Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Под общей редакцией профессора И. Б. Тесленко

Владимир 2023

УДК 004.056
ББК 16.8
И74

Авторы-составители:
И. Б. Тесленко, Д. В. Виноградов, А. М. Губернаторов, В. Е. Крылов, И. Ю. Куликова, Н. В. Муравьева, Н. О. Субботина, Е. А. Уланов

Рецензенты:

Кандидат экономических наук, доцент
зав. кафедрой экономики и финансов Финансового университета при Правительстве Российской Федерации (Финуниверситет) (Владимирский филиал)
Д. В. Кузнецов

Генеральный директор СП ООО «ТехноСтройИнвест»
В. А. Вашурин

Издается по решению редакционно-издательского совета ВлГУ

Информационная безопасность : учеб. пособие / авт.-сост. И. Б. Тесленко [и др.] / под общ. ред. проф. И. Б. Тесленко ; Владим. гос. ун-т им. А. Г и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2023. – 212 с. – ISBN 978-5-9984-1783-2.

И74

Излагаются цели и задачи, подходы и методы, охватывающие основные теоретические и прикладные аспекты информационной безопасности в бизнесе, а также вопросы, связанные с освоением программных средств, используемых для преодоления внешних и внутренних угроз.

Предназначено для студентов бакалавриата и магистратуры всех форм обучения направления подготовки 38.03.05, 38.04.05 «Бизнес-информатика» и других экономических направлений, аспирантов, руководителей компаний и специалистов, занимающихся вопросами внедрения и эксплуатации информационных систем в бизнесе.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Ил. 9. Табл. 9. Библиогр.: 8 назв.

УДК 004.056
ББК 16.8

ISBN 978-5-9984-1783-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Несомненно, что информация имеет значительную ценность. Люди осознали это очень давно – недаром переписка «сильных мира сего» издавна была объектом пристального внимания не только их друзей, но и недругов. Тогда и возникла задача защиты этой переписки от чрезмерно любопытных глаз. Древние люди пытались использовать для решения этой задачи самые разнообразные способы; одним из них была тайнопись – умение составлять сообщения таким образом, чтобы его смысл был недоступен никому, кроме посвященных в тайну. Есть свидетельства, что искусство тайнописи зародилось еще в доантичные времена. На протяжении всей своей многовековой истории, вплоть до совсем недавнего времени, это искусство служило немногим, в основном верхушке общества, не выходя за пределы резиденций глав государств, посольств и, конечно же, разведывательных миссий. И лишь несколько десятилетий назад все изменилось коренным образом – информация приобрела самостоятельную коммерческую ценность и стала широко распространенным, почти обычным товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит, воруют и подделывают, следовательно, ее необходимо защищать.

Современное общество все в большей степени становится информационно обусловленным, успех любого вида деятельности все сильнее зависит от обладания определенными сведениями и отсутствия их у конкурентов. И чем активнее проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере и значительнее потребность в защите информации. Одним словом, появление индустрии обработки информации привело к возникновению индустрии средств ее защиты.

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В отличие от других методов они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения. Образно говоря, криптографические методы строят барьер между защищаемой информацией и реальным или потенциальным злоумышленником при его несанкционированном доступе к информации или ее присвоении. Конечно, под

криптографической защитой в первую очередь – так уж сложилось исторически – подразумевается шифрование данных. Раньше, когда эта операция выполнялась человеком вручную или с использованием различных приспособлений, а при посольствах содержались специальные отделы шифровальщиков, развитие криптографии сдерживалось проблемой реализации шифров, ведь придумать можно было все, что угодно, но реализовать сложно.

За последние годы компьютерный мир претерпел радикальные изменения. На заре компьютерной эры большинство компьютеров находилось в ведении вычислительных центров. Они содержались в запертых помещениях, а обслуживающий персонал отвечал за тщательность администрирования и физическую безопасность. Связи с внешним миром были явлением редким. Редко возникали и угрозы информационной безопасности, исходившие в подавляющем большинстве случаев от штатных сотрудников. Угрозы состояли в неправильном использовании полномочий со стороны авторизованных пользователей, в подделке электронных документов, вандализме и т. п. Для предотвращения подобных угроз было вполне достаточно стандартных мер: замков на дверях и учета использования всех ресурсов.

Изменились угрозы безопасности. С общемировыми связями через Интернет злоумышленник, находящийся на противоположной стороне Земли, может среди ночи проникнуть в вашу систему и выкрасть данные, несмотря на то, что здание вашей организации закрыто на все замки. Вирусы и черви могут передаваться от машины к машине. По Интернету могут «разгуливать электронные воры». Теперь злоумышленник может за несколько часов проверить наличие слабых мест в защите сотен компьютеров.

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин. Прежде всего – это расширение сферы применения средств вычислительной техники и возросший уровень доверия к автоматизированным системам управления и обработки информации.

Проблема защиты вычислительных систем становится еще более серьезной и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам. Доступность средств вычислительной техники и прежде всего персональных ЭВМ привела

к распространению компьютерной грамотности в широких слоях населения, что закономерно привело к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих автоматизированных систем как со злым умыслом, так и чисто из «спортивного интереса». К сожалению, многие из этих попыток имеют успех и наносят значительный урон всем заинтересованным субъектам информационных отношений.

Еще одним весомым аргументом в пользу усиления внимания к вопросам безопасности вычислительных систем являются бурное развитие и распространение так называемых компьютерных вирусов, способных скрытно существовать в системе и совершать потенциально любые несанкционированные действия. Особую опасность для компьютерных систем представляют злоумышленники, специалисты-профессионалы в области вычислительной техники и программирования, досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией и самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты.

На решение указанных выше проблем и направлено данное учебное пособие. Оно ориентировано прежде всего на подготовку студентов по дисциплине «Информационная безопасность», но может эффективно использоваться при изучении таких дисциплин, как «Основы консалтинговой деятельности», «Информационная инфраструктура предприятия», «Информационные системы управления производственной компанией» и быть полезным для магистрантов направления 38.04.05 – Бизнес-информатика.

Учебное пособие имеет цель сформировать у студентов определенную систему знаний в области:

– борьбы с угрозами несанкционированного доступа к информации;
– защиты информации в персональном компьютере;
– криптографических методов защиты информации;
– борьбы с вирусным заражением информации;
– правового обеспечения информационной безопасности.

При написании книги авторский коллектив руководствовался важнейшими методологическими и методическими положениями.

Дополнительный материал, содержащийся в издании, может быть использован студентами для углубления знаний при подготовке докладов, рефератов, контрольных работ, а также магистрантами, аспирантами и преподавателями.

Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятие информации и ее виды

Термин «информация» происходит от латинского слова «informatio» (сведения, разъяснения, изложение).

Этот термин вошел в употребление в русскую речь в середине XX века.

Впервые слову «информация», помимо обычного, первоначального значения (сведения, сообщения), Рональдом Фишером, английским математиком и биологом, в ходе разработки методов математической статистики был придан немного иной смысл, а именно – статистические данные (1921г.). Американский ученый-электрик Ральф Хартли ввел понятие информации как математической переменной и был первым, кто в 1928 году попытался определить «меру» информации. Он развивал понятие информации для изучения электрических коммуникаций и рассматривал информацию как средство коммуникации между передатчиком и приемником информации по электрическим проводам. В конце 40-х годов XX века работы Р. Хартли послужили началом разработки теории информации[1].

В большей степени понятие «информация» связано с такими научными направлениями, как теория связи (основатель Клод Шеннон) и кибернетика (основатель Норберт Винер). Но ни К. Шеннон, ни Н. Винер не давали четкого определения информации, хотя принято считать, что именно Н. Винер ввел это понятие в научное употребление[2].

В. Шнейдеров отмечает, что известно более 400 определений термина «информация», которые используются в различных сферах знаний[3].

В обыденной жизни информацию понимают, как сведения, данные, сообщения, сигналы, знания. Ими обмениваются между собой

---

[1] Эволюция понятия «информация». URL: https://www.sites.google.com/site/kollenderinformation/home/stati-ob-informacii/-evolucia-ponatia-informacia (дата обращения: 12.11.2022).

[2] История понятия «информация». URL: https://иванов-ам.рф/informatika_kabinet/inf_prozes/inf_prozes_01.html?ysclid=l9nu2m9oe9249867300 (дата обращения: 12.11.2022).

[3] Полнота информации – это что означает? Читайте подробнее на FB.ru: URL: https://fb.ru/article/272863/polnota-informatsii---eto-chto-oznachaet?ysclid=l9nuvj9gap137777829 (дата обращения: 12.11.2022).

субъекты, субъекты и объекты; представители животного и растительного мира; передаются признаки от организма к организму и внутри организма.

В официальных документах страны к информации относят сведения независимо от формы их представления (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»[4]).

В научной литературе нет единого подхода к пониманию термина «информация». Философы рассматривают информацию как некую фундаментальную субстанцию, как форму «отражения» процессов окружающего нас мира. В естественных науках к информации относят уже известные знания об объектах и процессах в мире.

В связи с развитием информационно-коммуникационных технологий (ИКТ) подходы к определению понятия информации еще больше расширяются. Основоположник кибернетики Н. Винер так определяет информацию: это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств[5].

Информация может существовать в виде текстов, рисунков, схем, фотографий, световых или звуковых сигналов, радиоволн, электрических и нервных импульсов, магнитных записей, жестов и мимики, запахов и вкусовых ощущений, хромосом и т. д.

Часто в литературе понятия «информация», «данные», «знания» отождествляются. Однако между ними есть различия.

Данные – это факты и идеи, представленные в форме, пригодной для передачи и обработки. Данные несут в себе сведения о каких-то событиях, регистрируют сигналы, характеризующие эти события. Но не всегда они превращаются в информацию.

Например, слыша разговор на иностранном языке, люди получают данные в виде звуков, а вот информации они не получают, так как не понимают передаваемые данные из-за отсутствия знания необходимого кода.

---

[4] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 12.11.2022).

[5] Информация и информатика. URL: techn. sstu.ru/kafedri/подразделения/1/MetMat/shaturn/inform/Лекция%201%5CЛекция%201.htm (дата обращения: 12.11.2022).

Знание – это переработанная и проанализированная человеческим мозгом информация, обобщенная в виде законов, теорий, совокупностей взглядов и понятий; это осознание, понимание и толкование информации с учетом имеющегося опыта для наилучшего ее использования при достижении конкретных целей.

Знания бывают:

– научные (логически обоснованы, доказательны, их результаты воспроизводимы, проверяемы);

– обыденные (основа повседневного поведения человека и предвидения, они могут быть ошибочными и противоречивыми);

– интуитивные;

– религиозные и др.

Итак, при использовании данных в процессе решения конкретных задач может появиться информация.

Информация как объект познания имеет ряд особенностей:

– она нематериальна, отображается в виде символов на носителях;

– на материальном носителе информацию можно хранить, обрабатывать, передавать;

– любой материальный объект может содержать информацию о самом себе или других объектах.

Поскольку информация весьма разнообразна, ее можно классифицировать по ряду критериев (табл. 1.1).

Таблица 1.1. Критерии классификации информации

Критерий	Вид информации
По способам восприятия	Визуальная, аудиальная, тактильная, обонятельная, вкусовая
По форме представления	Буквенная, цифровая, графическая, кодированная, комбинированная
По форме передачи	Вербальная (словесная, звуковая), невербальная (представленная на определенном носителе: бумаге, диске и т. д.), письменная, печатная, телефонная, электронная, спутниковая и т. д.
По назначению	Экономическая, техническая, социальная, организационная и т. д.
По общественному значению: – массовая	Обыденная, общественно-политическая, эстетическая
– личная	Знания, интуиция
– специальная	Научная, производственная, техническая, управленческая

Окончание табл. 1.1

Критерий	Вид информации
По изменчивости во времени	Условно-постоянная (например, место жительства человека), условно-переменная (например, последовательность календарных месяцев), постоянная (дата рождения человека), переменная
По режиму передачи от одного потребителя информации другому	В произвольные сроки, по запросу, принудительно в определенные сроки

Е. В. Вострецова отмечает, что в литературе выделяют несколько уровней представления информации: уровень носителей; уровень средств взаимодействия с носителем; логический уровень; синтаксический и семантический уровни[6].

1. Уровень носителей. В чистом виде информация человеку недоступна. Он ее воспринимает, если есть материальный носитель: вещество (вещественный носитель), энергия (энергетический носитель), другой человек.

Роль человека по отношению к информации многообразна: человек может быть не только носителем информации, но и генератором новой информации, источником информации, ее владельцем, пользователем. Он может выступать и как нарушитель, и как защитник. Поскольку информация крайне важна при принятии решений, то очень важна достаточная информированность человека[7].

Вещественные носители весьма разнообразны: бумага, электронные носители информации. Они используются для хранения информации, и их следует защищать от повреждения, преждевременного износа, хищения, утери и при копировании.

2. Уровень средств взаимодействия с носителем. Непосредственное взаимодействие с носителем не всегда возможно и часто осуществляется через сложные технические устройства. Для защиты на этом

---

[6] Вострецова Е. В. Основы информационной безопасности : учеб. пособие для студентов вузов. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с. URL: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf https://elar.urfu.ru (дата обращения: 12.11.2022).

[7] Вострецова Е. В. Указ. соч.

уровне нужно следить за исправностью устройств считывания информации и отсутствием технических средств несанкционированного доступа к информации[8].

3. Логический уровень. Здесь информация может быть представлена в виде дисков, каталогов, файлов, кластеров. Удаление информации на высоком логическом уровне (например, на уровне файла) не приводит к удалению информации на нижних уровнях, откуда она может быть считана.

4. Синтаксический уровень[9]. Представление информации на этом уровне связано с кодированием. Информация записывается и передается при помощи символов (знаков, имеющих определенный смысл). Линейный набор символов образует алфавит. В процессе кодирования один алфавит может быть преобразован в другой. В зависимости от целей[10] кодирования различают архивирование, линейное, помехоустойчивое, криптографическое кодирование.

5. Семантический уровень. Он связан со смыслом передаваемой информации. Одинаковые лексические конструкции могут иметь различный смысл в разном контексте. Использование профессионализмов, многозначных слов и слов, значение которых изменилось с течением времени, может исказить смысл информации[11].

Уточняя понимание термина «информация», В. В. Сухостат называет два вида информации, которые рассматриваются в современной науке:

– объективная (первичная) информация – свойство материальных объектов и явлений (процессов) порождать многообразие состояний, которые посредством взаимодействий передаются другим объектам и запечатлеваются в их структуре;

– субъективная (семантическая, смысловая, вторичная) информация – смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием человека с помощью смысловых образов (слов, ощущений) и зафиксированное на каком-либо материальном носителе.

---

[8] Вострецова Е. В. Указ. соч.

[9] Там же.

[10] Там же.

[11] Там же.

Объективная информация – это данные, сообщения, а субъективная – это сведения. Сведения отличаются от данных и сообщений тем, что отражают смысловое содержание последних, отраженное человеческим сознанием.

По принадлежности к виду собственности информационные ресурсы могут быть государственными или негосударственными, находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных организаций[12].

Наличие права собственности на информацию как результат интеллектуальной деятельности определяет законодательную основу защиты информационных ресурсов. Ценная информация охраняется нормами права (патентного, авторского, смежных прав и др.), товарным знаком или защищается включением ее в категорию информации, составляющей определенный вид тайны[13].

Информация может быть конфиденциальной, секретной, ограниченного доступа.

Конфиденциальная информация (от лат. confidentia – доверие) характеризуется тем, что доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Секретная информация – информация, не подлежащая разглашению, либо на распространение которой наложены ограничения вследствие возможного причинения вреда лицам, заинтересованным в ее нераспространении.

Информация ограниченного доступа – информация, доступ к которой ограничен в интересах обеспечения национальной безопасности в соответствии с законодательством о государственных секретах и иными нормативно-правовыми актами, регулирующими отношения в области защиты государственных секретов.

В ст. 9 Федерального закона РФ «Об информации, информационных технологиях и о защите информации» выделяют следующие виды информации ограниченного доступа:

---

[12] Вострецова Е. В. Указ. соч.

[13] Исследование эффективных методов защиты электронного документооборота научно-производственного объединения. URL: http://elibrary.ru (дата обращения: 12.11.2022).

– государственная тайна;
– коммерческая тайна;
– информация о частной жизни лица;
– профессиональная тайна;
– служебная тайна и иная тайна.

Виды тайн и их содержание представлены в табл. 1.2.

Таблица 1.2. Виды тайн

Вид тайны	Содержание
Государственная	Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации[14]
Коммерческая	Информация, которую компания не разглашает, чтобы увеличить доходы, избежать неоправданных расходов, сохранить или улучшить свое положение на рынке либо получить любую другую коммерческую выгоду
Профессиональная	Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности, подлежащая защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации
Служебная	Информация о деятельности государственных органов власти и органов местного самоуправления, доступ к которой ограничен нормативно-правовыми актами государства, а также сведения, которые поступают в вышеупомянутые органы на законном основании для исполнения служебных обязанностей
Личная	Информация о частной жизни, семейная тайна, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

[14] Закон РФ от 21.07.1993 № 5485-1 (ред. от 14.07.2022) «О государственной тайне». URL: https://www.consultant.ru/document/cons_doc_LAW_2481/b276619673d4311ef4fce8f08192952409f7b208/ (дата обращения: 12.11.2022).

Нарушение конфиденциальности, разглашение секретной информации называется хищением, утечкой либо раскрытием информации.

Накопленная информация об окружающей действительности, зафиксированная на материальных носителях, обеспечивающих передачу информации во времени и пространстве между потребителями для решения конкретных задач, образует информационные ресурсы. Это отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)[15].

Информационные ресурсы подразделяются на классы. Информация о количественных и качественных характеристиках разных социальных процессов образует класс **«снимаемой информации».** Сюда относят естественные, производственные, социально-экономические информационные ресурсы.

Другой класс информационного ресурса образуют **сведения, получаемые искусственно в процессе научно-исследовательской интеллектуальной деятельности,** когда уже имеющаяся информация специальным образом обрабатывается (математическая обработка, логическая, семантическая и т. д.). В результате появляются **вторичная информация**, возникающая на основе переработки уже имеющейся информации, и **новая информация**, которую человечество еще не знало[16] (открытия, прогнозы социальных и природных процессов и др.).

26 ноября во многих странах мира отмечают Всемирный день информации, который проводится ежегодно с 1994 года. И это неслучайно. Дело в том, что человечество ежегодно производит количество информации, равное 500 тыс. Библиотек Конгресса США. При этом 92 % общемировой информации содержится в электронном виде. А чтобы прочитать весь англоязычный интернет-контент понадобится 226532 года при скорости чтения 250 слов в минуту[17].

---

[15] Информационные ресурсы. URL: https://discovered.com.ua/business/informacionnye-resursy/ (дата обращения: 12.11.2022).

[16] Там же.

[17] Всемирный день информации. URL: https://relax.com.ua/holidays/information-day/ (дата обращения: 12.11.2022).

1.2. Свойства информации и структура информационного процесса

Как всякий объект, информация обладают определенными свойствами. К ним относят:

1. Атрибутивные свойства – самые главные свойства, формирующие информацию (передаваемость, воспроизводимость, преобразуемость, копируемость).

2. Прагматические свойства демонстрируют степень полезности информации непосредственно для пользователя и для практики (адекватность, актуальность, доступность, достоверность, защищенность, объективность и субъективность, полезность, полнота, релевантность, смысл и новизна, точность, ценность, эргономичность).

3. Динамические свойства – свойства, которые характеризуют изменение информации во времени (кумулятивность, рост информации, старение, стираемость, запоминаемость).

При этом различают внутренние и внешние свойства.

Внутренние – это свойства, органически присущие объекту. Они обычно «скрыты» от изучающего объект и проявляют себя косвенным образом при взаимодействии данного объекта с другими.

Внешние – это свойства, характеризующие поведение объекта при взаимодействии с другими объектами[18].

Остановимся на характеристике некоторых свойств информации. Такое свойство, как ценность информации, определяется степенью ее полезности для обладателя. Если информация искажена умышленно, то ее называют дезинформацией[19].

Ценность информации изменяется во времени, поскольку информация стареет. Как любое явление информация имеет свой жизненный цикл: получение данных, хранение, выборка, обработка, подготовка к хранению, использование, оценка, уничтожение, отчетные данные (рис. 1.1).

---

[18] Виды и свойства информации URL: https://helpiks.org (дата обращения: 12.11.2022).

[19] Сухостат В. В., Васильева И. Н. Основы информационной безопасности : учеб. пособие. СПб. : Изд-во СПбГЭУ, 2019. 103 с. URL: https://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informaczionnoj-bezop https://infosec.spb.ru (дата обращения: 12.11.2022).

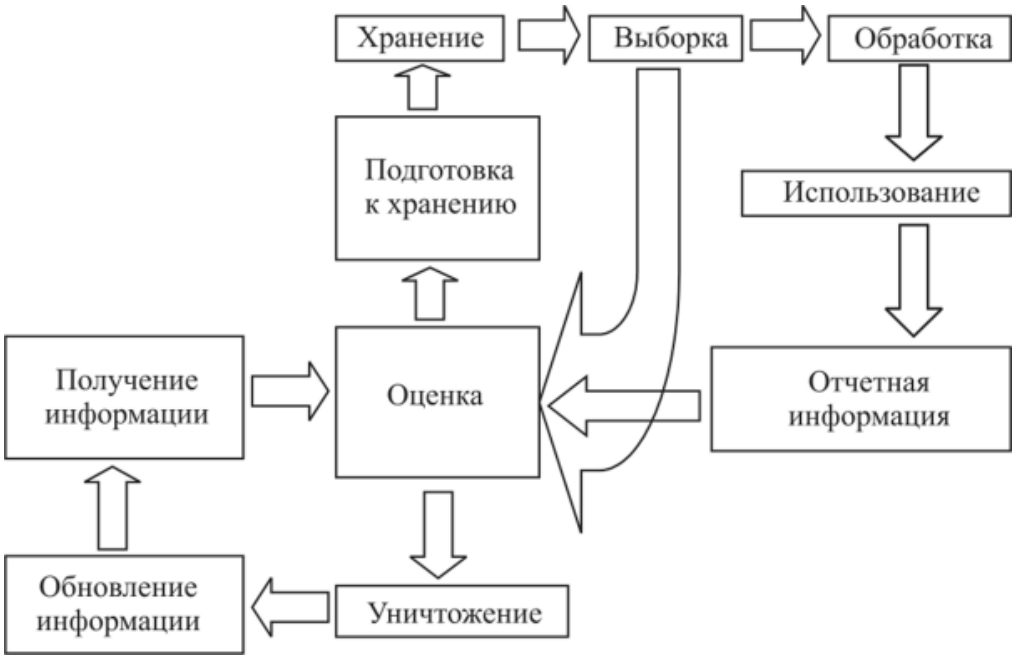

Рис. 1.1. Жизненный цикл информации

Степень ценности информации и необходимая надежность ее защиты находятся в прямой зависимости. Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например учредительные документы, программы и планы, договоры с партнерами и посредниками и т. д.

