг), имущественных прав (п. 1 ст. 169 НК РФ) [10]. Счет-фактура выставляется при реализации товаров (работ, услуг), передаче имущественных прав, а также при получении предоплаты в счет поставки
Товарная накладная	Документ, применяемый для оформления перехода права собственности (путем продажи, отпуска) на товар или другие материальные ценности от продавца к покупателю

- определяет условия функционирования информационных систем;
- предоставляет информацию об эксплуатации и обслуживании информационных систем;
- регламентирует процедуру защиты информации, регулирует права различных групп пользователей;
- определяет возможности модернизации системы.

Раскроем характеристику документов, относящихся к основной технической документации по аппаратному и программному обеспечению (табл. 6).

Приведем этапы аудита юридической и технической документации по аппаратному и программному обеспечению (рис. 5).

Аудит средств физической защиты информации

Физические средства защиты информации — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, сооружения и организационные меры, предназначенные для создания препятствий для злоумышленников. К ним относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Все физические средства защиты объектов можно разделить на три категории:

- средства предупреждения (забор вокруг объектов компании, усиленные двери, стены, потолки, решетки на окнах зданий и т.д.);
- средства обнаружения (охранная сигнализация и охранное телевидение);
- системы ликвидации угроз (средства пожаротушения и т.д.).

К системам контроля доступа относятся:

- системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце;
- системы опознавания по отпечаткам пальцев;
- системы опознавания по голосу;
- системы опознавания по почерку;
- система опознавания по геометрии рук.

Этапы аудита средств физической защиты информации представлены нами на рис. 6.

Для полноценной и своевременной защиты информации нужно регулярно проводить в качестве превентивной меры аудит информационной безопасности в целях постоянного мониторинга и непрерывного совершенствования

Таблица 6

Основная техническая документация по аппаратному и программному обеспечению

Наименование документа	Описание документа
Технический паспорт	Документ установленной формы, содержащий сведения о совокупности программных и технических средств, используемых для обеспечения деятельности компании
Техническое задание	Документ, содержащий сведения об описании системы, объема работ, границ проекта, порядка разработки, оценки и приемки.
Технический проект	Совокупность документов, описывающих и обосновывающих все подходы, методы, архитектурные и технические решения, применяемые для создания системы. Например, в технический проект включают макеты интерфейсов, описание протоколов для интеграции со смежными системами и оборудованием, пользовательские сценарии, описание алгоритма и их формирование, структура серверов и баз данных, а также другие требования к системе и ее взаимодействию с другими внешними системами.
Техническое руководство или техническая литература	Набор документов, используемых при проектировании (конструировании), изготовлении и использовании объектов техники: зданий, сооружений, промышленных изделий, включая программное и аппаратное обеспечение. В составе технической документации выделяют: конструкторские документы, включая чертежи, спецификации, пояснительные записки, технические отчеты, технические условия, эксплуатационные и ремонтные документы (регламенты, руководства и т.п.) и др.

Этапы аудита юридической и технической документации по аппаратному и программному обеспечению

1 этап	Сбор и систематизация списка юридической и технической документации по аппаратному и программному обеспечению. Сопоставление наличия полного комплекта документации по всему используемому программному и аппаратному обеспечению с учетом того, что версия документации должна соответствовать версии используемого программного обеспечения
2 этап	Проверка соответствия каждого события обработки или передачи информации в схеме обработки регламенту, описывающему действия пользователя или процесс обработки информации программным обеспечением [8]
3 этап	Проверка возможности ведения документации с учетом ее регулярного обновления следом за изменением алгоритмов обработки информации в компании

Рис. 5. Этапы аудита юридической и технической документации по аппаратному и программному обеспечению

методов и средств защиты информации. Именно аудит является эффективным инструментом получения независимой и объективной оценки защищенности информации компании от внешних и внутренних угроз информационной безопасности. Первоочередными и наиболее важными мероприятиями по сохранности информации могут быть: запрет на распространение государственной и коммерческой тайн и конфиденциальной информации, прописанный в корпоративных актах компании и ознакомление с ними персонала; запрет на использование личных адресов электронной почты и личных компьютеров; запрет на выкладку документов в облачные хранилища; кодировка, установка сложных паролей при

Этапы аудита средств физической защиты информации	
1 этап	Проверка совместно со службой физической защиты и охраны предприятия, а также инженерной службой здания того, кто имеет доступ в помещения, где установлено оборудование обработки и хранения информации и оборудование каналов связи, а также, где хранится документация и не имеют ли туда доступ неавторизованные лица. Список сотрудников, имеющих доступ в эти помещения, должен быть строго ограничен
2 этап	Проверка возможности функционирования в полном объеме при отключении питания системы СКУД и системы видеонаблюдения. Если при отключении питания эти системы прекращают функционирование — возможна физическая утечка информации (хищение физических носителей при отключении электропитания) [8]
3 этап	Проверка помещения, где установлено оборудование обработки и хранения информации и оборудование каналов связи, а также где хранится документация, с целью оценки оснащения ее системой автоматического пожаротушения, не использующей токопроводящие жидкости
4 этап	Проверка помещения, где установлено оборудование обработки и хранения информации и оборудование каналов связи, с целью оценки оснащения ее системой резервного питания, автоматически включающейся при отключении основного источника питания
5 этап	Проверка помещения, где установлено оборудование обработки и хранения информации и оборудование каналов связи, с целью оценки оснащения ее системой поддержания постоянной температуры (системой охлаждения воздуха)
6 этап	Проверка осуществления контроля физического доступа в помещения в рабочее и нерабочее время, визуального контроля перемещения сотрудников в помещении, системы отчетности и оповещений о доступе и перемещении в офисе компании, а при их отсутствии — возможности внедрения таких направлений проверки

Рис. 6. Этапы аудита средств физической защиты информации

передаче электронных документов и электронных копий бумажных носителей, организация обработки и хранения документов, информационных ресурсов и источников.

Литература

1. Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
4. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
5. Конфиденциальная информация и способы ее защиты [Электронный ресурс]. — URL: https://www.business.ru/article/2034-konfidentsialnaya-informatsiya-vidy (дата обращения: 20.10.2021).
6. Регламент ФНС России № САЭ-3-13848@ «Об обмене электронными документами».
7. Коммерческая тайна предприятия — что это, отличие от конфиденциальной информации — Дело [Электронный ресурс]. URL: https://okarb.ru/oplata-truda/kommercheskaya-tajna-predpriyatiya-chto-eto-otlichie-ot-konfidentsialnoj-informatsii.html (дата обращения: 20.10.2021).
8. Как правильно проводить аудит внутренней информационной безопасности? [Электронный ресурс]. — URL: https://www.staffcop.ru/blog/pravila-audita-vnutrennej-informatsionnoj-bezopasnosti (дата обращения: 20.10.2021).
9. Гражданский кодекс РФ от 26 января 1996 г. № 14-ФЗ.
10. Налоговый кодекс РФ от 31 июля 1998 г. № 146-ФЗ.
11. *Шикина В.Е.* Техническая документация информационных систем: учебное пособие. — Ульяновск : УлГТУ, 2018. — 92 с.