Ценность может проявляться в ее перспективном научном, техническом или технологическом значении[20]. Не всегда она имеет текстовую форму. Большие объемы наиболее ценных документов могут быть представлены в виде схем, рисунков, конструкторских, картографических, научно-технических документов, документов на фотографических, магнитных и иных носителях и др.

В соответствии с этим обычно выделяют два вида интеллектуально ценной информации:

– техническая, технологическая (методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, рецептуры, результаты испытаний опытных образцов, данные контроля качества и т. п.[21]);

---

[20] Вострецова Е. В. Указ. соч.

[21] Исследование эффективных методов защиты электронного документооборота научно-производственного объединения. URL: http://elibrary.ru (дата обращения: 12.11.2022).

– деловая (стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы и т. п.)[22].

При нарушении хотя бы одного из свойств информации ее ценность снижается либо теряется вообще.

Такое свойство, как релевантность информации, представляет собой степень соответствия конкретной документации или целого списка документов, которые будут отвечать целям, нуждам, ожиданиям и запросам пользователя. Если человек получает сведения, которые не относятся к запросу, значит информация нерелевантна.

Полнота информации – это свойство информации характеризовать отображаемый объект, явление или процесс. Оно указывает на меру достаточности полученных данных для решения той или иной задачи. Это свойство весьма относительно, так как оценивается по тому, насколько данная информация может помочь при решении той или иной проблемы. Если информации достаточно для принятия правильного решения – она полная. Если нет, то ее использование не принесет ожидаемого эффекта. Чем полнее полученные данные, тем больше методов доступно человеку для решения проблемы, тем быстрее он сможет подобрать правильный метод и решить свою проблему. Неполная информация может привести к ошибочным решениям и выводам[23].

Эргономичность информации представляет удобство формы или объема информации с точки зрения конкретного потребителя. Если, например, говорить о создании сайтов, то эргономика предъявляет определенные требования к взаимодействию человека и машины в Интернете. Речь идет об объеме представляемых сведений, темпе предъявления, очередности, расположении знаков, символов и принципах их построения, т. е. о веб-инженерии (построение так называемой информационной модели).

Информационная модель формируется такими средствами, как изобразительный и звуковой ряды на экране и пространственно-временная структура строения сайта. Установленные языки разметки,

---

[22] Исследование эффективных методов защиты электронного документооборота научно-производственного объединения. URL: http://elibrary.ru (дата обращения: 12.11.2022).

[23] Полнота информации – это что означает? URL: http://fb.ru (дата обращения: 12.11.2022).

форматы, контенты сети Интернет, как правило, не ухудшают эргономических характеристик сайтов, если их грамотно придерживаться[24].

Адекватность представляет собой свойство информации однозначно соответствовать отображаемому объекту или явлению. Адекватность оказывается для потребителя внутренним свойством информации, проявляющим себя через релевантность и достоверность.

Целостность информации – это гарантия того, что при хранении или передаче информации не было произведено ее несанкционированного изменения или удаления[25]. Несанкционированное нарушение целостности информации называется фальсификацией.

Доступность информации – это гарантия получения своевременного доступа к запрашиваемому ресурсу. Если информация недоступна постоянно, это равносильно ее утрате.

Кумулятивность информации – это свойство содержательной информации, заключенной в массиве небольшого объема, достаточно полно отображать действительность. Задачу обеспечения кумулятивности информации (накопления и сохранения) можно решать, применяя соответственно формально-технические и социально-психологические приемы.

Источник информации со всеми ее свойствами, канал связи и получатель информации образуют простейшую информационную систему.

Перенос информации в виде сигнала от источника к получателю образует информационный процесс. Он состоит из следующих фаз:

1. Сбор (если реализуется человеком) или восприятие (если реализуется технической системой) представляет отображение источника информации в сигнал, а также хранение информации (способ распространения информации в пространстве и времени).

2. Передача – перенос информации в виде сигнала в пространстве посредством физических сред любой природы. Информация может поступать в информационные системы в аналоговом виде, т. е. в виде некоторой непрерывной функции времени, отображающей изменение

---

[24] Обзор методов эргономического представления информации. URL: https://neonstudio.ruinfo/ergonomika_informacii/?ysclid=l9nv6irjw728419584 (дата обращения: 12.11.2022).

[25] Сухостат В. В., Васильева И. Н. Указ. соч.

информации; в кодовом или цифровом виде, когда информация представляется в форме сочетаний «0» и «1», соответствующих определенным символам.

3. Обработка – любое преобразование информации для решения поставленных задач (определяются потребителем информации).

4. Представление (если потребителем информации является человек) или воздействие (если потребителем выступает техническая система) и использование. Представление предусматривает преобразование информации в нужный для потребителя вид (графики, тексты, диаграммы, таблицы и т. д.). Воздействие предполагает управляющее влияние на технические средства.

Информационный процесс должен завершаться защитой информации (комплексом мер по предотвращению угроз информационной безопасности и их устранению). Фазы информационного процесса представлены на рис. 1.2.

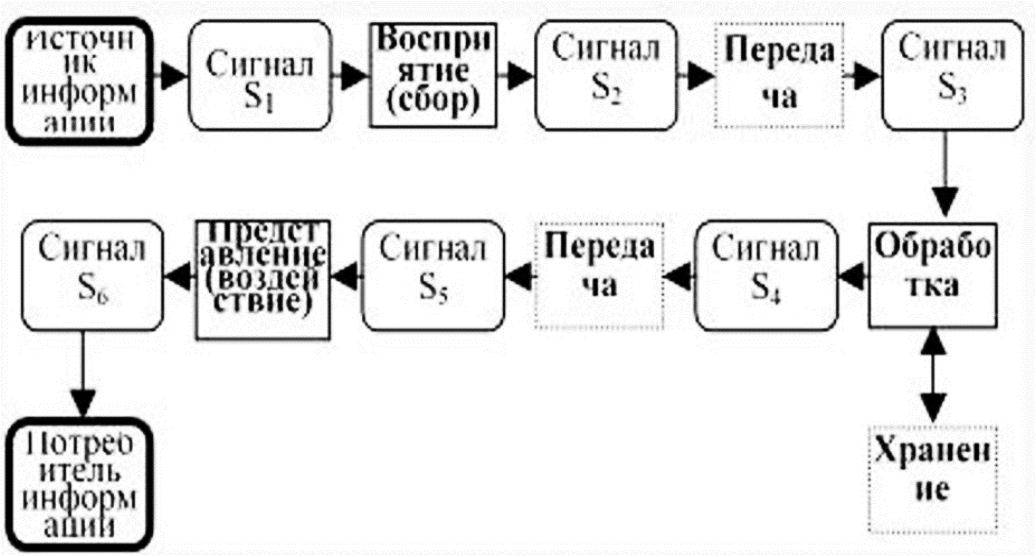

Рис. 1.2. Фазы информационного процесса

В качестве примера реализации информационного процесса можно рассмотреть деятельность геолога. Он изучает местность, берет пробы грунта и передает эти данные в институт геологии. В институте эти данные обрабатывают и делают вывод о наличии полезных ископаемых на данном участке местности. Часто информация является очень важной для субъектов, она не предназначается для других, поэтому ее защита становится крайне актуальной.

1.3. Информационная безопасность и защита информации

Современное общество называется информационным, поскольку его основу составляют новейшие информационные, телекоммуникационные технологии и технологии связи. С увеличением количества информации людям все труднее контролировать ее поток, найти в нем то, что действительно необходимо. В этом незаменимую помощь оказывают ИКТ и, конечно, ресурсы интернета. 30 сентября в России отмечается День интернета (первый домен в зоне ru был зарегистрирован в 1994 году).

Данные об использовании интернета впечатляют. В конце 2021 года существовало более 1,9 миллиарда веб-сайтов. Среднестатистический россиянин проводит в интернете примерно 7 ч 50 мин. На социальные сети в среднем пользователи тратят 2 ч 27 мин в день. По прогнозам, люди в 2022 году провели в Сети более 12,5 трлн ч[26].

Несмотря на положительную роль, прогресс в распространении ИКТ делает уязвимым любое общество. Дело в том, что в последнее время именно на информационном поле начинает разворачиваться противоборство стран. Этим объясняется актуальность изучения проблем защиты информации и информационной безопасности.

В настоящее время в научной литературе сформировалось два направления, изучающих возникновение феномена «информационная безопасность». Одна группа специалистов связывает развитие информационной безопасности с информационными революциями в истории человеческой цивилизации (И. Ю. Хитарова). Данный подход подразумевает, что уровень безопасности общества определен качеством и объемом информации, доступной социуму.

Второй подход, предложенный в свое время В. Н. Лопатиным, предполагает, что в истории человеческой цивилизации появление категории «информационная безопасность» связано с возникновением средств информационных коммуникаций и осознанием человеком возможности нанесения ущерба собственным интересам или интересам социальной системы посредством информационного обмена.

В рамках этого подхода становление информационной безопасности разделяют на несколько этапов.

---

[26] Есть всё: удивительные факты об интернете и сайтах. URL: https://barnaul.press/ (дата обращения: 12.11.2022).

По мнению зарубежных ученых, первый этап начинается с момента зарождения и накопления информации и знаний и длится до 1816 года. Он характеризуется стремлением людей сохранить и защитить значимую информацию и уникальные данные.

Второй этап, начиная с 1816 года до первой трети XX века, характеризуется созданием технических средств защиты информации.

Третий этап начался в 1935 году и длился[27] до середины 50-х годов XX века. Он связан с применением радиолокационных и гидроакустических средств.

На четвертом этапе (с 1946 года до середины 60-х годов XX века) задачи информационной безопасности решаются с помощью электронно-вычислительных машин. С 1965 года, на пятом этапе, осуществлялось создание локальных информационных сетей.

Шестой этап развития информационной безопасности разворачивается с 1973 года и характеризуется применением сверхмобильных коммуникационных устройств.

Седьмой этап начинается с 1985 года. Он связан с развитием глобальных информационных сетей и космических разработок.

Новый этап совершенствования системы информационной безопасности базируется на новейших ИКТ с использованием глобальной сети и космических систем. Он предполагает формирование глобальной системы информационной безопасности, поскольку в современных условиях достижение этой цели может быть обеспечено только усилиями всех стран мирового сообщества[28].

Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Это процесс, направленный на достижение состояния, когда определяется система средств и методов для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации. Понимание важности этой деятельности привело к тому, что 30 ноября был утвержден Международный день защиты информации, который отмечается с 1988 года.

---

[27] Григорьев С. М., Попов О. В. Возникновение и история развития проблемы защиты информации. URL: http://elibrary.ru (дата обращения: 12.11.2022).

[28] Там же.

Наряду с понятием «защита информации» используются такие понятия, как «безопасность информации» и «информационная безопасность». Все они взаимообусловлены и взаимосвязаны. В настоящее время нет единого подхода к определению этих понятий.

Безопасность информации понимается:

– как состояние защищенности информации от внутренних и внешних угроз[29];

– состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации;

– обеспечение защиты информации от случайного или преднамеренного доступа лиц, не имеющих права на ее получение, раскрытие, модификацию или разрушение;

– реализация требований и правил по защите информации, поддержанию информационных систем в защищенном состоянии, эксплуатация специальных средств защиты и обеспечение организационных и инженерно-технических мер защиты[30] информационных систем, обрабатывающих информацию с ограниченным доступом.

Исходя из представленных определений понятий «защита информации» и «безопасность информации» ясно, что защита информации направлена на обеспечение безопасности информации.

Понятие «информационная безопасность» зачастую отождествляют с понятием «безопасность информации». Однако первое понятие относится не к самой информации, а к субъектам информационной среды. Оно более широкое и включает защиту информации и безопасность информации.

В обыденной жизни информационная безопасность представляет собой борьбу с утечкой секретной и распространением ложной и враждебной информации. В научной литературе предлагается большое количество самых разных определений информационной безопасности, отражающих отдельные ее характеристики.

---

[29] Сухостат В. В., Васильева И. Н. Указ. соч.

[30] Организационная защита информации. URL: http://ibooks.ru (дата обращения: 12.11.2022).

Информационная безопасность понимается:

– как комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей;

– совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются;

– показатель, отражающий статус защищенности информационной системы;

– состояние защищенности информационной среды, информационных ресурсов и каналов, а также доступа к источникам информации, прав субъектов информационной деятельности;

– в узком смысле – надежность работы компьютера; сохранность ценных данных;

– невозможность нанесения вреда свойствам объекта безопасности либо его структурным составляющим.

В. Бетелин и В. Галатенко определяют информационную безопасность как защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры[31].

Понятие информационной безопасности как состояния защищенности положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации[32].

Информационная безопасность включает:

– состояние защищенности информационного пространства;

– состояние инфраструктуры, при котором информация используется строго по назначению;

---

[31] Гафнер В. В. Информационная безопасность [Электронный ресурс] : учеб. пособие : в 2 ч. Екатеринбург : Урал. гос. пед. ун-т, 2009. Ч. 1. 155 с. URL: http://elar.uspu.ru/bitstream/uspu/4122/1/ uch00029.pdf (дата обращения: 12.11.2022).

[32] Сухостат В. В., Васильева И. Н. Указ. соч.

– состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность.

Цели информационной безопасности:

– защита национальных интересов;

– обеспечение человека и общества достоверной и полной информацией;

– защита прав субъектов при совершении комплекса действий с информацией.

Обеспечение информационной безопасности – явление сложное, комплексное. В организации информационной безопасности задействованы специальные органы, службы, используются соответствующие средства, методы и проводятся мероприятия, обеспечивающие защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз. Все вместе они образуют систему информационной безопасности.

Объектами информационной безопасности являются:

– информационные ресурсы субъекта;

– документированная информация, представленная в виде информационных массивов и баз данных;

– средства и системы информатизации – средства вычислительной и организационной техники, сети и системы, системы связи и передачи данных;

– общесистемное и прикладное программное обеспечение;

– автоматизированные системы управления;

– технические средства сбора, регистрации, передачи, обработки и отображения информации.

Организация информационной безопасности основывается на определенных принципах. К ним относят принципы:

– баланса интересов личности, бизнеса, общества и государства;

– законности и правовой обеспеченности;

– интеграции с международными системами безопасности информации;

– экономической эффективности (соотношение результатов от проведенных мероприятий по обеспечению информационной безопасности с валовыми затратами на них);

– мобильности системы информационной безопасности (недопущение неоправданных режимных ограничений);

– презумпции несекретности информации (строгому нормированию подлежит конфиденциальность, а не гласность);

– невозможности миновать защитные средства;

– минимизации привилегий (пользователям и администраторам выделяются только те права доступа, которые необходимы им для выполнения служебных обязанностей);

– разделения обязанностей (распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для субъекта процесс или создать брешь в защите по заказу злоумышленников);

– простоты и управляемости информационной системы.

Система обеспечения безопасности информации включает следующие подсистемы (табл. 1.3):

– компьютерную безопасность;

– безопасность данных;

– безопасное программное обеспечение;

– безопасность коммуникаций.

Таблица 1.3. Подсистемы и средства обеспечения информационной безопасности

Подсистема обеспечения безопасности информации	Средство обеспечения
Компьютерная безопасность	Комплекс технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов
Безопасность данных	Защита данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения
Безопасное программное обеспечение	Общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы
Безопасность коммуникаций	Обеспечивается принятием мер по предотвращению[33] предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос

[33] Защита информации в экономических системах. URL: http://elibrary.ru (дата обращения: 18.12.2022).

В России Федеральным законом «Об информации, информационных технологиях и о защите информации» гарантируется право обладателя информации на ее использование и защиту от доступа к ней других лиц (организаций)[34]. Критерием для принятия решения о защите информации является ценность информации.

Укрепление информационной безопасности в концепции национальной безопасности Российской Федерации названо в числе важнейших долгосрочных задач. Система информационной безопасности выступает важным связующим звеном всех основных компонентов государственной политики в единое целое.

Государственная информационная политика должна быть нацелена на решение следующих важных задач:

– формирование единого информационного пространства России и ее вхождение в мировое информационное пространство;

– обеспечение информационной безопасности личности, общества и государства;

– формирование демократически ориентированного массового сознания;

– становление отрасли информационных услуг;

– расширение правового поля регулирования общественных отношений, в том числе связанных с получением, распространением и использованием информации.

Темы для обсуждения

1. Найдите определения информации в различных науках и в высказываниях разных ученых и исследователей, сделайте их обзор и анализ.

2. Раскройте сущность термина «информация» и опишите уровни ее представления.

3. Поясните, почему понятия «информация», «данные», «знания» не отождествляются.

4. Перечислите основные носители информации и укажите особенности их использования.

5. Раскройте особенности информации и перечислите ее виды.

---

[34] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 18.12.2022).

6. Расскажите, что понимается под информационными ресурсами и укажите, чем они отличаются от информации.

7. Назовите классы информационных ресурсов и приведите примеры на каждый класс.

8. Перечислите свойства ценности информации. Приведите примеры зависимости ценности информации от времени.

9. Приведите примеры, в которых одинаковые лексические конструкции могут иметь различный смысл в разном контексте.

10. Поясните, что представляет собой информационный процесс. Приведите примеры информационного процесса из вашей жизни.

11. Объясните, как соотносятся понятия «защита информации», «безопасность информации» и «информационная безопасность».

12. Раскройте сущность понятия «система обеспечения информационной безопасности».

13. Перечислите, на каких принципах строится организация системы информационной безопасности.

14. Поясните, почему укрепление информационной безопасности в концепции национальной безопасности Российской Федерации названо в числе важнейших долгосрочных задач.

15. Объясните и покажите на примерах, почему в современных условиях защита информации – это дело всего мирового сообщества.

Задания для самоконтроля

Подготовьте эссе на одну из предложенных тем (до 5 страниц).

1. Моя личная информационная безопасность.

2. Современные проблемы в области информационной безопасности.

3. Пути повышения информационной безопасности в современном мире.

4. Факторы, влияющие на экономическую безопасность государства.

5. Административная ответственность за правонарушения в информационной сфере.

6. Обеспечение безопасности и сохранности информации на примере организации … .

7. Новые подходы в обеспечении информационной безопасности.

8. Ценность информации. Цена информации.

9. Источники и носители информации: классификация и особенности.

10. Интернет и проблемы контроля информации.

Выполните тест

Выберите один или несколько правильных ответов.

1. Информация – это:
   а) визуальное восприятие объекта;
   б) сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии;
   в) фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира;
   г) обыденное восприятие действительности.
2. К уровням представления информации относят:
   а) физический уровень;
   б) уровень средств взаимодействия с носителем;
   в) логический уровень;
   г) уровень высшего порядка;
   д) семантический уровень.
3. К видам информации относят:
   а) буквенную;
   б) астральную;
   в) печатную;
   г) фантастическую;
   д) научную.
4. Информационные ресурсы – это:
   а) накопленная на предприятии информация о хозяйственной деятельности;
   б) информация, хранящаяся в компьютере человека;
   в) накопленная информация об окружающей действительности, зафиксированная на материальных носителях, обеспечивающих передачу информации во времени и пространстве между потребителями для решения конкретных задач;
   г) сведения о свойствах и состоянии объектов окружающей среды.
5. Выберите примеры, относящиеся к информационным ресурсам класса «снимаемой информации»:
   а) количество безработных в стране выросло на 3 %;
   б) секвенирован геном человека;
   в) на Марсе обнаружена вода;
   г) 20 студентов закончили сессию с долгами по математике.
6. К основным свойствам информации относят:
   а) атрибутивные;
   б) статистические;
   в) прагматические;
   г) бифокальные.

7. Информационный процесс состоит из следующих фаз:

а) зарождение;

б) передача;

в) рост;

г) обработка;

д) проектирование.

8. Понятие «информационная безопасность» отличается от понятия «безопасность информации» следующим:

а) относится к самой информации;

б) относится к субъектам информационной среды;

в) относится исключительно к предприятию;

г) относится к государственному уровню.

9. Система информационной безопасности включает:

а) специальные органы и службы, обеспечивающие защиту жизненно важных интересов;

б) специальные органы и службы, соответствующие средства, методы и мероприятия, обеспечивающие защиту[35] жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз;

в) специальные мероприятия, обеспечивающие защиту жизненно важных интересов личности, предприятия и государства.

10. Система обеспечения безопасности информации включает следующие подсистемы:

а) компьютерную безопасность;

б) безопасность личности;

в) безопасное программное обеспечение;

г) безопасность государственных органов.

11. Принцип экономической эффективности предполагает:

а) недопущение неоправданных режимных ограничений;

б) превышение результатов от мер по обеспечению информационной безопасности над совокупными затратами на них;

в) распределение ролей и ответственности при организации защиты информации;

г) строгое нормирование конфиденциальности.

12. Государственная информационная политика имеет целью:

а) становление отрасли информационных услуг;

б) формирование единого информационного пространства России;

в) обеспечение информационной безопасности предприятия;

г) защиту информации.

---

[35] Организационная защита информации. URL: http://ibooks.ru (дата обращения: 18.12.2022).

Библиографический список

1. Федеральный закон «О государственной тайне» от 21.07.1993 № 5485-1 (ред. от 14.07.2022) [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_2481/b276619673d4311ef4fce8f08192952409f7b208/ (дата обращения: 18.12.2022).

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 12.11.2022).

3. Виды и свойства информации. – Режим доступа: https://helpiks.org (дата обращения: 12.11.2022).

4. Григорьев, С. М. Возникновение и история развития проблемы защиты информации [Электронный ресурс] / С. М. Григорьев, О. В. Попов. – Режим доступа: http://elibrary.ru. (дата обращения: 12.11.2022).

5. Вострецова, Е. В. Основы информационной безопасности [Электронный ресурс] : учеб. пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с. – Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 12.11.2022).

6. Гафнер, В. В. Информационная безопасность [Электронный ресурс] : учеб. пособие : в 2 ч. / В. В. Гафнер. – Екатеринбург : Урал. гос. пед. ун-т, 2009. Ч. 1. – 155 с. – Режим доступа: http://elar.uspu.ru/bitstream/uspu/4122/1/uch00029.pdf (дата обращения: 12.11.2022).

7. Защита информации в экономических системах [Электронный ресурс]. – Режим доступа: http://elibrary.ru (дата обращения: 12.11.2022).

8. Есть всё: удивительные факты об интернете и сайтах [Электронный ресурс]. – Режим доступа: https://barnaul.press/ (дата обращения: 12.11.2022).

9. Информационная безопасность [Электронный ресурс] : учеб. пособие / В. Н. Ясенев [и др.] ; под общ. ред. проф. В. Н. Ясенева. – Нижний Новгород : Нижегород. гос. ун-т им. Н. И. Лобачевского, 2018. – 182 с. – Режим доступа: http://www.iee.unn.ru/wp-content/uploads/sites/9/2018/09/Yasenev_posobie_isecurity.pdf (дата обращения: 12.11.2022).

10. Информационные ресурсы [Электронный ресурс]. – Режим доступа: https://discovered.com.ua/business/informacionnye-resursy (дата обращения: 12.11.2022).

11. Информация и информатика [Электронный ресурс]. – Режим доступа: techn.sstu.ru/kafedri/подразделения/1/MetMat/shaturn/inform/Лекция%201%5CЛекция%201.htm (дата обращения: 12.11.2022).

12. Исследование эффективных методов защиты электронного документооборота научно-производственного объединения [Электронный ресурс]. – Режим доступа: URL: http://elibrary.ru (дата обращения: 12.11.2022).

13. Организационная защита информации [Электронный ресурс]. – Режим доступа: http://ibooks.ru (дата обращения: 12.11.2022).

14. Партыка, Т. Л. Информационная безопасность [Электронный ресурс] : учеб. пособие / Т. Л. Партыка, И. И. Попов. – 3-е изд., перераб. и доп. – М. : ФОРУМ, 2010. – 432 с. – (Профессиональное образование). – Режим доступа: URL: http://kfilial.mggeu.ru/wp-content/uploads/2021/02/Partyka-T.L.-Popov- I.I.-Informatsionnaya-bezopasnost-1.pdf (дата обращения: 12.11.2022).

15. Современные информационные технологии. – Режим доступа: http://elibrary.ru (дата обращения: 12.11.2022).

16. Сухостат, В. В. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / В. В. Сухостат, И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с. – Режим доступа: https://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informaczionnoj-bezopasnosti.pdf (дата обращения: 12.11.2022).

Глава 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОНЯТИЯ, ВИДЫ, КЛАССИФИКАЦИЯ И РИСКИ

2.1. Информационные угрозы: сущность, виды, способы воздействия на экономический объект, направления реализации

Изменение геополитической ситуации в связи с использованием рядом государств санкционных мер против России, проведением специальной военной операции привели к значительному возрастанию рисков угроз информационной безопасности. Взаимное противостояние в информационной сфере усилилось.

В начале 2022 года количество информационных атак в целом увеличилось почти на 15 % по сравнению с концом 2021 года. Чаще всего они организовывались на государственные и медицинские учреждения, промышленные предприятия. Серьезным атакам подверглись СМИ. Число атак в целом без привязки к отраслям экономики выросло с 18 до 23 %.

Усилились атаки на веб-ресурсы, их доля выросла до 22 % по сравнению с 13 %, наблюдаемыми в конце 2021 года. Увеличилась доля информационных атак, которые стали возможны из-за компрометации или подбора учетных данных. В основном такие воздействия проводятся на веб-ресурсы и аккаунты компаний в социальных сетях[36].

Угрозы информационной безопасности имеют отношение ко всем макроэкономическим субъектам – государству, предприятиям (бизнесу) и организациям и домохозяйствам (отдельным индивидам). В масштабе страны они имеют отношение к информационным ресурсам, функционированию информационных и телекоммуникационных систем на территории страны.

Для государства угрозы информационной безопасности выражаются в разглашении государственной тайны, вовлечении в информационные войны, подрыве репутации страны, нарушении международного взаимодействия, ухудшении инвестиционного климата, увеличении затрат на организацию защиты и т. д.

Для организаций и граждан информационные атаки создают риски подрыва деловой репутации, раскрытия коммерческой тайны, похищения секретов производства и управления, кражи денежных средств, незаконного использования персональных данных, нарушения целостности и доступности информации и т. д.[37]

Под угрозой информационной безопасности понимается случайное или преднамеренное явление, событие, действие или процесс, которые могут привести к искажению, несанкционированному использованию или к уничтожению информационных ресурсов, информационной системы, используемых программных и технических средств[38], т. е. к нанесению ущерба интересам хозяйствующих субъектов.

По мнению В. В. Сухостата, угроза информационной безопасности определяется как совокупность условий и факторов, создающих

---

[36] Актуальные киберугрозы: I квартал 2022 года. URL: https://www.ptsecurity. com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 12.11.2022).

[37] Партыка Т. Л., Попов И. И. Информационная безопасность : учеб. пособие. 3-е изд., перераб. и доп. М. : ФОРУМ, 2010. 432 с. (Профессиональное образование). URL: http://kfilial.mggeu.ru/wp-content/uploads/2021/02/Partyka-T.L.-Popov-I.I.-Informatsionnaya-bezopasnost-1.pdf (дата обращения: 12.11.2022).

[38] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.]. Н. Новгород : Нижегород. гос. ун-т им. Н. И. Лобачевского, 2018. 182 с. URL: iBEZOPM.docx http://unn.ru (дата обращения: 12.11.2022).

потенциальную или реально существующую опасность нарушения безопасности информации[39].

Принято считать, что информационная безопасность обеспечена тогда, когда для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности, целостности и доступности.

Исходя из этого для информационных систем (ИС) выделяют три основных вида угроз:

– нарушение конфиденциальности;

– нарушение целостности;

– отказ служб.

Эти угрозы являются непосредственными или прямыми, так как наносят вред защищаемой информации.

Преодоление системы защиты также представляет собой угрозу – угрозу раскрытия параметров ИС. Такая угроза считается опосредованной, или косвенной, поскольку ее реализация не причиняет вред защищаемой информации, но дает возможность реализации непосредственных угроз информационной безопасности.

Источниками угроз информационной безопасности могут быть субъект (физическое лицо), материальный объект или физическое явление: хакеры, пользователи ИС, имеющие или не имеющие злой умысел, компьютерные процессы, сбои и др.

Среди имеющихся источников информационных опасностей и угроз выделяют внутренние и внешние.

Источниками внутренних угроз выступают:

– сотрудники организации;

– программное обеспечение;

– аппаратные средства.

К внешним источникам угроз относятся:

– компьютерные вирусы и вредоносные программы;

– организации и отдельные лица;

– стихийные бедствия[40].

Поскольку источников угроз достаточно много, то и виды угроз весьма разнообразны. Виды угроз можно классифицировать по разным признакам. Остановимся на некоторых классификациях видов угроз.

---

[39] Сухостат В. В., Васильева. И. Н. Указ. соч.

[40] Гафнер В. В. Указ. соч.

1. По своему влиянию на объект информационные угрозы делятся на две группы:

а) внутренние. Они могут проявляться в следующих формах:

– ошибки пользователей и системных администраторов;

– нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;

– ошибки в работе программного обеспечения;

– отказы и сбои в работе компьютерного оборудования;

б) внешние. Они связаны с неправомерными действиями конкурентов, партнеров, хакеров, мошенников и т. д.

Объектами воздействия информационной угрозы могут быть:

– информационная система как таковая (взламывание логина и пароля для входа в систему, запуск вируса, препятствующего нормальному функционированию системы и т. д.);

– составные элементы системы (программные и технические средства, базы данных и т. д.);

– узлы и каналы передачи информации.

2. По причине возникновения информационные угрозы можно разделить на две основные группы:

– естественные (аварии, стихийные бедствия);

– искусственные (связаны с деятельностью человека).

Искусственные информационные угрозы бывают:

а) случайными или неумышленными (нарушения, допущенные системными администраторами, работниками, отвечающими за все виды работ с информацией);

б) преднамеренными или умышленными (для нанесения разного рода ущерба пользователям информационной системы).

В свою очередь, умышленные угрозы по характеру воздействия можно разделить:

– на пассивные – не влияют на функционирование информационной системы (копирование трафика, документации, подслушивание переговоров и т. п.);

– активные – нарушают нормальный процесс функционирования информационной системы[41] (промышленный шпионаж, передача документации, электронных носителей информации, внесение технических изменений в аппаратно-программные средства и др.).

---

[41] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

3. По степени зависимости от активности автоматизированной системы (АС) различают:

– угрозы, которые могут проявляться независимо от активности АС (вскрытие шифров криптозащиты информации, хищение магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем);

– угрозы, которые могут проявляться только в процессе автоматизированной обработки данных (угрозы выполнения и распространения программных вирусов).

4. По текущему месту расположения информации, хранимой и обрабатываемой в АС, выделяют угрозы доступа к информации:

– на внешних запоминающих устройствах (жестком диске);

– в оперативной памяти;

– циркулирующей в линиях связи;

– информации, отображаемой на терминале или печатаемой на принтере[42].

5. По виду воздействия на объект информационной безопасности информационные угрозы делятся на три группы:

1) Разглашение – умышленные или неосторожные действия, приведшие к раскрытию конфиденциальной информации (утеря, передача, пересылка, опубликование по различным каналам распространения).

2) Утечка – бесконтрольный выход конфиденциальной информации за пределы информационной системы или круга лиц, которым она была доверена, вследствие разглашения, ухода по различным каналам через соответствующие носители информации.

3) Несанкционированный доступ – противоправное преднамеренное ознакомление с конфиденциальной информацией недопущенных лиц (подслушивание, выведывание, хищение носителей информации, документальных отходов, копирование носителей информации, фотографирование, скрытая видеосъемка, несанкционированное подключение к линиям связи и аппаратным средствам информационной системы с нейтрализацией средств ее защиты[43], распространение вредоносных программ).

---

[42] Голиков А. М. Основы информационной безопасности : учеб. пособие / А. М. Голиков. – Томск : Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. 288 с. URL: https://edu.tusur.ru/publications/1024/download (дата обращения: 18.12.2022).

[43] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

6. По способам воздействия информационных угроз выделяют следующие группы:

1) Информационные (нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации, несанкционированный доступ к информационным ресурсам, манипулирование информацией (дезинформация, сокрытие или сжатие информации), нарушение технологии обработки информации).

2) Программно-математические (внедрение компьютерных вирусов, установка программных и аппаратных закладных устройств, уничтожение или модификация данных в автоматизированных информационных системах).

3) Организационно-правовые (несвоевременное применение нормативно-правовых положений или неправомерное ограничение доступа к нормативно-правовым документам в информационной сфере).

4) Физические (уничтожение или порча средств обработки информации и связи, машинных или других носителей информации; хищение программных или аппаратных ключей и средств криптографической защиты информации; воздействие на персонал; перехват информации в технических каналах ее возможной утечки, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи; внедрение электронных устройств перехвата информации в технические средства и помещения и др.).

На рисунке представлены некоторые классификации угроз информационной безопасности и соответствующие им виды.

Классификация и виды угроз информационной безопасности

Ущерб от возможных угроз может быть не только экономическим, связанным с потерей денежных средств, но и социальным, когда информация используется в противоправных и аморальных целях.

Злоумышленники используют разные направления и методы реализации угроз. К основным направлениям относят:

– непосредственное обращение к объектам доступа;

– создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

– модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;

– внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС[44].

Источники, мотивация и действие угрозы представлены в табл. 2.1.

Таблица 2.1. Источник, мотивация и действие угрозы

Источник угрозы	Мотивация	Действие угрозы
Хакер, взломщик	Вызов	Хакерство
	Сомнение	Социальная инженерия
	Бунтарство	Проникновение в систему, взлом
	Статус	Несанкционированный доступ к системе
	Деньги	
Лицо, совершающее компьютерное преступление	Разрушение информации	Компьютерное преступление (например, компьютерное преследование)
	Незаконное раскрытие информации	Мошенническая деятельность (например, воспроизведение, выдача себя за другого, перехват)
	Денежная выгода	Информационный подкуп
	Несанкционированное изменение данных	Получение доступа обманным путем
		Проникновение в систему
Террорист	Шантаж	Взрыв/Терроризм
	Разрушение	Информационная война
	Использование в личных интересах	Системная атака (например, распределенный отказ в обслуживании)
	Месть	Проникновение в систему
	Политическая выгода	Порча системы
	Охват среды (передачи данных)	

[44] Угрозы информационной безопасности. URL: learn.urfu.ru›resource/index/data…id…revision_id/0 (дата обращения: 18.12.2022).

Для защиты интересов субъектов информационных отношений на разных уровнях разрабатываются соответствующие меры.

1. Законодательный уровень: регламентация деятельности на основе действующего законодательства, наступление ответственности за нарушение правильности таких действий.

2. Административный уровень: разработка программ в области информационной безопасности и обеспечение их выполнения.

3. Процедурный уровень: разработка конкретных мер безопасности, ориентированных на людей.

Эти мероприятия осуществляются:

– при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;

– проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения;

– разработке правил доступа пользователей к ресурсам системы;

– подборе и подготовке персонала, обслуживающего систему;

– организации охраны и режима допуска к системе;

– организации учета, хранения, использования и уничтожения документов и носителей информации;

– организации явного и скрытого контроля за работой пользователей.

4. Программно-технический уровень. Технические меры защиты основаны на использовании специальных программ и аппаратуры, которые выполняют функции защиты через идентификацию и аутентификацию пользователей; разграничение доступа к ресурсам; регистрацию событий; криптографические преобразования; проверку целостности системы; отсутствие вредоносных программ; программную защиту передаваемой информации и каналов связи; защиту системы от наличия и появления нежелательной информации; создание физических препятствий на путях проникновения нарушителей; мониторинг и сигнализацию соблюдения правильности работы системы; создание резервных копий ценной информации и др.[45]

Угрозы информационной безопасности находят свое проявление в компьютерных преступлениях.

---

[45] Гафнер В. В. Указ. соч.

2.2. Компьютерные преступления: сущность и виды

В последнее время компьютерные преступления в связи с масштабированием процессов цифровизации становятся постоянным явлением. Сущность термина «компьютерные преступления» трактуется как противоправное действие, поведение, как род преступления.

Так, компьютерные преступления, по мнению Б. К. Леонтьева, – это действия, совершаемые с целью получения и использования информации в компьютерной сфере. Компьютерная информация может быть как предметом, так и средством совершения преступления.

С. Ю. Седаков и Т. П. Филиппова к компьютерным преступлениям относят любого рода преступления, связанные с компьютерной техникой, которые при этом противоречат праву.

По мнению А. К. Бекряшева, компьютерным преступлением следует считать незаконное и неразрешенное поведение, которое тесно соприкасается с обработкой и передачей данных.

В. Б. Вехов считает, что компьютерные преступления – это опасные действия, предусмотренные уголовным законом, в которых информация ЭВМ является объектом преступления[46].

Для компьютерных преступлений характерны следующие особенности:

– высокая латентность (низкая степень раскрываемости)[47];

– отсутствие четкой программы и методики борьбы с компьютерными преступлениями[48];

– отсутствие следственной практики по расследованию компьютерных преступлений;

– транснациональный характер;

– значительный материальный ущерб;

– высокий профессионализм преступников.

Поскольку компьютерные преступления не знают государственных границ, Советом Европы в 2001 году была принята Конвенция по

---

[46] Минаев С. В. Компьютерные преступления: сущность, особенности и возможности предотвращения. URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya#:~:text=Компьютерные%20преступления%20-%20это%20действия%2C,которые%20при%20этом%20противоречат%20праву (дата обращения: 18.12.2022).

[47] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

[48] Там же.

борьбе с киберпреступлениями, которая стала первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений.

Согласно Европейской Конвенции киберпреступления – это правонарушения, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерное использование указанных систем, сетей и данных.

К компьютерным преступлениям «в чистом виде» в Конвенции отнесены: незаконный доступ, незаконный перехват информации, вмешательство в данные, вмешательство в систему.

Остальные преступления (нарушения авторских и смежных прав; использование компьютера как орудия преступления, например мошенничества, и как интеллектуального средства, например для размещения информации, разжигающей национальную рознь) – это либо связанные с компьютером (computer-related), либо совершаемые с помощью компьютера (computer-facilitated) преступления[49].

По способу совершения компьютерные преступления классифицируют на несколько групп.

1. *Несанкционированный доступ*. Его виды представлены в табл. 2.2.

Таблица 2.2. Виды несанкционированного доступа и их содержание

Вид несанкционированного доступа	Содержание
Подключение	Несанкционированный доступ к вычислительным ресурсам, воздействие на парольно-ключевые системы, установка программных и закладных устройств
Модификация	Внесение в информацию любых изменений, обусловливающих ее отличие от оригинальной
Блокирование	Невозможность доступа к ней со стороны законного пользователя
Уничтожение	Полная или частичная ликвидация как самой информации, так и ее носителей

[49] Киберпреступность – определение, классификация киберпреступлений. URL: https://elcomrevue.ru/blog/cybercrime/kibeoprestupnost-chto-eto?ysclid=l9n22cd25b604635415 (дата обращения: 18.12.2022).

Причинами возникновения несанкционированного доступа могут стать:

а) неверно настроенная система контроля доступа к определенным базам данных;

б) пробелы в организации защиты различных средств авторизации;

в) программное обеспечение;

г) превышения служебных полномочий.

К основным способам получения несанкционированного доступа относят:

– взлом информационных ресурсов;

– перехват сообщений;

– сбор данных (может производиться законными способами, но преследовать противоправную цель);

– шантаж, вымогательство, дача взятки;

– похищение информации.

Получение несанкционированного доступа предполагает утечку данных, риск модификации сведений, вероятность внедрения дистанционно управляемого программного обеспечения (ПО), даже полное выведение из строя компьютерной системы.

Несанкционированный доступ ведет к риску потери управления организацией. Для защиты от несанкционированного доступа применяются электронные замки, одноразовые пароли, биометрия. Максимальный уровень безопасности достигается при многофакторной аутентификации, когда доступ предоставляется при совпадении данных из разных источников (например, результатов сканирования радужки глаза, предъявления смарт-карты и введения пароля)[50].

2. *Вирусная модификация* – это разработка, использование или распространение компьютерных вирусных программ, которые заведомо приводят к нарушению работы ЭВМ или их сетей, внесению в компьютерную информацию несанкционированных собственником изменений.

Компьютерными вирусами называют виды вредоносного программного обеспечения, которые внедряются в код других программ, системную память или загрузочные секторы и могут распространять

---

[50] Несанкционированный доступ (НСД). URL: https://www.anti-malware.ru/threats/unauthorized-access (дата обращения: 18.12.2022).

собственные копии по различным каналам цифровой связи[51]. Такие программы пишутся специально для получения доступа к компьютеру без разрешения его владельца для кражи или уничтожения компьютерных данных.

Большинство систем заражается вирусами из-за ошибок в программах, уязвимости операционных систем и плохой защиты. По данным AV-Test, независимой организации, занимающейся анализом и оценкой антивирусного и защитного программного обеспечения, каждый день обнаруживается около 560 000 новых вредоносных программ.

Существуют различные типы компьютерных вирусов[52], которые отличаются в зависимости от их происхождения, возможностей распространения, места хранения, файлов, которые они заражают, и разрушительной природы.

Перечислим некоторые из них.

1. Вирус загрузочного сектора.
2. Вирус прямого действия.
3. Вирус перезаписи.
4. Скрипт-вирусы.
5. Каталоговый вирус.
6. Полиморфный вирус.
7. Резидентный вирус памяти.
8. Макровирус.
9. Вирус-компаньон.
10. Многосторонний вирус[53].
11. FAT-вирус.
12. Троянский конь.
13. Червь.
14. Логические бомбы (не вирус, но по своей сути вредонос, как червь и вирус).

Первый в истории компьютерный вирус (под названием Creeper) был написан Бобом Томасом из компании BBN Technologies в 1971 году.

---

[51] На всякий пожарный: загрузочные диски скорой антивирусной помощи. Последние новости России и Мира сегодня. URL: https://anticwar.ru (дата обращения: 18.12.2022).

[52] 14 различных типов компьютерных вирусов. URL: https://new-science.ru/14-razlichnyh-tipov-kompjuternyh-virusov/ (дата обращения: 18.12.2022).

[53] На всякий пожарный: загрузочные диски скорой антивирусной помощи …

Creeper был экспериментальной самовоспроизводящейся программой, которая не имела никакого злого умысла[54]. Она только выводила надпись на экран компьютера: «I'M THE CREEPER. CATCH ME IF YOU CAN!» («Я – Крипер. Поймай меня, если сможешь!»).

В том же 1971 году появился и первый антивирус. Это была программа Reaper, в задачи которой входило находить копии программы Creeper и прекращать их работу[55].

В 1986 году Амджад Фарук Алви и Басит Фарук Алви написали вирус для загрузочного сектора под названием «Brain», чтобы предотвратить несанкционированное копирование созданного ими программного обеспечения. «Brain» считается первым компьютерным вирусом[56] для IBM PC и совместимых компьютеров[57].

2 ноября 1988 года студент Корнельского университета Роберт Моррис-младший запустил программу-червь. Червь Морриса стал первым успешно распространившимся сетевым червем и одной из первых программ, эксплуатирующих такую уязвимость, как переполнение буфера. Всего за 1,5 часа червь заразил 6000 компьютеров.

Именно из-за червя Морриса были пересмотрены требования к безопасности систем и созданы специальные институты, занимающиеся безопасностью компьютеров и разрабатывающие рекомендации по устранению вирусов[58].

Первым вирусом, специально нацеленным на Microsoft Windows, был WinVir. Он был обнаружен в 1992 году. Вирус не содержал никаких вызовов Windows API. Вместо этого он использовал API DOS.

Самой разрушительной вредоносной программой на сегодняшний день остается MyDoom. Впервые обнаруженный в январе 2004 года, он стал самым быстро распространяющимся почтовым червем в истории. Он создавал сетевые дыры, через которые злоумышленники получали доступ к зараженным машинам. В 2004 году почти четвертая часть всех электронных писем была заражена MyDoom. Ущерб от этого вируса составил более 38 млрд дол.[59].

---

[54] На всякий пожарный: загрузочные диски скорой антивирусной помощи …

[55] Когда появился первый компьютерный вирус URL: https://www.pnp.ru/social/kogda-poyavilsya-kompyuternyy-virus.html Автор: Мария Соколова. (дата обращения: 18.12.2022).

[56] На всякий пожарный: загрузочные диски скорой антивирусной помощи ...

[57] Там же.

[58] 14 различных типов компьютерных вирусов.

[59] На всякий пожарный: загрузочные диски скорой антивирусной помощи …

3. *Перехват информации* – это получение информации непосредственно через подключение к коммуникационным каналам системы или линиям периферийных устройств (кабельные и проводные системы, системы спутниковой связи и т. д.), а также путем приема электромагнитного и акустического излучения пассивными средствами приема[60].

Информация – важный ресурс, это конкурентное преимущество любой компании. Некоторые компании прибегают к незаконным способам добычи сведений – несанкционированному перехвату информации. Перехваченная информация может быть использована для шантажа, получения наживы, конкурентного преимущества, проведения вредоносных кампаний. Перехват информации осуществляется именно во время ее передачи. Хранящиеся данные, как правило, надежно защищены.

Перехват информации может производиться путем подключения к каналам ее передачи, получения контроля над одним из этапов передачи, внедрения шпионской программы или использования аппаратных средств[61].

При прослушке телефонов, подключенных к сотовой связи, используются как специальные программы, так и прямое подключение к кабелю, позволяющее перехватывать весь трафик. Однако если связь использует шифрование, то такое подключение бесполезно.

Перехватывать информацию могут не только злоумышленники. Этим может заниматься и сама организация, владеющая конфиденциальными данными, чтобы их защитить. Для этих целей компании используют DLP-системы. Это класс программ, которые созданы для того, чтобы держать под контролем каналы цифровой коммуникации[62].

Цель такого перехвата – проверка, не используются ли цифровые каналы для передачи секретов организации, и не вредят ли сотрудники интересам работодателя. Программа решает, какая информация отно-

---

[60] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

[61] Перехват информации. Что это такое и какие способы перехвата существуют? – Falcongaze URL: https://falcongaze.com (дата обращения: 18.12.2022).

[62] Там же.

сится к конфиденциальной, сравнивая ее с хранящимися в базе образцами. Система может срабатывать не только на файлы, но и на отдельные слова и фразы[63].

Таким образом, перехват информации может быть не только угрозой безопасности, но и методом борьбы с угрозами. Многие компании, особенно связанные с финансами, обороной, передовыми разработками, энергетикой, хранящие и обрабатывающие персональные или секретные данные, прибегают к фильтрации входящего и исходящего трафика, чтобы гарантировать сохранность этих данных. В Уголовном Кодексе РФ установлено наказание за преступления в сфере компьютерной информации (гл. 28)[64].

Зарубежные специалисты утверждают, что в последнее время стал стремительно меняться ландшафт киберугроз. Они выделяют следующие современные тенденции в сфере кибербезопасности.

1. Масштабирование атак на цепочки распространения ПО, что увеличивает число «жертв» среди крупных компаний.

Злоумышленники ищут слабые звенья в программном обеспечении вендора (поставщик, который продает и продвигает товары и услуги под собственным брендом или торговой маркой); их интересует распространенный среди предприятий и организаций по всему миру софт или они сосредоточиваются на конкретном программном обеспечении, которое используют компании.

Злоумышленники нацеливаются прежде всего на вертикально интегрированные организации: медицинские компании, предприятия из области энергетики и добывающей промышленности, которые используют большое количество оборудования и ПО от разных производителей[65].

2. Усиление прессинга со стороны преступных группировок, использующих программы-вымогатели.

В последнее время хакеры применяют тактику нападения на одну и ту же компанию по несколько раз подряд. Специалисты сравнивают сложившуюся ситуацию с травлей в социальных сетях. Если компания покажет свою «слабость» в вопросе информационной безопасности,

---

[63] Перехват информации. Что это такое и какие способы перехвата существуют?

[64] Там же.

[65] Кибербезопасность в 2022 году. Прогнозы. URL: http://mobilecomm.ru (дата обращения: 18.12.2022).

она тут же окажется в поле зрения других злоумышленников, которые тоже захотят получить свою долю[66]. Очень часто хакеры, работающие с программами-вымогателями, не просто шифруют данные, они крадут их, тем самым вынуждая жертву платить выкуп как за разблокировку информации, так и за неразглашение[67].

В сферу интересов киберпреступников все чаще попадают объекты критически важной инфраструктуры (совокупность информационных систем и телекоммуникационных сетей, жизненно важных для работы таких сфер жизнедеятельности государства, как промышленность, связь, топливно-энергетический комплекс, транспорт, финансовый сектор, здравоохранение, жилищно-коммунальное хозяйство[68] и др.), где риск значительного ущерба выше и, соответственно, быстрее будет решаться вопрос выплат.

По данным Лаборатории Касперского, летом 2022 года предположительно китайскоязычная кибергруппа TA 428 атаковала оборонные предприятия и государственные органы в России, странах Восточной Европы и Афганистане. Скорее всего, целью злоумышленников был кибершпионаж. В предпринятой серии атак применялись новые модификации известных ранее бэкдоров (дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом). Атакующим удалось в ряде случаев полностью захватить ИТ-инфраструктуру. Для этого они использовали хорошо подготовленные фишинговые письма[69].

В последнее время разные группы хакеров стали активно сотрудничать в реализации нападений, и есть большая доля вероятности, что эта тенденция сохранится и будет развиваться. Уже сформировался рынок киберпреступности. Благодаря этому неподготовленные злоумышленники могут получить все необходимое для успешных кибератак от опытных хакеров. Такое сотрудничество делает атаки еще более опасными.

---

[66] Кибербезопасность в 2022 году. Прогнозы.

[67] Там же.

[68] Критическая инфраструктура России. URL: https://tadviser.ru (дата обращения: 18.12.2022).

[69] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

3. Активное использование уязвимостей встроенного программного обеспечения.

Есть вероятность, что все большее распространение получат атаки на firmware (прошивку устройства, встроенные программы). В ближайшее время наработанные техники, приемы и процедуры для взлома микропрограммного обеспечения могут попасть в руки рядовых хакеров. Взлом прошивки предоставляет злоумышленникам возможность долгое время оставаться незамеченными и не бояться обнаружения, собирая необходимую информацию и готовясь нанести серьезный удар. Организации часто пренебрегают безопасностью аппаратного программного обеспечения на своих устройствах и обновляют его намного реже по сравнению с обычным софтом[70]. В этих условиях требуется разработка стандартов безопасности микропрограммного софта, которые позволят повысить уровень защиты.

4. Гибридная работа и проведение массовых мероприятий открывают новые возможности для киберпреступников.

В условиях гибридного формата работы проблема идентификации сотрудников будет играть крайне важную роль в обеспечении безопасности. Каждый сотрудник становится мишенью для злоумышленников, поскольку количество используемых незащищенных устройств растет. Киберпреступники могут начать атаковать домашние сети руководителей высшего звена[71] и правительственных чиновников, поскольку их личные устройства взломать легче, чем корпоративную сеть.

Сотрудники привыкли использовать домашние устройства для выполнения рабочих задач или корпоративные устройства для личных целей. Это многократно увеличивает шансы злоумышленников на успешный взлом. В связи с этим можно ожидать увеличения количества фишинговых атак. В случае проведения массовых мероприятий злоумышленники нацеливаются и на организаторов, спонсоров, участников, и на гостей мероприятия и применяют фишинговые приманки с использованием вредоносных программ и программ-вымогателей[72].

Учет данных тенденций должен стать стимулом для пересмотра отношения к защите рабочих мест, чтобы снизить риски и обеспечить устойчивость перед кибератаками преступников.

---

[70] Кибербезопасность в 2022 году. Прогнозы.

[71] Там же.

[72] Основные прогнозы в области кибербезопасности на 2022 год. URL: https://globalcio.ru/news/20593/?ysclid=l9n82whgc9184256888 (дата обращения: 18.12.2022).

2.3. Роль государства в минимизации рисков угроз информационной безопасности

В текущих реалиях (санкции зарубежных стран против России, проведение специальной военной операции) ведется организованная кибервойна с целью вывода из строя всей критической инфраструктуры страны.

Критическая инфраструктура используется крупнейшими компаниями страны, поэтому очень важно иметь надежную защиту, ведь в условиях кибервойны любые ошибки и неконкурентные решения могут привести к катастрофическим последствиям. Здесь важную роль играет объединение усилий ведущих компаний страны и активизация роли государства в области кибербезопасности[73].

Роль государства видится в усилении руководящей и контролирующей функций, в создании единого органа управления, разработке единых правил и требований, единых процессов, которые распространялись бы и на государство, и на бизнес. От государства требуется аудит российских решений в сфере кибербезопасности, чтобы понимать, какие из них действительно можно использовать и в каких сегментах бизнеса.

Без государства не обойтись и в подготовке кадров, поскольку именно государство формирует заказ на специалистов. В начале 2022 года в сфере кибербезопасности в России работало около 5 тыс. специалистов, а это лишь двадцатая часть потребности страны[74].

В отношении киберзащиты в стране сделано уже достаточно много, но и предстоит сделать немало. Две области требуют особого внимания и подключения государственных институтов: защита облаков и защита высоконагруженных систем, потому что для крупных компаний российских конкурентоспособных решений здесь пока еще нет.

В свете усиления напора киберпреступников летом 2022 года Минцифры РФ запустило реестр недопустимых событий в информационной безопасности для госструктур и объектов критической информационной инфраструктуры.

---

[73] Безопасность критической информационной инфраструктуры Российской Федерации. URL: https://www.tadviser.ru/index.php/Статья:Безопасность_критической_информационной_инфраструктуры_РФ (дата обращения: 18.12.2022).

[74] Там же.

Серьезную работу в плане защиты от киберпреступников проводит Сбербанк, у него имеется несколько разработок в сфере кибербезопасности. Среди них система *антифрода*, которая позволяет предотвращать 99 % угроз телефонного мошенничества, и система *анализа киберугроз*.

Основу противостояния киберпреступникам составляют центры киберзащиты, которые должны в первую очередь использовать отечественный софт. В стране в целом таких центров пока немного – всего пять и один из них – в Сбербанке[75]. Переход на собственные разработки для защиты всего периметра государства – важнейшая задача страны на ближайшие два года.

ИТ-компания «Цифра» в 2022 году назвала порядка 10 – 15 ПО импортного производства, которое установлено на ведущих промышленных предприятиях страны; ограничение или прекращение доступа к ним усилит риски и приведет к серьезным угрозам[76]. Например, это продукты Aveva (Wonderware) в области управления производством для непрерывных производств, которые используют большинство нефтеперерабатывающих и металлургических предприятий в России. Если вендор решит отозвать лицензии, то крупнейшие нефтеперерабатывающие предприятия России останутся без системы сопровождения[77].

То же относится и к продуктам разработчика Petroleum Experts, которые используются в нефтяном комплексе для интегрированного моделирования активов и интегрированного планирования добычи углеводородов; к продуктам для сбора данных и диспетчерского контроля уровня SCADA (используются для управления заглушками, насосами нефти и воды). Их отключение может привести к полной остановке транспортировки нефти и нефтепродуктов по трубопроводам[78] и воды по водоканалам.

Примерно по 400 видам корпоративного ПО бизнес подтвердил критическую зависимость от импорта, а объем ежегодных расходов частного сектора составляет около 200 млрд. руб. (покупка лицензий,

---

[75] Безопасность критической информационной инфраструктуры Российской Федерации.

[76] Критическая инфраструктура России.

[77] Там же.

[78] Там же.

внедрение и поддержка).[79] Некоторые риски, связанные с использованием импортного программного обеспечения, уже наступили. Например, SAP отказал «Силовым машинам» в поддержке облачной платформы, фактически запретив доступ к ней. О приостановке или прекращении деятельности на территории России сообщали[80] GE, Honeywell, Emerson.

Риск заключается еще и в том, что критически важные системы зависят от разработчика, который работает в другой стране, и если система начнет выдавать ошибки, то ее нельзя будет исправить из-за недоступности разработчика. А собственная служба поддержки не имеет исходных кодов решений[81].

Сейчас стране важно обеспечить технологическую независимость от используемого иностранного программного обеспечения, стимулировать спрос на отечественные продукты. Чем больше в ПО инженерного знания, тем сложнее его импортозаместить, например, различные CAD/CAM-системы или системы геологического цифрового моделирования – наиболее сложные для импортозамещения[82]. Тем не менее в стране были определены важнейшие ниши и направления, где доминирует иностранное ПО, и сформирован пул проектов по импортозамещению.

В рамках этой работы по решению Правительства Российской Федерации были созданы 33 индустриальных центра компетенций, объединивших более 300 организаций[83]. Официальные лица утверждают, что уже для 80 % иностранного софта есть российские аналоги, причем по примерно 30 % имеются два или более отечественных варианта. Исследователи считают, что по другим разработкам важно не воссоздавать текущий функционал зарубежных программных продуктов, а запустить свои, отвечающие конкретным нуждам компаний[84]. Часть решений должна быть ориентирована на экспорт и нисколько не уступать по качеству импортным аналогам.

---

[79] Критическая инфраструктура России.
[80] Там же.
[81] Там же.
[82] Там же.
[83] Там же.
[84] Там же.

В марте 2022 года был издан Указ о мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры страны. Согласно ему с 31 марта 2022 года заказчики, выполняющие закупки по 223-ФЗ, не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации. С 1 января 2025 года госорганам и госкомпаниям будет запрещено использовать иностранное ПО на значимых объектах критической информационной инфраструктуры.

По планам доля российского и евразийского программного обеспечения на значимых объектах критической информационной инфраструктуры должна была вырасти к концу 2022 года по сравнению с показателями конца августа на 10 %; а к концу 2023 года эта доля должна превышать исходные показатели уже на 40 %. За период с 2024 по 2027 годы все ПО на объектах критической информационной инфраструктуры на 100 % должно быть отечественным[85].

Темы для обсуждения

1. Перечислите причины, вызвавшие усиление угроз информационной безопасности.
2. Раскройте содержание информационных угроз в отношении государства, организаций и индивидов.
3. Перечислите основные виды угроз для информационных систем.
4. Назовите источники информационных угроз.
5. Перечислите критерии классификации видов угроз и приведите примеры угроз, относящихся к разным классификациям.
6. Опишите уровни, на которых разрабатываются меры для защиты интересов субъектов информационных отношений.
7. Охарактеризуйте подходы к определению сути компьютерных преступлений.
8. Раскройте особенности компьютерных преступлений.
9. Перечислите причины возникновения несанкционированного доступа к информации и раскройте его последствия.

---

[85] Критическая инфраструктура России.

10. Поясните назначение компьютерных вирусных программ и приведите примеры таких программ.

11. Назовите причины перехвата информации злоумышленниками.

12. Перечислите, на каких принципах строится организация системы информационной безопасности.

13. Объясните, в каком случае перехват информации не является угрозой информационной безопасности.

14. Раскройте роль государства и крупнейших компаний национальной экономики в обеспечении информационной безопасности.

15. Опишите планы России по импортозамещению зарубежного программного обеспечения.

Задания для самоконтроля

Подготовьте сообщения на темы:

1. Процесс развития средств и методов защиты информации.

2. Обеспечение информационной безопасности в ведущих зарубежных странах (на примере разных стран).

Составьте таблицу, содержащую виды преступлений в сфере информационной безопасности и установленные за них наказания, после ознакомления с российским законодательством в области информационной безопасности (УК РФ, гл. 28).

Выполните тест

Выберите один или несколько правильных ответов.

1. Несанкционированный доступ – это:

а) несоблюдение работниками правил защиты информации;

б) слабый контроль за соблюдением правил защиты информации;

в) хищение носителей информации и документальных отходов.

2. Реализации угроз информационной безопасности способствуют:

а) болтливость;

б) простудные заболевания[86];

в) локальные акты;

в) невнимательность.

3. Типовыми путями несанкционированного доступа к информации являются:

а) несанкционированное фотографирование;

б) поломка ПЭВМ;

в) стихийные бедствия.

---

[86] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

4. Несанкционированным доступом к информации НЕ является:

а) использование программных ловушек;

б) любительское фотографирование;

в) включение в библиотеки программ специальных блоков типа «троянский конь».

5. К способам воздействия угроз на информационные объекты НЕ относятся:

а) программно-математические;

б) организационно-правовые[87];

в) социально-экономические.

6. Хакерная война – это:

а) атака компьютеров и сетей гражданского информационного пространства;

б) использование информации для влияния на умы союзников и противников;

в) блокирование информации, преследующее цель получить экономическое превосходство.

7. Угрозы доступности данных возникают в том случае, когда:

а) объект не получает доступа к законно выделенным ему ресурсам;

б) легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность;

в) случается ураган.

8. Внедрение компьютерных вирусов является _____ способом воздействия угроз на информационные объекты:

а) информационным;

б) физическим;

в) программно-математическим способом.

9. Логическая бомба – это:

а) способ ведения информационной войны;

б) компьютерный вирус;

в) дебаты на техническую тему.

10. К объектам информационной атаки НЕ относятся:

а) АС в целом;

б) каналы передачи данных;

в) природоохранные мероприятия.

11. «Мобильные» вирусы распространяются:

а) путем взлома программ ЭВМ;

б) в виде «червей» и «троянцев» для мобильных телефонов;

---

[87] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

в) по линии связи между узлами сети[88];

г) по телефонной связи.

12. Для компьютерных преступлений НЕ характерна:

а) сложность сбора доказательств;

б) наличие достаточной следственной практики по раскрытию компьютерных преступлений в Российской Федерации;

в) высокая латентность[89].

13. К современным тенденциям в сфере кибербезопасности относят:

а) расширение атак на цепочки распространения ПО;

б) преобладание прослушки телефонов;

в) активизация преступных группировок;

г) импортозамещение.

14. Основная задача России в плане обеспечения кибербезопасности:

а) тщательный отбор сотрудников на работу в ИТ-отделы компаний;

б) импортозамещение программного обеспечения;

в) ужесточение наказаний за киберпреступления;

г) закупка нового китайского ПО за рубежом.

Библиографический список

1. Актуальные киберугрозы: I квартал 2022 года. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 18.12.2022).

2. Безопасность критической информационной инфраструктуры Российской Федерации [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Безопасность_критической_информационной_инфраструктуры_РФ (дата обращения: 18.12.2022).

3. Гафнер, В. В. Информационная безопасность [Электронный ресурс] : учеб. пособие : в 2 ч. / В. В. Гафнер. – Екатеринбург : Урал. гос. пед. ун-т, 2009. – Ч. 1. – 155 с. – Режим доступа: http://elar.uspu.ru/bitstream/uspu/4122/1/uch00029.pdf (дата обращения: 18.12.2022).

4. Голиков, А. М. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / А. М. Голиков. – Томск : Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 288 с. – Режим доступа: https://edu.tusur.ru/publications/1024/download (дата обращения: 18.12.2022).

---

[88] Информационная безопасность : учеб. пособие / В. Н. Ясенев [и др.].

[89] Там же.

5. Информационная безопасность [Электронный ресурс] : учеб. пособие / В. Н. Ясенев [и др.] ; под общей ред. проф. В. Н. Ясенева. – Н. Новгород : Нижегород. гос. ун-т им. Н. И. Лобачевского, 2018. – 182 с. – Режим доступа: iBEZOPM.docx http://unn.ru (дата обращения: 18.12.2022).

6. Киберпреступность – определение, классификация киберпреступлений [Электронный ресурс]. – Режим доступа: https://elcomrevue.ru/blog/cybercrime/kibeoprestupnost-chto-eto?ysclid=l9n22cd25b604635415 (дата обращения: 18.12.2022).

7. Кибербезопасность в 2022 году. Прогнозы [Электронный ресурс]. – Режим доступа: http://mobilecomm.ru (дата обращения: 18.12.2022).

8. Когда появился первый компьютерный вирус [Электронный ресурс]. – Режим доступа: https://www.pnp.ru/social/kogda-poyavilsya-kompyuternyy-virus.html (дата обращения: 18.12.2022).

9. Критическая инфраструктура России [Электронный ресурс]. – Режим доступа: https://tadviser.ru (дата обращения: 18.12.2022).

10. Минаев, С. В. Компьютерные преступления: сущность, особенности и возможности предотвращения [Электронный ресурс] / С. В. Минаев. – Режим доступа: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya#:~:text=Компьютерные%20преступления%20-%20это%20действия%2C,которые%20при%20этом%20противоречат%20праву (дата обращения: 18.12.2022).

11. На всякий пожарный: загрузочные диски скорой антивирусной помощи. Последние новости России и Мира сегодня [Электронный ресурс]. – Режим доступа: https://anticwar.ru (дата обращения: 18.12.2022).

12. Несанкционированный доступ (НСД) [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/threats/unauthorized-access (дата обращения: 18.12.2022).

13. Основные прогнозы в области кибербезопасности на 2022 год [Электронный ресурс]. – Режим доступа: https://globalcio.ru/news/20593/?ysclid=l9n82whgc9184256888 (дата обращения: 18.12.2022).

14. Партыка, Т. Л. Информационная безопасность [Электронный ресурс] : учеб. пособие / Т. Л. Партыка, И. И. Попов. – 3-е изд., перераб. и доп. – М. : ФОРУМ, 2010. – 432 с. – (Профессиональное образование). – Режим доступа: http://kfilial.mggeu.ru/wp-content/uploads/2021/02/Partyka-T.L.-Popov-I.I.-Informatsionnaya-bezopasnost-1.pdf (дата обращения: 18.12.2022).

15. Перехват информации. Что это такое и какие способы перехвата существуют? – Falcongaze [Электронный ресурс]. – Режим доступа: https://falcongaze.com (дата обращения: 18.12.2022).

16. Сухостат, В. В. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / В. В. Сухостат, И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с. – Режим доступа: https://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informaczionnoj-bezopasnosti.pdf (дата обращения: 18.12.2022).

17. Угрозы информационной безопасности [Электронный ресурс]. – Режим доступа: learn.urfu.ru›resource/index/data…id…revision_id/0 (дата обращения: 18.12.2022).

18. 14 различных типов компьютерных вирусов [Электронный ресурс]. – Режим доступа: https://new-science.ru/14-razlichnyh-tipov-kompjuternyh-virusov/ (дата обращения: 18.12.2022).

Глава 3. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Основные понятия защиты информации

В современном мире информация представляет собой определенную для человека ценность. Как и любую другую ценность, информацию стоит защищать от ее искажения или несанкционированного доступа к ней. Особого внимания заслуживает информация, содержащая государственную и коммерческую тайну, а также персональные данные человека. Поэтому защита данных от несанкционированного доступа считается одной из приоритетных задач при проектировании любой информационной системы.

В связи с этим встает вопрос о том, как правильно защитить информацию и существует ли абсолютная защита информации. Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [1] под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Цель защиты информации – это желаемый результат защиты информации: предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной ее утечки или несанкционированного и непреднамеренного воздействия на информацию.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации

от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящее к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [1].

Защита информации от разглашения – деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Объект защиты – информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Техника защиты информации – средства защиты информации, контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Следует отметить, что защита информации является слабоформализуемой задачей, не имеющей формальных методов решения. В основе решения такого рода задач стоит системный подход, т. е. для решения задачи обеспечения информационной безопасности необходимо построить систему ее защиты. Эта система представляет собой совокупность органов или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Входами любой системы являются воздействия, меняющие состояние системы. Относительно защиты информации входами выступают угрозы информационной безопасности, создающие потенциальную или реальную опасность для защищенной информации. Источниками таких угроз следует рассматривать попытки проникновения злоумышленников к таким данным, а также ошибки персонала, выход из строя аппаратных и программных средств и стихийные бедствия. Выходами системы будет ее реакция на различные значения входов. Выходами данной системы как раз и являются меры для защиты информации.

В общем случае защита информации представляет собой противостояние специалистов по информационной безопасности и злоумышленников, которые незаконным путем добывают, изменяют или уничтожают информацию законных пользователей. Таким образом, главной целью защиты информации считается обеспечение информационной безопасности. Более детально цели и задачи защиты информации перечислены в Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации». Среди них можно выделить:

– предотвращение утечки, хищения, утраты, искажения и подделки информации;

– предотвращение угроз безопасности личности, общества, государства;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, а также других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения [2].

Но, как говорилось ранее, основная цель защиты информации – прежде всего обеспечение информационной безопасности. Информационная безопасность – одна из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки, обусловленной возрастающей ролью информации в общественной жизни.

Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными.

Информационная безопасность – это защита не только информации, но и поддерживающей инфраструктуры. Если рассматривать только информацию, то безопасность информации – это состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность. Именно эти три качества представляют собой наиболее важные свойства информации и служат равнозначными составляющими ее безопасности (рис. 3.1).

Рис. 3.1. Базовые составляющие информационной безопасности

Конфиденциальность информации – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена. Конфиденциальность является самым проработанным у нас в стране аспектом информационной безопасности. К сожалению, прак-

тическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишены возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт или анкетные данные сотрудников. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными выступают пароли для доступа к системе.

Доступность информации – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время. Информационные системы создаются для оперативного получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям. Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и т. п. Менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет. Доступность информации – настолько важное свойство, что даже главный принцип современной защиты информации звучит как поиск оптимального соотношения между доступностью и безопасностью.

Целостность информации – гарантия того, что информация сейчас существует в ее исходном виде, т. е. при ее хранении или передаче не было произведено несанкционированных изменений. Целостность информации условно подразделяется на статическую и динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др. Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими или социальными. Так, ошибка в управляющей программе приведет к остановке управляемой системы; неправильная трактовка закона может привести к его нарушениям; точно так же неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности. Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности ведет к ее фальсификации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

3.2. Абсолютная и относительная защита информации

Существует два вида защиты информации: абсолютная и относительная.

Несмотря на обилие данных про защиту информации, точного определения абсолютной защиты информации нигде нет. Поэтому предлагается рассмотреть следующий подход к определению этого термина.

Абсолютная защита информации – это совокупность мер по защите информации, которая обеспечивает ей стопроцентную безопасность в любой период времени. При этом информация не должна утратить свои ключевые свойства, т. е. быть доступной, целостной и конфиденциальной. В современных условиях технического прогресса обеспечить абсолютную защиту информации почти невозможно, задается лишь определенный уровень информационной безопасности, который отображает допустимый риск ее хищения, уничтожения или изменения.

Полностью защищенной считается информация, находящаяся на компьютере, который отключен от всех сетей, даже от электрической, и помещен в бронированный сейф, который, в свою очередь, находится в комнате, охраняемой не только с помощью охранников, но и разного рода сигнализации. Действительно, такая информация имеет стопроцентный уровень защиты. Но использовать ее нельзя, поэтому не выполняется требование доступности. А как уже было сказано ранее, нарушение хотя бы одного свойства информации приведет к нарушению системы в целом.

«Абсолютности» защиты мешает не только необходимость пользоваться защищаемыми данными, но и усложнение защищаемых систем. Использование постоянных, неразвивающихся механизмов защиты опасно, ведь с развитием техники трудно определить, какое новое устройство сможет запросто обойти вашу защиту. Многие компании, стремясь повысить уровень своего дохода, заявляют о создании абсолютно защищенных систем. Но все эти компании делают это только ради пиара, чтобы привлечь к себе внимание. На самом же деле таких систем на данный момент времени не существует.

Рассмотрим параметры, от которых зависит вероятность взлома той или иной сети. Всего этих параметров три:

– надежность средств, защищающих сеть;
– качество настройки и конфигурации системы защиты;
– быстрота реагирования на атаки злоумышленников.

Можно заметить, что так или иначе каждый параметр зависит от человеческого фактора. Но если в двух последних критериях этот фактор можно свести к минимуму или даже к нулю, то первый параметр всегда будет оставаться уязвимым. Связано это с тем, что людям, создающим эти довольно сложные системы, свойственно ошибаться и эти ошибки могут стоить очень дорого. Поэтому надежность даже суперзащищенной системы может быть сведена на нет некачественной или неграмотной настройкой, т. е. любая система требует квалифицированного персонала, не только знающего, но и умеющего грамотно настраивать средства защиты. Поэтому создание абсолютных систем защиты информации возможно только в том случае, если устранить из процесса ее создания человеческий фактор, являющийся главной причиной всех ошибок. Очевидно, что на современном этапе развития науки и информационных технологий это невозможно.

Поскольку абсолютная защита информации почти нереализуема, на всех предприятиях обычно приходится довольствоваться относительной защитой информации, гарантированно защищающей ее на тот период времени, пока несанкционированный доступ к ней влечет какие-либо последствия, т. е. секретная информация должна быть недоступна до того момента, когда она станет либо очевидной и понятной, либо уже никому не нужной.

В современной мировой практике существует огромное количество способов для предотвращения утечки информации или ее потери. Но в основном используются только шесть основных технологий защиты данных:

– препятствие;
– маскировка;
– регламентация;
– управление;
– принуждение;
– побуждение.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможности попасть на охраняемую территорию (к аппаратуре, носителям информации и т. д.). Препятствия являются одними из самых простых и относительно надежных средств защиты информации. Так, на любом большом предприятии вся аппаратура, на которой содержится определенное количество секретной информации, находится в строго охраняемом помещении. Причем такие помещения могут охраняться как людьми (охранниками), так и специальными защищающими системами, для прохождения которых необходимо знать специальный код или пароль.

Маскировка – способы защиты информации, предусматривающие преобразование данных в форму, непригодную для восприятия посторонними лицами. Говоря о маскировке информации, нельзя не сказать про такую древнюю науку, как криптография. Формально криптография (или тайнопись) определяется как наука, обеспечивающая секретность сообщения. Для расшифровки такого сообщения требуется знание принципа. Еще с древних времен люди научились шифровать информацию так, чтобы никто не мог догадаться о ее смысле. Данный способ защиты информации активно используется во время военных

конфликтов. Например, во время второй мировой войны корабли ВМФ США осуществляли связь на языке малочисленного и компактно проживающего индейского племени. На каждом корабле было несколько индейцев-«шифровальщиков», у противника не было практически никаких шансов раздобыть себе такого «криптографа». Однако у этого способа защиты есть и свои минусы. За всеми посвященными в такой язык уследить трудно, и рано или поздно он станет понятен тем, от кого пытаются скрыть зашифрованную информацию. В этом случае возникнет необходимость заменить его другим, а разработать новый язык для защиты информации и обучить ему нужное количество людей весьма затруднительно и дорого, а сделать это оперативно невозможно.

Управление – способ защиты информации, при котором осуществляется управление всеми компонентами информационной системы. Управление доступом включает в себя следующие функции защиты:

– идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

– опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

– проверку полномочий;

– разрешение и создание условий работы в пределах установленного регламента;

– регистрацию обращений к защищаемым ресурсам;

– регистрацию при попытках несанкционированных действий [3].

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Таким образом, риск доступа к секретной информации компании извне сводится к нулю. Однако работники таких компаний должны обладать высоким уровнем информационной культуры во избежание случайного рассекречивания защищенных данных.

Должностные лица компании, допущенные к работе с защищенной информацией, обязаны:

– надежно охранять имеющуюся у них информацию от хищений, утраты и несанкционированного доступа к ней;

– учитывать, хранить, обрабатывать и передавать информацию в строгом соответствии с порядком, установленным в компании;

– при обнаружении недостачи документов или электронных носителей, содержащих защищенную информацию, незамедлительно поставить в известность своего руководителя и предпринять срочные меры по их розыску.

Побуждение – метод защиты информации, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

3.3. Методы защиты информации

Основными направлениями мероприятий и методов защиты информации являются обеспечение конфиденциальности, целостности и доступности информации. Можно выделить несколько обобщенных категорий методов защиты информации. На рис. 3.2 изображены организационные, технологические и правовые методы [5].

Рис. 3.2. Классификация методов и средств защиты информации [4]

К организационным (административным) методам защиты информации относятся меры и мероприятия, регламентируемые внутренними положениями и инструкциями организации, эксплуатирующей информационную систему. Организационные меры защиты информации осуществляют поддержку технологических методов и средств и выступают неотъемлемой частью политики информационной безопасности организации:

– определение полномочий и должностных обязанностей сотрудников организации;

– определение и контроль порядка доступа сотрудников к защищаемым документам;

– обучение и информирование сотрудников, регулярное проведение семинаров и тренингов по вопросам информационной безопасности;

– присвоение грифов секретности и меток конфиденциальности документам и материалам;

– определение порядка хранения и уничтожения носителей информации;

– определение порядка регистрации пользователей информационной системы, выдачи, хранения и отзыва паролей, секретных ключей и т. п.

К технологическими методам и средствам защиты относится использование:

– программных и программно-аппаратных модулей защиты: парольных и антивирусных систем, систем идентификации и аутентификации, разграничения доступа, регистрации и аудита событий, систем резервирования и восстановления информации, межсетевых экранов и т. д.;

– аппаратных устройств: шифровальной аппаратуры, источников бесперебойного питания, специальных систем вентиляции и кондиционирования и т. п.;

– технических систем контроля физического доступа, охранной и противопожарной сигнализации, систем видеонаблюдения др.;

– криптографических методов защиты информации.

Криптографические методы – это методы шифрования и электронной подписи данных.

Для любого предприятия или компании существует своя типовая информационная система, как правило, она включает в себя четыре основных уровня, приведенные в табл. 3.1. Атаки на информационную систему, так же как и функционирование подсистем и модулей защиты, могут осуществляться на любом из этих уровней.

Таблица 3.1. Особенности защиты информации на разных уровнях информационной системы [4]

Уровень ИС	Назначение	Основные методы защиты
Прикладное программное обеспечение (приложения)	Взаимодействие с пользователем	Системы подсказок, откатов, резервирования информации. Идентификация и аутентификация, разграничение доступа. Парольная защита, скрытие, шифрование
Система управления базами данных (СУБД)	Хранение и обработка данных ИС	Идентификация и аутентификация, разграничение доступа. Архивирование, парольная защита, шифрование
Операционная система (ОС)	Обслуживание СУБД и приложений	Системы резервирования и восстановления. Идентификация, аутентификация и авторизация, разграничение доступа, скрытие, шифрование
Сеть	Взаимодействие узлов ИС	Ограничение размеров сети, скрытие топологии сети. ЭЦП сообщений и игнорирование неподписанных сообщений, шифрование. Использование специальных средств фильтрации сетевого трафика: межсетевых экранов, антивирусных средств

Эффективная защита корпоративной информации может быть достигнута только путем согласованного применения комплекса защитных мер и средств, функционирующих на разных уровнях организации информационной системы. Типовые методы обеспечения основных качеств защищенной информации представлены в табл. 3.2.

Таблица 3.2. Типовые методы защиты информации [4]

Направление защиты	Методы защиты
Конфиденциальность	Разграничение доступа к данным Парольная защита Шифрование (криптографические методы) Скрытие данных Уничтожение остаточных данных Защита от копирования Антивирусная защита
Целостность	Разграничение доступа к данным Резервирование (создание копий) данных Обеспечение доступа к файлам и данным в режиме «только чтение» Использование контрольных сумм и цифровой подписи Скрытие данных Антивирусная защита
Доступность	а) внесение избыточности: – на уровне данных – резервное копирование – на уровне приложений – использование альтернативного программного обеспечения – на аппаратном уровне – использование дублирующих периферийных устройств, дублирующей ЭВМ б) антивирусная защита

Правовые методы защиты включают:

– механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации;

– меры контроля за исполнением нормативно-правовых актов общегосударственного значения;

– разработку в рамках организации нормативных и нормативно-методических актов (инструкции, положения) по вопросам информационной безопасности и защиты информации.

В рамках каждой организации принимается своя политика безопасности, определяемая набором защищаемых информационных объектов, особенностями используемой ИС, выбранными приоритетами в сфере защиты и размера доступных ресурсов как финансовых, так и кадровых, технических, программно-аппаратных [6].

Политика безопасности – это совокупность конкретных норм, правил и практических рекомендаций, регламентирующих работу

средств защиты информационной системы организации от заданного множества угроз безопасности.

Методика создания политики безопасности организации состоит из учета основных (наиболее опасных) рисков информационной безопасности, современной ситуации, факторов непреодолимой силы и стоимости программы обеспечения безопасности. Для вычисления рисков определяются существующие угрозы информационной безопасности, их источники, а также оценивается возможность реализации и размер ущерба от атак на защищаемые информационные объекты.

Большинство типовых методов и средств защиты информации предназначены для противодействия внешним угрозам информационной безопасности. Вместе с тем в последнее время достаточно остро встает проблема противодействия инсайдерской деятельности – защита от преднамеренных действий сотрудников организаций, имеющих санкционированный доступ к информации. Наиболее распространенный подход к предотвращению инсайдерских угроз – аутентификация и контроль деятельности пользователей, а также блокирование возможных каналов утечки информации (съемных устройств, электронной почты и т. п.).

3.4. Средства защиты информации

Под средством защиты информации понимается техническое, аппаратное, программно-аппаратное или программное средство, предназначенное для решения различных задач информационной безопасности, в том числе предотвращения и блокирования атак на ИС. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп. К ним относят средства, обеспечивающие:

– защиту от разрушающего воздействия вредоносного программного обеспечения (вирусов, троянских программ, программ-шпионов и т. п.);

– разграничение доступа к информации в автоматизированных системах;

– защиту информации при передаче ее по каналам связи;

– защиту от утечки информации по различным каналам;

– материалы и средства, обеспечивающие безопасность хранения, транспортировки носителей информации и их защиту от копирования.

Растет доля комплексных решений, совмещающих функциональность различных защитных средств и обеспечивающих более полную и надежную защиту информации.

Рассмотрим указанные средства более подробно.

1. Средства, обеспечивающие защиту от разрушающего воздействия вредоносного программного обеспечения (вирусов, троянских программ, программ-шпионов и т. п.).

Как сохранность данных, так и надежная работа программного обеспечения невозможны без решения задачи их защиты от разрушающих воздействий компьютерных вирусов [5]. В настоящее время термином «компьютерный вирус» обычно называют любое вредоносное программное обеспечение.

Компьютерный вирус – программа, специально написанная для выполнения несанкционированных действий на несущем компьютере. Она способна создавать свои копии и внедрять их в файлы, системные области компьютера, на диски, сетевые папки и т. п. Основным признаком компьютерного вируса является способ его распространения наподобие биологических организмов – возможность самовоспроизводства в компьютерных системах и сетях.

Выделяют три рубежа защиты от вирусов:

– предотвращение поступления вирусов;

– предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;

– предотвращение разрушительных последствий, если атака все-таки произошла.

К организационным мерам защиты от вредоносного ПО относится соблюдение следующих правил:

– резервное копирование данных;

– использование только лицензионного программного обеспечения, полученного из надежных источников;

– ограничение круга лиц, имеющих доступ к компьютеру;

– соблюдение правил безопасности при работе в сети Интернет;

– обязательная проверка съемных носителей с помощью антивирусной программы перед использованием;

– периодическое сканирование жесткого диска с помощью антивирусной программы;

– своевременное регулярное обновление антивирусных баз.

Современными методами вирусных технологий являются:

– полиморфизм;

– метаморфизм;

– обфускация (запутывание кода), упаковка или шифрование программного кода вируса;

– стелс- или руткит-технологии.

Полиморфизм. Полиморфные вирусы не имеют постоянного кода, а значит, не могут быть обнаружены сигнатурными методами, применяемыми в большинстве антивирусных программ. Каждый экземпляр полиморфного вируса будет отличаться от остальных, что достигается шифрованием основного тела вируса и модификациями программы-расшифровщика (вирусы с самомодифицирующимися расшифровщиками).

Метаморфизм. Вирусы и другие вредоносные программы уже имеют возможность менять свои сигнатуры каждые несколько часов. Видоизменение (метаморфозы) кода вируса происходит за счет изменения команд на эквивалентные перестановки команд, вставки несущественных команд, изменения назначения адресов и т. д. Все это осуществляется «на лету» и может сопровождаться встроенным шифрованием тела вируса, еще больше усложняющим работу антивируса. По данным антивирусной лаборатории PandaLabs, более половины всех современных вирусов, червей и троянов живут в активном виде в Интернете менее суток после своего запуска, затем их код модифицируется. Динамическая «мутация» программного кода вируса делает традиционные сигнатурные методы малоэффективными.

Обфускация (запутывание кода), упаковка или шифрование программного кода вируса хоть и не исключают возможности детектирования вируса сигнатурными методами, но существенно затрудняют анализ его кода.

Стелс- или руткит-технологии предназначены для сокрытия следов присутствия вредоносной программы в системе. Технологии этого класса могут иметь разный уровень сложности.

Направления развития методов антивирусной защиты сегодня определяются перспективными методами и средствами, такими как:

– адаптивные и самообучающиеся средства;

– интеллектуальные методы;

– аппаратные средства.

2. Системы идентификации и аутентификации. Системы разграничения доступа.

Основным защитным рубежом против атак на компьютерную систему является система идентификации и аутентификации [5].

Идентификация – это присвоение пользователям идентификатора и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация – проверка принадлежности пользователю предъявленного им идентификатора (подтверждение подлинности пользователя).

Под безопасностью (стойкостью) системы идентификации и аутентификации понимается степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя. Одной из разновидностей систем идентификации и аутентификации можно назвать парольные системы. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от несанкционированного доступа любой информационной системы.

По экономическим причинам пароли включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Аутентификация без передачи проверяющей стороне секретной информации, позволяющей проверить подлинность пользователя, называется строгой аутентификацией. Строгая аутентификация обычно реализуется совместно с криптографическими методами (шифрованием) с помощью «активных» аппаратных устройств. При этом секретная информация вообще не покидает устройства, которое пользователь предъявляет для аутентификации.

Системы разграничения доступа. Дискреционное и мандатное управление доступом.

Средства управления доступом – система разграничения доступа – позволяют определить и контролировать действия, которые субъекты ИС могут выполнять над ее объектами. Имеется в виду логическое управление доступом как основном механизме безопасности много-

пользовательских информационных систем, призванном обеспечить конфиденциальность и целостность объектов. В отличие от физического реализуется программными средствами.

Субъект – это активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы (например, пользователи, программы или процессы).

Объект – пассивный компонент системы, хранящий, принимающий или передающий информацию (например, папки и файлы, объекты базы данных). Доступ к объекту означает доступ к содержащейся в нем информации. Предполагается, что существует безошибочный способ различения объектов и субъектов.

С теоретической точки зрения доступ – взаимодействие между субъектом и объектом, в результате которого производится перенос информации между ними. Существуют два фундаментальных типа доступа: чтение – операция, результатом которой будет перенос информации от объекта к субъекту, и запись – операция, результатом которой является перенос информации от субъекта к объекту.

Санкционированный доступ к информации – доступ, не нарушающий установленные правила разграничения доступа. В настоящее время широко распространена двухуровневая схема назначения прав доступа (в сетевых ОС, СУБД), являющаяся развитием идеи ролевого управления.

3. Стеганографические и криптографические средства.

Задача защиты конфиденциальной информации от несанкционированного доступа решалась на протяжении всей истории человечества. Уже в древнем мире появилось два основных направления решения этой задачи, существующие и по сей день: криптография и стеганография.

Цель криптографии – скрытие содержимого сообщений за счет их шифрования. В отличие от этого при стеганографии скрывается сам факт существования тайного сообщения. При этом оба способа могут быть объединены и использованы для повышения эффективности защиты информации [7].

Стеганографические методы позволяют скрывать секретные сообщения путем их встраивания в послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Слово «стеганография» происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и означает буквально «тайнопись». Исторически это направление защиты секретных сообщений появилось первым, но затем во многом было вытеснено криптографией.

Историческими методами стеганографии можно назвать дощечки с воском; голову раба; полоски шелка; специальные чернила; использование известного смещения слов, предложений, абзацев, букв; выбор определенных позиций букв (акростих – частный случай этого метода); использование имитирующих функций (mimic-function).

Методы компьютерной стеганографии основаны на использовании специальных свойств компьютерных форматов. Направлениями приложений стеганографии являются сокрытие данных (сообщений), цифровые водяные знаки, заголовки.

Цифровые водяные знаки используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям. В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкополосным сигналом, в широком диапазоне частот маркируемого изображения.

Заголовки используются в основном для маркирования изображений в больших электронных хранилищах (библиотеках) цифровых изображений, аудио- и видеофайлов. В данном случае стеганографические методы используются не только для внедрения идентифицирующего заголовка, но и иных индивидуальных признаков файла. Внедряемые заголовки имеют небольшой объем, а предъявляемые к ним требования минимальны: заголовки должны вносить незначительные искажения и быть устойчивы к основным геометрическим преобразованиям.

Криптографические методы защиты информации. Цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. При использовании криптографических методов посторонний наблюдатель может довольно легко обнаруживать сами сообщения, при этом очевиден факт их секретности.

Людей, занимающихся криптографией, называют криптографами. Криптоаналитики – это специалисты в области криптоанализа – науки о методах вскрытия шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным. Раздел науки, объединяющий криптографию и криптоанализ, именуется криптологией.

Попытка проведения криптоанализа шифра называется криптоаналитической атакой. Успешная криптоаналитическая атака, в результате которой противнику становится известно содержание зашифрованного сообщения, называется взломом, или вскрытием шифра. Если противник узнал (например, выкрал или купил) ключ шифрования, то говорят, что ключ был скомпрометирован.

Различные криптографические алгоритмы обладают разной надежностью, чаще называемой стойкостью шифра. Стойкость шифра – это его способность противостоять криптоаналитическим атакам, т. е. степень гарантии того, что шифр невозможно взломать без знания ключа шифрования.

Таким образом, стойкость зависит от того, насколько легко криптоаналитик может взломать шифр. К сожалению, даже стойкий шифр не застрахован на практике от взлома. В большинстве случаев современные шифры бывают взломаны не из-за слабой математики или недостатков их внутренней структуры, а из-за ошибок и уязвимостей реализаций, а также из-за кражи ключей или получения их агентурными методами.

Криптографические системы можно разделить на два типа по стойкости: теоретически нераскрываемые (абсолютно стойкие, безусловно стойкие) и те, стойкость которых основана на вычислительной сложности методов вскрытия.

Требования к абсолютно стойкому алгоритму шифрования:

– длина ключа и длина открытого сообщения одинаковы;

– ключ используется только один раз;

– выбор ключа из ключевого пространства осуществляется равновероятно.

Временные ресурсы (время, необходимое для проведения определенных вычислений) приведены в табл. 3.3.

Таблица 3.3. Время жизни секретной информации [4]

Тип информации	Время жизни
Военная тактическая информация	Минуты/часы
Информация о выпуске продукции	Дни/недели
Долгосрочные бизнес-проекты	Годы
Производственные секреты	Десятилетия
Секрет создания водородной бомбы	> 40 лет
Информация о разведчиках	> 50 лет
Личная информация	> 50 лет
Дипломатическая тайна	> 65 лет
Информация о переписи населения	100 лет

4. Технология электронной подписи.

Назначение подписи заключается в неоспоримом доказательстве авторства какого-либо документа [8]. Электронная подпись (ЭП) – 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.

Электронная подпись – это не изображение собственноручной подписи, а специальные криптографические преобразования, обеспечивающие те же свойства, что и собственноручная подпись автора сообщения, т. е. гарантирующие аутентичность, неотрекаемость и целостность электронного документа (сообщения). В процессе электронного документооборота участвуют две стороны: отправитель и получатель сообщения. Отправитель подписывает сообщение (заверяет его своей электронной подписью), а получатель проверяет полученную вместе с сообщением подпись.

Современные алгоритмы электронной подписи являются вероятностными, т. е. вносят в подпись элемент случайности, что усиливает их стойкость к взлому.

Цифровые сертификаты.

Цифровой сертификат – электронный документ, который связывает открытый ключ с определенным пользователем или приложением. Информация сертификата подтверждает истинность открытого ключа и владельца соответствующего личного ключа.

Функции выдачи, отзыва и управления цифровыми сертификатами берет на себя служба сертификации (удостоверяющий центр, центр сертификации, Certification Authority – CA). Наряду с удостоверяющими центрами государственных структур существуют и коммерческие службы сертификации.

Служба сертификации упаковывает передаваемый ключ вместе с набором специальных удостоверений, подтверждающих истинность владельца ключа, а затем скрепляет весь подготовленный таким образом пакет своей цифровой подписью.

Сами центры сертификации тоже получают сертификаты своих ключей у центров более высокого уровня. В пакет включается и удостоверение, подтверждающее полномочия самой службы сертификации, а также ее идентификатор. Таким образом, служба сертификации выступает в качестве гаранта истинности связи между открытым ключом субъекта и идентифицирующей этот субъект информацией, т. е. позволяет соотнести открытые ключи с их владельцами.

Служба сертификации должна пользоваться доверием сторон, обменивающихся сообщениями, которые добровольно передают ей полномочия на проверку аутентичности отправителей сообщений. Если абоненты сети пользуются разными службами сертификации, нужно последовательно пройти через несколько служб, образующих иерархическую «цепь доверия», пока в ней не встретится узел, общий для ветвей обеих сторон.

5. Средства защиты в операционных системах. Сетевые технологии защиты.

Наиболее эффективными можно назвать средства защиты компьютерной информации на уровне операционной системы (ОС). От уровня реализации безопасности в каждой конкретной ОС во многом зависит и общая безопасность ИС [5]. Особенностью защищенной операционной системы является то, что в ней каждое выполняемое действие должно быть авторизовано. Авторизация – это проверка полномочий пользователя на выполнение каких-либо действий.

Защищенные системы, в том числе и ОС, базируются на трех основных процедурах: аутентификации, авторизации и администрировании и реализуют большинство типовых методов защиты информации: идентификация и аутентификация пользователей, контроль доступа,

регистрация событий, резервное копирование и восстановление данных, шифрование и т. д.

Оценка безопасности операционной системы складывается из функциональной и эксплуатационной безопасности. Функциональная безопасность характеризуется набором средств и механизмов защиты информации в составе операционной системы и дает качественную экспертную оценку эффективности механизмов защиты. Качественный уровень функциональной безопасности операционной системы может быть определен (подтвержден) при его сертификации по требованиям безопасности (например, при официальной сертификации ФСТЭК).

Основным механизмом безопасности ОС является управление доступом к ресурсам системы. Таковым может быть дискреционная или мандатная модель управления доступом. Также вспомогательными механизмами безопасности являются:

– идентификация и аутентификация;
– мониторинг, регистрация и учет;
– контроль целостности;
– резервное копирование и восстановление;
– криптографическая защита;
– удаление остаточной информации.

Операционная система может не реализовать отдельные вспомогательные механизмы либо реализовать их не в полном объеме. Эксплуатационная безопасность отражает реальный уровень безопасности, оцениваемый в процессе практического использования ОС. Она характеризуется количественными оценками, учитывающими следующие факторы:

– количество обнаруженных уязвимостей (за определенный промежуток времени);

– степень критичности обнаруженных уязвимостей (число критических уязвимостей);

– скорость устранения критических уязвимостей (среднее время, прошедшее с момента обнаружения уязвимости до ее устранения).

Основные принципы организации сетевой защиты. Угрозы информационной безопасности в сетях вызваны невозможностью обеспечить физическую защиту каналов передачи данных ввиду их протяженности и открытостью большинства сетевых протоколов.

На уровне сетевого программного обеспечения возможна реализация прослушивания сегмента локальной сети, перехвата сообщений на маршрутизаторе, создания ложного маршрутизатора, навязывания сообщений, отказа в обслуживании. Прослушивание сегмента локальной сети происходит в пределах одного и того же сегмента. При этом любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента. Поэтому, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента.

Перехват сообщений на маршрутизаторе. Если хакер имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту.

Создание ложного маршрутизатора. Путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям.

Навязывание сообщений. Отправляя в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера.

Отказ в обслуживании. Хакер отправляет в сеть сообщения специального вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя.

Семиуровневая модель взаимодействия. Компьютерные сети являются открытыми распределенными системами. Для таких систем определена эталонная семиуровневая модель взаимодействия. Вопросы информационной безопасности распределенных систем (сетей) достаточно полно и глубоко трактуются в технической спецификации X.800.

Выделяются следующие сервисы безопасности:

– аутентификация партнеров по общению (взаимная или односторонняя);

– управление доступом;

– конфиденциальность данных;

– целостность данных;

– неотрекаемость и аутентичность источника данных.

Функции безопасности могут быть реализованы на разных уровнях эталонной модели взаимодействия открытых систем.

Для реализации сетевых сервисов безопасности используются следующие механизмы и методы защиты информации: шифрование, подписывание сообщений, управление доступом.

Специальными технологиями сетевой защиты следует назвать экранирование и туннелирование. Экранирование выполняет функцию защиты внутреннего пространства сети (например, локальной сети организации) от внешних воздействий. Для организации экранирования используются межсетевые экраны. Туннелирование лежит в основе построения виртуальных частных сетей (VPN).

Защита на сетевом уровне – более универсальный подход, поскольку вне зависимости от протоколов наиболее высокого уровня, физической среды и технологии канального уровня передача данных невозможна в обход протокола IP. Таким образом, на сетевом уровне обеспечивается защита передаваемых данных всех вышележащих уровней.

Таким образом, проблема защиты информации в настоящее время стоит довольно остро. Используя знания о методах и средствах ее защиты, можно обезопасить как персональные данные человека и коммерческую тайну, так и сведения, составляющие государственную тайну.

Темы для обсуждения

1. Перечислите основные нормативно-правовые акты, определяющие и регламентирующие организацию защиты информации.

2. Укажите основные цели и задачи защиты информации.

3. Дайте определения доступности, целостности и конфиденциальности информации.

4. Приведите пример абсолютно защищенной информации.

5. Перечислите основные технологии защиты данных.

6. Раскройте классификацию методов и средств защиты информации.

7. Опишите особенности защиты информации на разных уровнях информационной системы.

8. Охарактеризуйте типовые методы защиты информации.

9. Сгруппируйте средства защиты информации.

10. Опишите систему программно-аппаратных средств защиты информации.

Задание для самоконтроля

Выполните тест

1. Информация может составлять коммерческую тайну, если:
   а) к ней нет свободного доступа на законном основании;
   б) содержится в учредительных документах;
   в) содержится в бухгалтерском балансе.
2. Не являются коммерческой тайной:
   а) сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью;
   б) сведения о научных разработках;
   в) сведения о персонале предприятия.
3. Конфиденциальность компьютерной информации – это:
   а) предотвращение проникновения компьютерных вирусов в память ПЭВМ;
   б) свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;
   в) безопасное программное обеспечение.
4. Банковская тайна – это информация:
   а) о банковском счете, вкладе, операциях по счету, о клиентах банка;
   б) сотрудниках банка;
   в) режиме работы банка.
5. Объектами профессиональной тайны НЕ являются:
   а) тайна страхования;
   б) врачебная тайна;
   в) бухгалтерский баланс.
6. Организационное обеспечение информационной безопасности – это:
   а) реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.;
   б) совокупность средств, обеспечивающих удобства работы пользователей;
   в) нормативные документы по информационной безопасности, требования которых являются обязательными в рамках сферы действия каждого подразделения.

7. Найдите из списка угрозу случайной потери информации:

а) использование антивирусных программ;

б) возможность отмены неверного действия;

в) профилактические меры по уменьшению вероятности заражения программ;

г) архивация файлов.

8. Чтобы предотвратить угрозы конфиденциальности (несанкционированный доступ) данных пользователи применяют:

а) установку специальных атрибутов документа, например «Только чтение»;

б) возможность отмены неверного действия;

в) шифрование информации;

г) запрос на подтверждение выполненных команд.

9. К методам защиты информации относится угроза заражения вирусом, найдите из списка пункт, который раскрывает данный метод:

а) использование антивирусных программ;

б) архивация файлов;

в) резервное копирование данных;

г) электронные замки.

10. Требования по защите информации в автоматизированных информационных системах (АИС) формируются вокруг необходимости оградить конфиденциальные данные от утечек или искажений. Угрозы имеют различный генезис: информация страдает от (тест на множественный выбор):

а) техногенных аварий, повреждающих оборудование;

б) копирования данных;

в) архивации файлов;

г) действий хакеров и вредоносных программ.

11. Определите, что НЕ является методом защиты информации:

а) резервное копирование;

б) архивирование данных;

в) маскировка;

г) специализированные программы.

12. Одним из методов защиты информации можно назвать резервное копирование данных. Определите, что НЕ относится к данному методу:

а) копирование личных и рабочих файлов;

б) копирование IP адресов компьютеров;

в) копирование операционной системы;

г) копирование программ.

13. Взлом серверов является одним из способов несанкционированного проникновения в информационную среду. Какой из методов защиты будет наиболее существенным для данного случая:

а) специализированные программы;

б) резервное копирование;

в) управление доступом;

г) шифрование.

14. Что находится под защитой государства от несанкционированного доступа к различным данным (тест на множественный выбор):

а) программные средства;

б) спутниковые системы связи;

в) платежные реквизиты различных организаций;

г) персональные данные граждан.

15. Определите, что или кто выступает источником угроз информационной безопасности (тест на множественный выбор):

а) отдельные физические лица (хакеры);

б) недостаточное количество квалифицированных кадров;

в) низкая компьютерная грамотность пользователей;

г) небольшое количество персональных компьютеров в системе образования.

Библиографический список

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М. : Изд-во стандартов, 2006. – 56 с.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.10.2022).

3. Шубин, М. А. Методы и средства защиты информации [Электронный ресурс] / М. А. Шубин // Материалы X Международной научной конференции [Электронный ресурс]. – Режим доступа: https://scienceforum.ru/2018/article/2018005046 (дата обращения: 30.10.2022).

4. Сухостат, В. В. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / В. В. Сухостат, И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с. – Режим доступа: http://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informaczionnoj-bezopasnosti.pdf (дата обращения: 25.10.2022).

5. Васильева, И. Н. Управление комплексной информационной безопасностью информационных технологий : учеб. пособие / И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2022. – 90 с.

6. Зенков, А. В. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие для вузов / А. В. Зенков. – М. : Юрайт, 2022. – 104 с. – (Высшее образование). – Режим доступа: https://urait.ru/bcode/497002 (дата обращения: 26.10.2022).

7. Грибунин, В. Г. Цифровая стеганография [Электронный ресурс] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – Режим доступа: https://royallib.com/read/gribunin_vadim/tsifrovaya_steganografiya.html#0 (дата обращения: 20.10.2022).

8. Васильева, И. Н. Криптографические методы защиты информации [Электронный ресурс] : учеб. для вузов / И. Н. Васильева. – М. : Юрайт, 2022. – 349 с. – (Высшее образование). – Режим доступа: https://urait.ru/bcode/489919 (дата обращения: 19.10.2022).

Глава 4. ПРЕДНАМЕРЕННЫЕ И НЕПРЕДНАМЕРЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И БОРЬБА С НИМИ

4.1. Непреднамеренные искусственные угрозы и меры по их нейтрализации

Угрозы безопасности информации – это некая совокупность факторов и условий, которые создают опасность в отношении защищаемой информации. С точки зрения методов воздействия на информацию различают естественные и искусственные угрозы.

К естественным угрозам безопасности информации относят стихийные бедствия, явления и несчастные случаи, которые не зависят от человека: пожары, наводнения, ураганы, удары молний и т. д. В качестве мер противодействия данному типу угроз выступает обеспечение зданий и сооружений, которые используются в работе информационных систем, инженерно-техническими системами безопасности (системами пожарной сигнализации, пожаротушения, защиты от импульсных перенапряжений, защиты от протечки воды и т. д.).

К искусственным угрозам безопасности информации относят действия со стороны человека. Различают непреднамеренные и преднамеренные искусственные угрозы.

Непреднамеренные угрозы – это действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла. Данный вид угроз практически не поддается контролю, так как его реализуют внутренние нарушители информационной безопасности (т. е. лица, имеющие право доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей) [1]:

1) разработчики программных, программно-аппаратных средств;

2) лица, обеспечивающие поставку программных, программно-аппаратных средств, а также обеспечивающих систем;

3) поставщики вычислительных услуг, услуг связи;

4) лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

5) авторизованные пользователи систем и сетей;

6) системные администраторы и администраторы безопасности;

7) лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.).

Рассмотрим основные пути реализации непреднамеренных искусственных угроз и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба.

Во-первых, реализация непреднамеренных искусственных угроз может быть вызвана действиями сотрудников (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и подобное), которые приводят:

– к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств;

– отключению оборудования или изменению режимов работы устройств и программ;

– разрушению информационных ресурсов системы.

В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба выступают:

– организационные меры (регламентация действий, введение запретов);

– применение физических средств, препятствующих неумышленному совершению нарушения;

– применение технических (аппаратно-программных) средств разграничения доступа к ресурсам;

– резервирование критичных ресурсов.

Во-вторых, реализация непреднамеренных искусственных угроз может быть вызвана несанкционированным запуском технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и подобное).

В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба применяют:

– организационные меры (удаление всех потенциально опасных программ с дисков автоматизированных рабочих мест);

– технические (аппаратно-программные) средства разграничения доступа к технологическим и инструментальным программам на дисках автоматизированных рабочих мест).

В-третьих, реализация непреднамеренных искусственных угроз может быть вызвана несанкционированным внедрением и использованием неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т. п.). В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба применяют:

– организационные меры (введение запретов);

– технические (аппаратно-программные) средства, препятствующие несанкционированному внедрению и использованию неучтенных программ.

В-четвертых, реализация непреднамеренных искусственных угроз может быть вызвана непреднамеренным заражением компьютера вирусами. В качестве мер по нейтрализации данного способа реализации

непреднамеренных угроз и снижению возможного наносимого ущерба применяют:

– организационные меры (регламентация действий, введение запретов);

– технические (аппаратно-программные) средства, препятствующие заражению компьютеров компьютерными вирусами;

– технологические меры (применение специальных программ обнаружения и уничтожения вирусов).

В-пятых, реализация непреднамеренных искусственных угроз может быть вызвана непреднамеренной передачей или утратой атрибутов разграничения доступа (паролей, ключей шифрования или ключей ЭЦП, идентификационных карточек, пропусков).

В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба предусматривают:

– организационные меры (регламентация действий, введение запретов, усиление ответственности);

– применение физических средств обеспечения сохранности паролей, ключей шифрования или ключей ЭЦП, идентификационных карточек, пропусков.

В-шестых, реализация непреднамеренных искусственных угроз может быть вызвана игнорированием организационных ограничений (установленных правил) при работе в информационной системе. В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба используют:

– организационные меры (усиление ответственности и контроля);

– дополнительные физические и технические средства защиты.

В-седьмых, реализация непреднамеренных искусственных угроз может быть вызвана некомпетентным использованием, настройкой или неправомерным отключением средств защиты персоналом, ответственным за информационную безопасность.

В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба выступают организационные меры (обучение персонала, усиление ответственности и контроля).

В-восьмых, реализация непреднамеренных искусственных угроз может быть вызвана вводом ошибочных данных. В качестве мер по нейтрализации данного способа реализации непреднамеренных угроз и снижению возможного наносимого ущерба выступают:

1) организационные меры (усиление ответственности и контроля);

2) технологические меры контроля за ошибками операторов ввода данных.

В России внутренние нарушители, которые реализуют непреднамеренные угрозы информационной безопасности, являются главной угрозой для информационных активов бизнеса и государственных структур. Тем не менее для минимизации данной угрозы у компаний и организаций есть все возможности. Необходимо внедрять и правильно настраивать современные системы контроля за действиями персонала, средства управления доступом, продвинутую аналитику на основе машинного обучения и, конечно, проводить регулярные мероприятия для повышения цифровой грамотности сотрудников [2].

4.2. Преднамеренные искусственные угрозы и меры по их нейтрализации

Преднамеренные угрозы – это действия по выводу информационных систем из строя, проникновению в информационные системы и несанкционированному доступу к информации, совершаемые людьми с корыстными целями, по принуждению, из желания отомстить и т. п.

Данный вид угроз реализуется либо внутренними, либо внешними нарушителями информационной безопасности (лица, не имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации) с использованием программных, программно-аппаратных средств или без использования таковых.

Среди внешних нарушителей можно выделить следующие их виды, каждый из которых может преследовать свои цели реализации преднамеренных угроз безопасности информации:

1) специальные службы иностранных государств (нанесение ущерба государству в области обеспечения обороны, безопасности и

правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса);

2) террористические, экстремистские группировки (совершение террористических актов, угроза жизни граждан, нанесение ущерба отдельным сферам деятельности или секторам экономики государства, дестабилизация общества и деятельности органов государственной власти, организаций);

3) криминальные структуры (получение финансовой или иной материальной выгоды, желание самореализации или подтверждения статуса);

4) отдельные физические лица (хакеры) (получение финансовой или иной материальной выгоды, желание самореализации или подтверждения статуса);

5) конкурирующие организации (получение конкурентных преимуществ, финансовой или иной материальной выгоды);

6) бывшие работники (получение финансовой или иной материальной выгоды, месть за ранее совершенные действия).

Внутренние нарушители при реализации угроз безопасности информации, как правило, преследуют в качестве целей:

1) получение финансовой или иной материальной выгоды;

2) получение конкурентных преимуществ;

3) любопытство или желание самореализации (подтверждение статуса);

4) месть за ранее совершенные действия.

Рассмотрим основные пути реализации преднамеренных искусственных угроз и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба.

Во-первых, реализация преднамеренных искусственных угроз может быть вызвана:

– физическим разрушением или выводом из строя всех или отдельных наиболее важных компонентов автоматизированной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.);

– отключением или выводом из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т. п.).

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба выступают:

– организационные меры (регламентация действий, введение запретов);

– применение физических средств, препятствующих неумышленному совершению нарушения;

– резервирование критичных ресурсов;

– обеспечение личной безопасности сотрудников.

Во-вторых, реализация преднамеренных искусственных угроз может быть вызвана:

– внедрением агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

– вербовкой (путем подкупа, шантажа, угроз и т. п.) пользователей, имеющих определенные полномочия по доступу к защищаемым ресурсам.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба предусматривают:

– организационные меры (подбор, расстановка и работа с кадрами, усиление контроля и ответственности);

– автоматическую регистрацию действий персонала.

В-третьих, реализация преднамеренных искусственных угроз может быть вызвана:

– хищением носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

– хищением производственных отходов (распечаток, записей, списанных носителей информации и т. п.)

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба выступают организационные меры (организация хранения и использования носителей с защищаемой информацией).

В-четверых, реализация преднамеренных искусственных угроз может быть вызвана:

– несанкционированным копированием носителей информации;

– чтением остаточной информации из оперативной памяти и с внешних запоминающих устройств.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба выступают:

– организационные меры (организация хранения и использования носителей с защищаемой информацией);

– применение технических средств разграничения доступа к защищаемым ресурсам и автоматической регистрации получения твердых копий документов.

В-пятых, реализация преднамеренных искусственных угроз может быть вызвана незаконным получением паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т. д.) с последующей маскировкой под зарегистрированного пользователя.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба применяют:

– организационные меры (регламентация действий, введение запретов, работа с кадрами);

– технические средства, препятствующие внедрению программ перехвата паролей, ключей и других реквизитов.

В-шестых, реализация преднамеренных искусственных угроз может быть вызвана несанкционированным использованием автоматизированного рабочего места пользователей, владеющих уникальными физическими характеристиками, такими как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба предусматривают:

– организационные меры (строгая регламентация доступа в помещения и допуска к работам на данных автоматизированных рабочих местах);

– применение физических и технических средств разграничения доступа.

В-седьмых, реализация преднамеренных искусственных угроз может быть вызвана несанкционированной модификацией программного обеспечения, а именно: внедрением программных «закладок» и «вирусов» («троянских коней» и «жучков»), т. е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяют преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования системы.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба применяют:

– организационные меры (строгая регламентация допуска к работам);

– физические и технические средства разграничения доступа, препятствующие несанкционированной модификации аппаратно-программной конфигурации автоматизированного рабочего места;

– средства контроля целостности программ.

В-восьмых, реализация преднамеренных искусственных угроз может быть вызвана перехватом данных, передаваемых по каналам связи, и их анализом с целью получения конфиденциальной информации и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба выступают:

– физическая защита каналов связи;

– применение средств криптографической защиты передаваемой информации;

– применение средств электронной подписи.

В-девятых, реализация преднамеренных искусственных угроз может быть вызвана вмешательством в процесс функционирования ин-

формационных систем из сетей общего пользования с целью несанкционированной модификации данных, доступа к конфиденциальной информации, дезорганизации работы подсистем и т. п.

В качестве мер по нейтрализации данного способа реализации преднамеренных угроз и снижению возможного наносимого ущерба применяют:

– организационные меры (регламентация подключения и работы в сетях общего пользования);

– специальные технические средства защиты (межсетевые экраны, средства контроля защищенности и обнаружения атак на ресурсы системы и т. п.).

В последние годы на фоне успехов в цифровизации отмечается активизация внешних нарушителей: когда структурированных хранилищ информации становится больше, это неизбежно привлекает киберпреступников.

Более того, в пандемию коронавируса значительно усложнился вектор ряда инцидентов; все чаще приходится говорить об использовании злоумышленниками многоступенчатых схем похищения информации, когда в сговор вступают внутренний и внешний злоумышленники. В результате внутренний нарушитель создает условия для успешных действий внешних или совершает копирование и передачу сам, переводя акцент на внешних нарушителей, тем самым избегая внимания служб безопасности, а продажу данных осуществляют его «сотоварищи» под видом хакеров [2].

4.3. Вредоносные программы и антивирусы

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы [3].

Соответственно несанкционированное воздействие на информацию – это воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Таким образом, вредоносность программы определяется ее функциональным предназначением, а именно возможностью оказывать неправомерное (несанкционированное) воздействие исключительно на компьютерные данные и системы [4].

Для того чтобы программа считалась вредоносной, она должна соответствовать следующим трем критериям [5]:

1) направленность на уничтожение информации;

2) несанкционированный характер работы;

3) оказание неправомерного воздействия на информационные ресурсы.

Однако такое толкование вредоносности компьютерной программы, к сожалению, имеет свои изъяны. Например, оно не позволяет отнести к таковым программы-шпионы (Spyware), целью которых является не причинение вреда информационным активам или инфраструктуре, а собирание сведений об активности пользователя в сети Интернет (о посещаемых сайтах, совершаемых покупках и т. п.); программы «злые шутки» (Bad Jokes), так называемые «вирусные конструкторы» (программы, предназначенные не для осуществления атак на компьютерные ресурсы, а для генерирования новых вирусов) [6].

При общепринятом подходе нельзя отнести к вредоносным также программы, объективно приспособленные к совершению преступлений, но выполненные на основе легального программного обеспечения. Поэтому существует более широкое определение термина «вредоносная программа» как компьютерной программы, созданной (в том числе путем модификации легальной программы) для осуществления противоправной деятельности.

Вредоносные программы довольно разнообразны и могут быть разделены на следующие подкатегории: вирусы и черви, троянские программы и вредоносные утилиты.

Компьютерный вирус – вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Основная цель вируса – его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов – удаление файлов и операционной си-

стемы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтенных тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В настоящее время не существует единой системы классификации и именования вирусов. Основными классификационными признаками могут выступать:

1) вид поражаемых объектов (файловые вирусы, в том числе паразитирующие и «спутники», загрузочные и сценарные вирусы, макровирусы, поражающие исходный код вирусы);

2) поражаемые операционная система и платформа (DOS, Windows, Unix, Linux, Android);

3) используемая технология (полиморфные вирусы, стелс-вирусы, руткиты);

4) дополнительная вредоносная функциональность (бэкдоры, кейлогеры, шпионы, ботнеты и др.).

Файловый вирус – компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой операционной системы. Объектом вирусного поражения могут выступать исполняемые двоичные файлы, файлы динамических библиотек, драйверы, командные файлы и т. п.

Заражая файл, вирус может внедриться в его начало, конец или середину. Чтобы скрыть свое присутствие в системе, файловый вирус может предварительно сохранить дату и время последней модификации и значения атрибутов заражаемого файла, восстановив эти данные уже после заражения. После того как вирус получил управление, он выполняет следующие действия:

1) восстанавливает в оперативной памяти компьютера исходную программу (или ее необходимую часть) для последующего ее выполнения;

2) осуществляет дальнейшее заражение, инфицируя другие файлы или оперативную память компьютера;

3) выполняет иные деструктивные действия, если это предусмотрено алгоритмом.

При этом все действия вируса, как правило, незаметны для пользователя программы.

Загрузочный вирус – компьютерный вирус, записывающийся в первый сектор диска и выполняющийся при загрузке компьютера с идущих после главной загрузочной записи, но до первого загрузочного сектора раздела [7]. Перехватив обращения к дискам, вирус либо продолжает загрузку операционной системы, либо нет (MBR-Locker). Размножается вирус записью в загрузочную область других накопителей компьютера.

Простейшие загрузочные вирусы, находясь в памяти зараженного компьютера, обнаруживают в нем незараженный диск и производят следующие действия:

1) выделяют некоторую область диска и делают ее недоступной для операционной системы;

2) замещают программу начальной загрузки в загрузочном секторе диска, копируя корректную программу загрузки, а также свой код, в выделенную область диска;

3) организуют передачу управления так, чтобы вначале выполнялся код вируса и лишь затем – программа начальной загрузки.

Макровирус – это разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие. Большая часть таких вирусов написана для MS Word.

Стелс-вирусы пользуются слабой защищенностью некоторых операционных систем и заменяют некоторые их компоненты (драйверы дисков, прерывания) таким образом, что вирус становится невидимым (прозрачным) для других программ.

Полиморфные вирусы содержат алгоритм порождения дешифрованных тел вирусов, непохожих друг на друга. При этом в алгоритмах дешифрования могут встречаться обращения практически ко всем командам процессора Intel и даже использоваться некоторые специфические особенности его реального режима функционирования.

Сетевой червь – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.

Все механизмы распространения червей делятся на две большие группы. Использование уязвимостей и ошибок администрирования в программном обеспечении, установленном на компьютере. Такие черви способны распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме. Используя средства так называемой социальной инженерии, провоцируется запуск вредоносной программы самим пользователем. Данный метод широко применяется в спам-рассылках, социальных сетях и т. д.

Иногда встречаются черви с целым набором различных векторов распространения, стратегий выбора жертвы и даже эксплойтов под различные операционные системы.

Классификация программ-червей включает [8]:

1) почтовые программы-черви (Email-Worms) – вредоносные программы, использующие для своего распространения электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо веб-сервере;

2) программы-черви, использующие интернет-пейджеры (IM-Worms), – вредоносные программы, которые используют для своего распространения рассылку на обнаруженные контакты из контакт-листа интернет-пейджера (программы ICQ, MSN Messenger, Yahoo Messenger, Google Talk, AOI. Instant Messenger, Trillian, Miranda, QIP и др.);

3) программы-черви в IRC-каналах (IRC-Worms) – вредоносные программы, которые распространяются, используя среду IRC-каналов (Internet Relayed Chat channels);

4) классические сетевые программы-черви (Net-Worms) – вредоносные программы, использующие для своего распространения уязвимости в операционных системах и прикладном ПО или распространяющиеся с помощью копирования себя на сетевые ресурсы;

5) программы-черви для файлообменных сетей (P2P-Worms) – вредоносные программы, использующие для своего распространения P2P-сети (распространяющиеся с помощью программ eMule, eDonkey, Kazzaa, DC++, BitTorrent, Gnutella, FastTrack и др.);

6) вирусные черви – вредоносные программы, которые незаметно перемещаются между узлами вычислительной сети, не нанося никакого вреда до тех пор, пока не доберутся до целевого узла. В нем программа размещается и перестает размножаться.

Троянская вирусная программа – разновидность вредоносной программы, проникающей в компьютер под видом легитимного программного обеспечения в отличие от вирусов и червей, которые распространяются самопроизвольно.

Троянские программы могут производить следующие действия:

1) удаление данных;

2) блокирование данных;

3) изменение данных;

4) копирование данных;

5) замедление работы компьютеров и компьютерных сетей.

Троянские программы можно классифицировать в соответствии с типом действий, выполняемых ими на компьютере: бэкдор, кейлогеры, эксплойты, руткиты, шпионы, ботнеты и др.

Бэкдор – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом. Основная цель бэкдора – скрытное и быстрое получение доступа к данным, в большинстве случаев – к зашифрованным и защищенным. Например, бэкдор может быть встроен в алгоритм шифрования для последующей прослушки защищенного канала злоумышленником.

Кейлогер – программное обеспечение, регистрирующее различные действия пользователя – нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.

Эксплойты – программы, которые содержат данные или исполняемый код, способные использовать уязвимость в работающих на компьютере приложениях. Основной целью выполнения эксплойтов может стать повышение привилегий в целевой системе или отказ в обслуживании.

Нередко эксплойты объединяются в эксплойт-пак (эксплойт-pack) или эксплойт-кит (эксплойт-kit), т. е. набор эксплойтов. Функциональность этих наборов предполагает помимо собственно эксплуата-

ции уязвимости проведение предварительного уточнения среды функционирования объекта воздействия: определение того, не выполняется ли ОС в среде виртуализации, присутствует ли в атакуемой среде отладчик, какие установлены антивирусные средства.

В качестве «полезной нагрузки» эксплойта (функции, выполняемой после эксплуатации уязвимости и проникновения в систему) используется shell-код, предоставляющий атакующему доступ к командному интерпретатору в целевой системе.

Руткит – набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), обеспечивающих:

1) маскировку объектов (процессов, файлов, каталогов, драйверов);

2) управление (событиями, происходящими в системе);

3) сбор данных (параметров системы).

Основная цель руткитов – предотвратить обнаружение вредоносных программ, чтобы увеличить время работы этих программ на зараженном компьютере. В систему руткит может быть установлен различными способами: загрузка посредством эксплойта, в исходном коде или ресурсах программного продукта.

По принципу действия различают следующие виды руткитов:

1) изменяющие алгоритмы выполнения системных функций;

2) изменяющие системные структуры данных.

Шпионы – вредоносные программы, которые без согласия пользователя собирают и передают информацию с устройства.

Ботнет – компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании.

Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов и профилактики – предотвращения заражения (модификации) файлов или операционной

системы вредоносным кодом. Для защиты от вирусов используют три группы методов [9]:

1) методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд;

2) методы, основанные на отслеживании поведения программ при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции;

3) методы регламентации порядка работы с файлами и программами. Они относятся к административным мерам обеспечения безопасности.

Метод сканирования сигнатур основан на поиске в файлах уникальной последовательности байтов – сигнатуры, характерной для определенного вируса [10]. Для каждого вновь обнаруженного вируса специалистами антивирусной лаборатории выполняется анализ кода, на основании которого определяется его сигнатура. Полученный кодовый фрагмент помещают в специальную базу данных вирусных сигнатур, с которой работает антивирусная программа.

Достоинством данного метода считается относительно низкая доля ложных срабатываний, а главным недостатком – принципиальная невозможность обнаружения в системе нового вируса, для которого отсутствует сигнатура в базе данных антивирусной программы, поэтому требуется своевременная актуализация базы данных сигнатур.

Метод контроля целостности основывается на том, что любое неожиданное и беспричинное изменение данных на диске воспринимается подозрительным событием, требующим особого внимания антивирусной системы. Вирус обязательно оставляет свидетельства своего пребывания (изменение данных существующих файлов (особенно системных или исполняемых), появление новых исполняемых файлов и т. д.). Факт изменения данных – нарушение целостности – легко устанавливается путем сравнения контрольной суммы (дайджеста), заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они не совпадают, значит, целостность нарушена и имеются все

основания провести для этого кода дополнительную проверку, например, путем сканирования вирусных сигнатур.

Указанный метод работает быстрее метода сканирования сигнатур, поскольку подсчет контрольных сумм требует меньше вычислений, чем операции побайтового сравнения кодовых фрагментов, кроме того, он позволяет обнаруживать следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур.

Метод сканирования подозрительных команд (эвристическое сканирование, эвристический метод) основан на выявлении в сканируемом файле некоторого числа подозрительных команд и(или) признаков подозрительных кодовых последовательностей (например, команда форматирования жесткого диска или функция внедрения в выполняющийся процесс или исполняемый код). После этого делается предположение о вредоносной сущности файла и предпринимаются дополнительные действия по его проверке. Этот метод обладает хорошим быстродействием, но довольно часто он не способен выявлять новые вирусы.

Метод отслеживания поведения программ принципиально отличается от методов сканирования содержимого файлов, упомянутых ранее. Этот метод основан на анализе поведения запущенных программ и сравнивается с поимкой преступника «за руку» на месте преступления.

Антивирусные средства данного типа часто требуют активного участия пользователя, призванного принимать решения в ответ на многочисленные предупреждения системы, значительная часть которых может оказаться впоследствии ложными тревогами. Частота ложных срабатываний (подозрение на вирус для безвредного файла или пропуск вредоносного файла) при превышении определенного порога делает этот метод неэффективным, а пользователь может перестать реагировать на предупреждения или выбрать оптимистическую стратегию (разрешать все действия всем запускаемым программам или отключить данную функцию антивирусного средства).

При использовании антивирусных систем, анализирующих поведение программ, всегда существует риск выполнения команд вирусного кода, способных нанести ущерб защищаемому компьютеру или сети. Для устранения подобного недостатка позднее был разработан метод эмуляции (имитации), позволяющий запускать тестируемую

программу в искусственно созданной (виртуальной) среде, которую часто называют песочницей (sandbox), без опасности повреждения информационного окружения. Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных вредоносных программ.

Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы:

1) детекторы (выявляют вредоносные программы);

2) фаги (нейтрализуют вредоносные программы);

3) вакцины (обеспечивают предупреждение заражения вирусом);

4) прививки (маркируют зараженные файлы метками вирусов);

5) ревизоры (следят за состоянием файловой системы);

6) мониторы (обеспечивают перехват потенциально опасных прерываний, характерных для вирусов).

4.4. Актуальные способы реализации (возникновения) угроз безопасности информации

В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях, – актуальные способы реализации (возникновения) угроз безопасности информации [11].

Исходными данными для определения актуальных способов реализации (возникновения) угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов компьютерных атак, содержащихся в базах данных и иных источниках, опубликованных в сети Интернет (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на системы и сети (в части сведений о составе и архитектуре, о группах пользователей и типах их доступа и уровней полномочий, о внешних и внутренних интерфейсах);

г) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с Методикой оценки угроз безопасности, утвержденной ФСТЭК России;

д) объекты воздействия угроз безопасности информации и соответствующие им виды воздействия, определенные в соответствии с настоящей Методикой;

е) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности.

К основным способам реализации (возникновения) угроз безопасности информации относятся:

1) использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

2) внедрение вредоносного программного обеспечения;

3) использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;

4) установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

5) формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

6) перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

7) инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

8) нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

9) ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования систем и сетей.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с настоящей Методикой, и применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Рассмотрим основные тактики и соответствующие им типовые техники, используемые для построения сценариев реализации угроз безопасности информации.

Первая тактическая задача, которая стоит перед нарушителем, – сбор информации о системах и сетях, т. е. получение любой технической информации, которая может оказаться полезной в ходе реализации угроз безопасности информации. Сбор информации может выполняться с использованием одной или более из перечисленных ниже техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжение атаки:

1) сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций;

2) сбор информации о подключенных к публичным системам и сетям устройствах и их службе при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможными уязвимыми версиями прошивок;

3) пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий программного обеспечения этих служб и в некоторых случаях – идентификационной информации пользователей;

4) направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств

с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера nmap;

5) сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера;

6) сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора. Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые серверы;

7) сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking;

8) сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера;

9) сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей. Пример: получение хэшей паролей из /etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства;

10) кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы);

11) сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга;

12) сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа),

в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами;

13) сбор информации через получение доступа к системам физической безопасности и видеонаблюдения;

14) сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации;

15) поиск и покупка баз данных идентификационной информации, скомпрометированных паролей и ключей на специализированных нелегальных площадках;

16) сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров;

17) пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах;

18) сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах;

19) сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах;

20) техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах.

Следующая тактическая задача, которая стоит перед нарушителем, – получение первоначального доступа к компонентам систем и сетей, т. е. нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий.

Получение доступа может выполняться в несколько шагов с использованием одной или более из перечисленных ниже техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки:

1) использование внешних сервисов организации в сетях публичного доступа (Интернет) (примеры: доступ к веб-серверу, расположенному в сети организации; доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации);

2) использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра (примеры: доступ к датчикам автономной системы дистанционного контроля давления газа участка газопровода; доступ к умному счетчику, расположенному на частном объекте, как к части инфраструктуры поставщика электроэнергии; доступ к интерфейсу управления камеры видеонаблюдения через сети ближнего действия);

3) эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке. Пример: обход межсетевого экрана путем эксплуатации уязвимостей реализации правил фильтрации;

4) использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке;

5) эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке (примеры: эксплуатация уязвимостей веб-сервера с целью выполнения произвольного кода в контексте этого сервера; эксплуатация уязвимостей операционной системы устройства человекомашинного интерфейса автоматизированной системы управления с целью внедрения средств получения вводимых на этом устрой-

стве паролей доступа; эксплуатация уязвимостей браузера вредоносными скриптами при посещении пользователем вредоносного или скомпрометированного веб-сайта);

6) использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок;

7) использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением, в том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций (примеры: передача флеш-носителя в комплекте материалов выездного мероприятия; подмена USB-адаптера беспроводной клавиатуры, схожего внешне, но реализующего функции сбора и передачи данных устройством);

8) применение методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы;

9) несанкционированное подключение внешних устройств. Пример: несанкционированное подключение точки доступа Wi-Fi;

10) несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц и др.);

11) несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд);

12) использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа. Пример: использование доступа третьей доверенной стороны (поставщики ИТ-услуг, поставщики услуг безопасности);

13) реализация атаки типа «человек посередине» для осуществления доступа, например NTLM/SMB Relaying атаки;

14) доступ путем эксплуатации недостатков систем биометрической аутентификации. Пример: демонстрация фотографии для аутентификации через функцию распознавания лиц.

Следующая тактическая задача, которая стоит перед нарушителем – внедрение и исполнение вредоносного программного обеспечения в системах и сетях, т. е. нарушитель, получив доступ к узлу сети или системы, стремится внедрить в его программную среду инструментальные средства, необходимые ему для дальнейших действий.

Внедрение и исполнение вредоносного программного обеспечения в системах и сетях может выполняться в несколько шагов с использованием одной или более из перечисленных ниже техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки:

1) автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с применением методов социальной инженерии;

2) активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программно-аппаратное обеспечение систем и сетей;

3) автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение;

4) копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами;

5) эксплуатация уязвимостей типа «удаленное исполнение программного кода» (RCE, Remotecodeexecution);

6) автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных;

7) подмена файлов легитимных программ и библиотек непосредственно в системе;

8) подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи;

9) подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации

о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями;

10) подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах;

11) компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (так называемый «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами;

12) компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы;

13) компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы;

14) планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т. п.;

15) планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии;

16) запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (так называемая техника проксирования запуска), а также через средства запуска кода элементов управления

ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL (примеры: запуск MSI-файлов в операционной системе Windows при помощи утилиты msiexec; использование утилит Regsvr32.exe (Microsoft Windows Register Server) и odbcconf.exe для проксирования исполнения кода библиотек dll в операционной системе Windows посредством внесения изменений в реестр операционных систем).

Следующая тактическая задача, которая стоит перед нарушителем, – закрепление (сохранение доступа) в системе или сети, т. е. нарушитель, получив доступ к узлу сети с помощью некоторой последовательности действий, стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного управления узлом, изменяет настройки средств защиты и другие действия).

Закрепление (сохранение доступа в системе) может производиться с использованием одной или более из перечисленных ниже техник:

1) несанкционированное создание учетных записей или кража существующих учетных данных;

2) использование штатных средств удаленного доступа и управления операционной системой;

3) скрытая установка и запуск средств удаленного доступа и управления операционной системой, а также внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода;

4) маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки);

5) внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети;

6) компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков;

7) резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей.

Следующая тактическая задача, стоящая перед нарушителем, – управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ, т. е. нарушитель, внедрив вредоносное программное обеспечение или обеспечив постоянное присутствие на узле сети, стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействие между скомпрометированным узлом и сервером управления, который может быть размещен в сети Интернет или в инфраструктуре организации.

Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ, может производиться нарушителем с использованием одной или более из перечисленных ниже техник для управления труднодоступными компонентами или для реализации резервных каналов управления:

1) удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования. Пример: использование средств удаленного управления RMS/teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников;

2) использование штатных средств удаленного доступа и управления операционной системой;

3) коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, размещенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.);

4) коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств;

5) управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах;

6) проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание

обнаружения (примеры: использование скомпрометированных систем в той же сети, для которых разрешен доступ в Интернет, в качестве прокси-серверов; использование инфраструктуры сети TOR для проксирования запросов к серверам управления; использование одного коммуникационного протокола для запроса, и другого – для ответа на запрос);

7) туннелирование трафика управления через VPN;

8) туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнение протоколов DNS, ICMP или других;

9) управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети;

10) использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления;

11) передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т. п.;

12) передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т. п.;

13) динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и тому подобное по известному алгоритму во избежание обнаружения.

Следующая тактическая задача, которая стоит перед нарушителем, – повышение привилегий по доступу к компонентам систем и сетей, т. е. нарушитель, получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, стремится повысить полученные привилегии и получить контроль над узлом.

Повышение привилегий по доступу к компонентам систем и сетей может производиться с использованием одной или более из перечисленных ниже техник, пока нарушитель не получит достаточно привилегий для реализации другой тактики в продолжение атаки:

1) получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных

в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими;

2) подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи;

3) эксплуатация уязвимостей ПО к повышению привилегий. Пример: эксплуатация уязвимости драйвера службы печати, позволяющей выполнить код с привилегиями системной учетной записи через доступ к этому драйверу из приложения, запущенного от имени непривилегированного пользователя;

4) эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи);

5) манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций. Пример: кража и подделка cookie сессии для получения авторизованного доступа к веб-интерфейсу управления сетевым устройством;

6) обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима. Пример: обход UserAccountControl в операционной системе Windows;

7) использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями;

8) эксплуатация уязвимостей, связанных с отдельным и, вероятно, менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе), для непривилегированных учетных записей. Пример: подмена на диске бинарных файлов или скриптов, предназначенных для исполнения в привилегированном контексте, приложением, исполняющимся в непривилегированном контексте;

9) эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т. п.) для исполнения кода вне этой среды. Пример: эксплуатация уязвимости обработки буфера данных в рамках песочницы, реализуемой браузером для ограничения работы мобильного кода (Javascript) с последующим выполнением кода в контексте процесса браузера.

Следующая тактическая задача, стоящая перед нарушителем, – сокрытие действий и применяемых при этом средств от обнаружения, т. е. нарушитель стремится затруднить применение мер защиты информации, которые способны помешать его действиям или обнаружить их.

Сокрытие действий и применяемых при этом средств от обнаружения может производиться с использованием одной или более из перечисленных ниже техник для сокрытия разных свидетельств компрометации системы или для более эффективного сокрытия:

1) использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения. Пример: использование популярной утилиты PsExec для ОС Windows как администраторами, так и нарушителями;

2) очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей;

3) удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей;

4) отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов;

5) отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса;

6) подделка данных вывода средств защиты от угроз информационной безопасности;

7) подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных;

8) выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки;

9) подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей.

10) внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения;

11) модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе. Пример: внесение изменений в модули и конфигурацию вредоносного ПО для удаления индикаторов компрометации этим ВПО после обнаружения его в других системах;

12) манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности (примеры: сокрытие окна приложения через параметры запуска процесса в ОС Windows; выбор для вредоносного приложения имени файла (процесса), похожего на имя известного и/или системного приложения или совпадающего с ним;

13) создание скрытых файлов, скрытых учетных записей;

14) установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов;

15) внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки;

16) искусственное временное ограничение распространения или активации вредоносного кода внутри сети во избежание преждевременного обнаружения факта атаки. Пример: распространение вредоносного ПО единовременно по всем интересующим злоумышленника системам и единовременный запуск его на выполнение по команде, до выполнения которой компрометацию системы обнаружить сложно;

17) обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети;

18) использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе;

19) туннелирование трафика управления через VPN;

20) туннелирование трафика управления в поля заполнения и данных служебных протоколов, например, туннелирование трафика управления в поля данных и заполнение протоколов DNS, ICMP или других;

21) изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами;

22) подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков;

23) подмена файлов легитимных программ и библиотек непосредственно в системе;

24) подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.

25) подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями;

26) подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах;

27) компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (так называемые «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами;

28) компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы;

29) компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы.

Другая тактическая задача, которая стоит перед нарушителем, – получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям, т. е. нарушитель, получив доступ к некоторым узлам инфраструктуры, стремится получить доступ к другим узлам (подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей).

Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям может выполняться в несколько шагов с использованием одной или более из перечисленных ниже техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки:

1) эксплуатация уязвимостей для повышения привилегий в системе или сети, для удаленного выполнения программного кода, для распространения доступа;

2) использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям;

3) использование механизмов дистанционной установки программного обеспечения и конфигурирования;

4) удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям;

5) изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами;

6) копирование вредоносного кода на съемные носители;

7) размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети;

8) использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях.

Следующая тактическая задача, стоящая перед нарушителем, – сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз, т. е. в ходе реализации угроз безопасности информации нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия.

Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз, могут выполняться с использованием одной или более из перечисленных ниже техник для реализации резервных каналов вывода информации:

1) доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а

также использование инфраструктуры провайдеров средств удаленного администрирования;

2) доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системой;

3) вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.);

4) вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств;

5) отправка данных по известным протоколам управления и передачи данных;

6) отправка данных по собственным протоколам;

7) проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения (примеры: использование скомпрометированных систем в той же сети, для которых разрешен доступ в Интернет в качестве прокси-серверов; использование инфраструктуры сети TOR для проксирования запросов к серверам управления; использование одного коммуникационного протокола для запроса, и другого – для ответа на запрос);

8) туннелирование трафика передачи данных через VPN;

9) туннелирование трафика управления в поля заполнения и данных служебных протоколов, например, туннелирование трафика управления в поля данных и заполнение протоколов DNS, ICMP или других;

10) вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах;

11) отправка данных через альтернативную среду передачи данных. Пример: вывод конфиденциальной информации через субтитры видеоряда, демонстрируемого на веб-сайте;

12) шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации;

13) вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей;

14) вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети).

Следующая тактическая задача, которая стоит перед нарушителем, – несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям, т. е. в ходе реализации угроз безопасности информации нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия.

Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям при реализации угроз безопасности информации или реализации новых угроз, могут выполняться с использованием одной или более из перечисленных ниже техник для повышения эффективности воздействия с точки зрения нарушителя или для реализации нескольких типов воздействия на атакуемую систему:

1) несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках;

2) несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа;

3) несанкционированное воздействие на программные модули прикладного программного обеспечения;

4) несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения;

5) несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения;

6) несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства;

7) подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей;

8) уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей;

9) добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости) ;

10) организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети;

11) нецелевое использование ресурсов системы (примеры: организация майнинговой платформы; организация платформы для осуществления атак отказа в обслуживании на смежные системы и сети);

12) несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов (примеры: воздействие на автоматизированные системы управления объектов транспорта; удаленное воздействие на цифровые системы и первичное оборудование объектов электроэнергетики; воздействие на системы управления технологическим процессом нефтехимического объекта);

13) несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов;

14) отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представля-

ющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов;

15) воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой. Пример сценария реализации угрозы безопасности информации приведен на рисунке.

Сценарий реализации угрозы безопасности информации*

Тактика				
Сбор информации	Получение первоначального доступа	Внедрение и использование вредоносного кода	Закрепление в системе и сети	Управление вредоносным кодом
Техника				
Сбор информации из публичных источников Направленное сканирование при помощи специализированного ПО Сбор информации о пользователе	Использование внешних сервисов организации в сетях публичного доступа (Интернет) Использование ошибок конфигурации сетевого оборудования и средств защиты	Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами	Несанкционированное создание учетных записей или кража существующих учетных данных Скрытая установка и запуск средств удаленного доступа и управления операционной системой Внесение в реестр соответствующих записей, обеспечивающих запуск вредоносного ПО	Туннелирование трафика управления через VPN Проксирование трафика управления для маскировки подозрительной сетевой активности

Окончание

Тактика				
Повышение привилегий	Скрытие действий	Получение доступа к другим компонентам	Сбор и вывод информации	Неправомерный доступ и воздействие
Техника				
Эксплуатация уязвимостей ПО к повышению привилегий Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи Использование уязвимостей конфигурации системы, позволяющих вредоносному ПО выполняться с повышенными привилегиями	Модификация модулей и конфигурации вредоносного ПО Очистка/ затирание истории команд и журналов регистрации	Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений	Доступ к системе для вывода информации через стандартные протоколы управления (например, RDP.SSH) Отправка данных по известным протоколам управления и передачи данных Отправка данных по собственным протоколам	Неправомерный доступ к информации к файловой системе, базам данных

* Способ реализации угроз: 1) использование уязвимостей конфигурации веб-сервера; 2) внедрение вредоносного кода

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации.

Темы для обсуждения

1. Приведите классификацию угроз безопасности информации. Опишите различные типы угроз безопасности информации в соответствии с этой классификацией.

2. Перечислите основные пути реализации непреднамеренных искусственных угроз и меры по их нейтрализации.

3. Перечислите основные виды внешних нарушителей и определите их цели при реализации угроз безопасности информации.

4. Приведите классификацию вредоносных программ, в том числе компьютерных вирусов. Опишите различные типы компьютерных вирусов в соответствии с этой классификацией.

5. Приведите примеры компьютерных вирусов, с которыми вы сталкивались. К какому типу вирусов вы их отнесете?

6. Опишите средства нейтрализации компьютерных вирусов. Приведите примеры использования антивирусных комплексов.

7. Что представляет собой статический и динамический анализ программ? При помощи каких средств проводится такой анализ?

8. Перечислите основные источники исходных данных для определения актуальных способов реализации (возникновения) угроз безопасности информации. Кратко охарактеризуйте их.

9. Перечислите основные тактики и соответствующие им типовые техники, используемые для построения сценариев реализации угроз безопасности информации.

10. Опишите сценарий реализации угрозы безопасности информации, с которой вам приходилось встречаться.

Задание для самоконтроля

Выполните тест

1. Непреднамеренные угрозы – это:

а) действия по выводу информационных систем из строя, проникновению в информационные системы и несанкционированному доступу к информации, совершаемые людьми с корыстными целями, по принуждению, из желания отомстить и т. п.

б) события, связанные со стихийными бедствиями, явлениями и несчастными случаями, которые не зависят от человека;

в) действия по выводу информационных систем из строя, проникновению в информационные системы и несанкционированному доступу к информации, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла;

г) действия по выводу информационных систем из строя, проникновению в информационные системы и несанкционированному доступу к информации, совершаемые людьми в состоянии алкогольного опьянения из хулиганских побуждений.

2. К внутренним нарушителям информационной безопасности относятся:

а) лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.).

б) лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

в) бывшие работники предприятия;

г) поставщики вычислительных услуг, услуг связи.

3. В качестве мер по нейтрализации несанкционированного внедрения и использования неучтенных программ с последующим необоснованным расходованием ресурсов применяют:

а) организационные меры (введение запретов);

б) технические (аппаратно-программные) средства, препятствующие несанкционированному внедрению и использованию неучтенных программ;

в) технические (аппаратно-программные) средства разграничения доступа к технологическим и инструментальным программам на дисках автоматизированных рабочих мест;

г) физические средства обеспечения сохранности информационных ресурсов.

4. В качестве мер по нейтрализации непреднамеренного заражения компьютера вирусами используют:

а) организационные меры (регламентация действий, введение запретов);

б) технические (аппаратно-программные) средства, препятствующие заражению компьютеров компьютерными вирусам;

в) технологические меры (применение специальных программ обнаружения и уничтожения вирусов);

г) технические (аппаратно-программные) средства разграничения доступа к технологическим и инструментальным программам на дисках автоматизированных рабочих мест.

5. К внешним нарушителям информационной безопасности относятся:

а) криминальные структуры;

б) лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

в) бывшие работники предприятия;

г) поставщики вычислительных услуг, услуг связи.

6. Целями реализации преднамеренных угроз безопасности информации со стороны хакеров являются:

а) получение финансовой или иной материальной выгоды;

б) желание самореализации;

в) срыв заключения международных договоров;

г) дестабилизация деятельности органов государственной власти.

7. В качестве мер по нейтрализации незаконного получения паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя применяют:

а) организационные меры (регламентация действий, введение запретов, работа с кадрами);

б) технические средства, препятствующие внедрению программ перехвата паролей, ключей и других реквизитов;

в) технологические меры (применение специальных программ обнаружения и уничтожения вирусов);

г) технические (аппаратно-программные) средства разграничения доступа к технологическим и инструментальным программам на дисках автоматизированных рабочих мест.

8. К мерам по нейтрализации перехвата данных, передаваемых по каналам связи, относят:

а) физическую защиту каналов связи;

б) использование средств криптографической защиты передаваемой информации;

в) применение средств электронной подписи;

г) применение межсетевых экранов.

9. Для того чтобы программа считалась вредоносной, она должна соответствовать следующим трем критериям:

а) направленность на уничтожение информации;

б) несанкционированный характер работы;

в) целью создания программы является оказание неправомерного воздействия на информационные ресурсы;

г) использование в противоправной деятельности.

10. Разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети:

а) вирус;

б) червь;

в) троян;

г) вредоносная утилита.

Библиографический список

1. Методика оценки угроз безопасности информации. Методический документ (утв. ФСТЭК России 05.02.2021) [Электронный ресурс]. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=451500 (дата обращения: 29.10.2022).

2. Россия. Утечки информации ограниченного доступа в 2021 году [Электронный ресурс] // Экспертно-аналитический центр InfoWatch: портал. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-rost-latentnosti-intsidentov-i-vnutrennikh-utechek.pdf (дата обращения: 29.10.2022).

3. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст) [Электронный ресурс]. – Режим доступа: https://gostrf.com/normadata/1/4293836/4293836037.pdf (дата обращения: 29.10.2022). – М. : Изд-во Стандартинформ. – 12 с.

4. Русскевич, Е. А. Понятие вредоносной компьютерной программы / Е. А. Русскевич // Актуальные проблемы российского права. – 2018. – № 11. – С. 207 – 215.

5. Малыковцев, М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : дис. ... канд. юрид. наук / Малыковцев М. М. – М., 2007. – 186 с.

6. Фатьянов, А. А. Правовое обеспечение безопасности информации в Российской Федерации : учеб. пособие / А. А. Фатьянов. – М. : Юрайт, 2001. – 421 с.

7. Климентьев, К. Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. – М. : ДМК-Пресс, 2013. – 656 с. – ISBN 978-5-94074-885-4.

8. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учеб. для вузов / О. В. Казарин, А. С. Забабурин. – М. : Юрайт, 2022. – 312 с. – ISBN 978-5-9916-9043-0.

9. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с. – ISBN 978-5-49807-389-7.

10. Язов, Ю. К. Защита информации в информационных системах от несанкционированного доступа : учеб. пособие / Ю. К. Язов, С. В. Соловьев. – Воронеж : Кварта, 2015. – 440 с. – ISBN 978-5-93737-107-2.

11. Приказ РРЛ «Об утверждении Концепции информационной безопасности РРЛ» от 06.03.2013 № 154 [Электронный ресурс]. – Режим доступа: https://legalacts.ru/doc/prikaz-rosrybolovstva-ot-06032013-n-154-ob-utverzhdenii-kontseptsii/ (дата обращения: 29.10.2022).

Глава 5. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Содержание и требования, предъявляемые к аудиту

Аудит информационной безопасности – один из ключевых инструментов, который позволяет оценить реальную защищенность активов (в том числе ИТ-активов) компании. Результаты аудита позволяют создать/улучшить существующую систему информационной безопасности (ИБ).

Аудит информационной безопасности – системный процесс сбора свидетельств, получение качественных и количественных оценок относительно состояния технологического или бизнес-процесса (с точки зрения ИБ), а также элементов ИТ-инфраструктуры и их соотнесение с критериями (законами, стандартами, политиками и т. д.).

В России аудитом информационной безопасности принято называть широкую категорию услуг и сервисов. В зависимости от области работ, состава информационных систем, методик и критериев аудита можно выделить десятки различных вариантов.

Аудит информационной безопасности – очень широкая категория услуг, соответственно цели аудитов могут существенно отличаться друг от друга. Например, целью аудита может быть подтверждение соответствия деятельности компании какому-либо стандарту. По результату такого аудита может выдаваться сертификат или иной документ, например, по результату аудита аккредитованным органом может выдаваться сертификат соответствия (ISO 27001).

В технических аудитах информационной безопасности конечной целью может быть определенное действие. Например, заказчик пентеста может обозначить в качестве цели внесение изменений в информационную систему (наиболее популярная цель – создание новой учетной записи с правами администратора в контроллере домена).

Основной целью аудита является получение объективной и независимой оценки состояния информационной безопасности. В дальнейшем все зависит от решаемых средствами аудита задач.

К задачам аудита информационной безопасности можно отнести (рис. 5.1):

1. Подтверждение соответствия требованиям (стандартов, регуляторов и пр.).

2. Выявление уязвимостей ИТ-инфраструктуры.

3. Выявление уязвимостей в процессах (в том числе в процессе самого обеспечения ИБ).

4. Получение рекомендаций по улучшению/изменению.

Рис. 5.1. Задачи аудита информационной безопасности

Процесс аудита информационной безопасности

Аудит ИБ предприятия может быть очным, заочным и смешанным. В любом случае эксперт получает информацию о состоянии информационной безопасности в организации и, обрабатывая и сопоставляя ее с критерием оценки, получает свидетельства (рис. 5.2).

В качестве свидетельств выступают:

– скриншоты и фотографии;

– интервью и записи сотрудников проверяемой организации;

– внутренние документы и документы контрагентов проверяемой организации;

– наблюдения эксперта.

Рис. 5.2. Свидетельства при проведении аудита ИБ

В зависимости от сложности критериев и размера области оценки варьируются срок и содержание плана проведения аудита.

После получения достаточного набора свидетельств аудитор выставляет оценку соответствия (количественная, например 0.84, или качественная – «соответствует» в зависимости от критерия).

По полученным результатам в обязательном порядке выдаются рекомендации по улучшению и/или повышению оценки.

Стандарты и виды аудита информационной безопасности

Принято разделять аудиты ИБ на экспертные аудиты и аудиты по стандартам (compliance).

Экспертные аудиты информационной безопасности как услуга разрабатываются под конкретную задачу проверяемой организации. Например, в компании произошел инцидент. По результатам внутреннего расследования было установлено, что причиной инцидента стала некорректная настройка сетевого оборудования. В таком случае может быть проведен аудит безопасности внутренней инфраструктуры, сочетающий в себе элементы тестирования на проникновение. В рамках такого аудита будут проанализированы настройки сетевого оборудования, процессы, опрошены лица, участвующие в технологическом процессе, и пр. Такой аудит призван выявить проблемы на одном из направлений системы обеспечения информационной безопасности.

Аудиты по стандартам подразумевают работу по какому-либо критерию, например, по стандарту или набору стандартов ISO, NIST, ГОСТ и пр. Соответственно проверяющий будет опираться на стандарт информационной безопасности в полном объеме, соблюдая все процедуры и требования конкретного критерия. В этом случае методика аудита заранее определена, подавляющее большинство стандартов предусматривают методики аудитов в самих стандартах.

Наиболее популярные стандарты/критерии/РД информационной безопасности в России, которыми пользуются аудиторы:

1. ISO 27001.
2. NIST SP 800-й серии.
3. ГОСТ Р ИСО/МЭК 18045.
4. Серия положений Банка России по информационной безопасности.
5. ГОСТ 57580.х.
6. ГОСТ Р ИСО/МЭК 27007.
7. Серии документов ФСТЭК России по персональным данным и защите критической информационной инфраструктуры.

Перечислять все стандарты не имеет смысла, так как документов много, а их актуальность часто меняется.

Варианты аудитов информационной безопасности

По типу исполнителя аудит информационной безопасности можно разделить на внутренний и внешний.

Внутренний аудит, как правило, проводят специалисты самого предприятия, внешний аудит – приглашенные эксперты.

Исходя из определения для проведения конкретного аудита ИБ можно выбрать разные его составляющие, приведенные на рис. 5.3:

– критерии аудита;

– проверяемые элементы ИТ-инфраструктуры (для аудита информационных систем);

– проверяемые процессы;

– варианты получения оценок (качественных или количественных);

– варианты собираемых свидетельств аудита;

– варианты процессов сбора свидетельств.

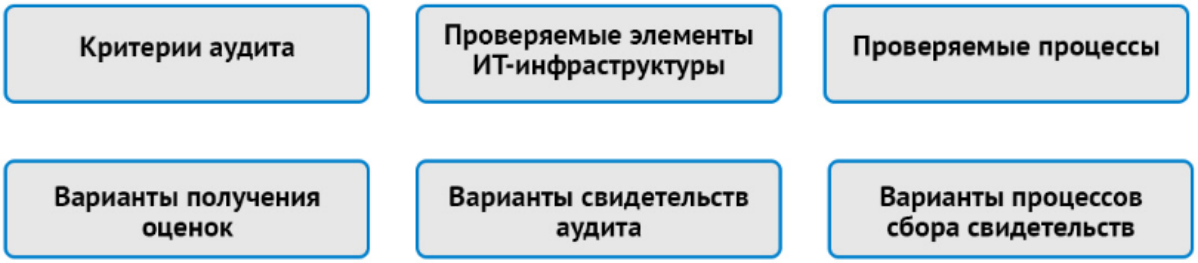

Рис. 5.3. Предпосылки для проведения аудита ИБ

Наиболее частыми критериями для аудита являются **законы, стандарты или требования регулирующих органов**. Основными регуляторами в области информационной безопасности следует назвать ФСТЭК России, ФСБ России и Банк России. Помимо этого применяется так называемый экспертный аудит, проводимый по неформализованному критерию обобщения лучших практик.

1. Аудит по 747-П.
2. Аудит элементов единой биометрической системы по ГОСТ Р 57580.1-2017.
3. Аудит по 683-П для банка.

4. Аудит по 757-П для НФО.

5. Аудит по 719-П.

6. Аудит (оценка соответствия) по ГОСТ Р 57580.

7. Аудит на соответствие 152-ФЗ «О персональных данных».

8. Аудит на соответствие стандартам серии ISO 27001.

В отдельную группу следует выделить **технические аудиты, или аудиты безопасности информационных систем** (даже в том случае, если проверка происходит по критерию). Дело в том, что технические аудиты требуют иных компетенций аудиторской команды. К наиболее популярным техническим аудитам относятся:

1. Тест на проникновение (пентест).

2. Аудит программного кода.

3. Аудит безопасности сайта или веб-сервиса.

4. Аудит безопасности сайта.

Большинство аудитов носят смешанный характер (оцениваются как техническая реализация, так и документальное обеспечение деятельности). К данной категории можно отнести:

1. Аудит программного обеспечения по ОУД4 и ГОСТ 15408-3.

2. Оценка соответствия по ОУД4.

3. Аудит безопасности сети на соответствие требованиям.

4. Аудит ИБ удаленной работы сотрудников.

5. Технико-правовой аудит безопасности интернет-банка.

6. Аудит системы мониторинга информационных систем.

7. Аудит системы инвентаризации оборудования.

8. Аудит безопасности процесса разработки программного обеспечения.

9. Аудит инфраструктуры на соответствие требованиям информационной безопасности.

10. Аудит непрерывности бизнеса с точки зрения информационной безопасности.

11. Аудит систем обеспечения физической безопасности.

12. Аудит безопасности внутренних процессов.

13. Аудит состояния информационной безопасности за определенный период времени.

14. Аудит состояния ИБ на соответствие требованиям клиентов и/или стандартов.

15. Аудит ИБ в рамках отдельных бизнес-процессов.

Существуют и иные варианты проверки, которые также можно отнести к вариантам аудита информационной безопасности, например экспертизы. Для данного варианта проверок характерно узкое применение результатов. Одним из наиболее частых применений экспертиз является их использование в судебном процессе.

1. Экспертиза по оценке защищенности программного обеспечения или ИТ-системы.

В рамках экспертизы по анализу защищенности ПО эксперту необходимо исследовать информационную систему на предмет наличия уязвимостей, а также выявить признаки их эксплуатации (если требуется). В ходе проведения исследования эксперт оценивает критичность обнаруженных уязвимостей и выстраивает причинно-следственную связь между наличием уязвимостей и событием, которое имеет отношение к делу.

Принято выделять три основных подхода к проведению анализа защищенности.

1. *Принцип черного ящика.* В данном подходе исследователь ничего не знает ни про объект исследования, ни про средства и методы защиты, ни про организационную структуру. Эксперт должен анализировать варианты внешнего проникновения и возможность получения доступа к инфраструктуре и информации. Для этого эксперт может анализировать порты у сетевого оборудования, применять социальную инженерию и пр. В конечном итоге задача эксперта – получить доступ к инфраструктуре, получить информацию и/или права в информационной системе, например пароль и логин администратора.

2. *Принцип серого ящика.* Предварительно у исследователя есть вводные данные, возможно, учетная запись, доступ к проводной сети или Wi-Fi. Эксперт может развивать атаку и получать дополнительные права.

3. *Принцип белого ящика.* В рамках данного подхода проводится внутреннее исследование с наличием большого объема первичной информации. При таком анализе защищенности исследователь видит всю инфраструктуру, понимает, как работает компания и используемые ей системы, может собрать данные о средствах и методах защиты, провести внутреннее сканирование и выявить максимальный объем уязвимостей.

Пентестом можно назвать только первый подход, когда эксперт работает по принципу черного ящика. Некоторые исследователи также называют пентестом серый ящик. Применительно к судебным экспертизам актуален подход белого ящика. Для исследователя важно получить максимальный объем исходных данных, найти и продемонстрировать суду возможность эксплуатации найденных уязвимостей.

В компании RTM Group накоплен большой опыт проведения судебных экспертиз, экспертами освоены все группы компьютерно-технических экспертиз и нормативных экспертиз по направлению информационной безопасности. Имеется обширная практика работы экспертами, специалистами, а также представителями стороны по делу. Эксперты обладают уникальным опытом участия в судебных процессах, требующих проведения анализа защищенности систем дистанционного банкинга (ДБО) и прочих ИТ-систем.

Экспертиза по анализу защищенности позволяет установить и продемонстрировать суду механизм атаки, проведенной внутренним или внешним злоумышленником.

Экспертиза по анализу защищенности ИТ-системы позволяет ответить на вопросы:

– Имеются ли уязвимости в исследуемом программном обеспечении? Каким образом они могут быть использованы? Описать обнаруженные уязвимости.

– Какие могут быть последствия неустранения обнаруженных уязвимостей?

– Какие действия могут быть произведены при наличии обнаруженных уязвимостей?

– Можно ли подтвердить или опровергнуть проведение анализа защищенности в отношении исследуемых систем в 20XX году?

– Возможно ли совершить операции по счету клиента банка путем использования обнаруженных уязвимостей?

– Какие действия должны быть совершены для эксплуатации уязвимости?

– Каким образом были совершены изменения в исследуемой системе, была ли проэксплуатирована уязвимость? Установить авторство изменений.

– Какие уязвимости системы эксплуатировались для совершения хищения?

При рассмотрении дел, в которых требуется установить наличие/отсутствие известных уязвимостей и фактов их эксплуатации, необходимо учитывать, что после того как злоумышленник обнаружил конкретные уязвимости, дальнейшие его действия направлены исключительно на поиск инструментария для эксплуатации найденных уязвимостей. Сложность и длительность процедуры поиска инструментария ограничивается только финансовыми возможностями злоумышленников.

Соответственно наличие уязвимостей уже само по себе является «приглашением» для злоумышленников. Взлом уязвимой системы становится лишь делом времени и экономической целесообразности для злоумышленников.

Чтобы минимизировать вероятность стать жертвой злоумышленников, возможно проведение анализа защищенности до этапа эксплуатации или в процессе эксплуатации. При этом методики и полнота исследований полностью идентичны судебной экспертизе с той лишь разницей, что результаты исследования полностью передаются заказчику и используются им для предотвращения инцидентов, а не для ликвидации их последствий. Помимо этого по результатам аудита экспертами может быть вынесен ряд рекомендаций по оптимизации защищенности рабочих мест, программного обеспечения и информационной инфраструктуры заказчика.

Принято выделять две большие категории злоумышленников: внутренний злоумышленник и внешний.

К внутренним злоумышленникам относятся сотрудники, клиенты и подрядчики, т. е. те лица, которые могут получить информацию об имеющихся уязвимостях в рамках легальной работы. К внешним злоумышленникам относятся все остальные. Как показывает опыт экспертов RTM Group, основная угроза исходит именно от внутренних злоумышленников. Таким образом, **экспертиза по анализу защищенности** может включать в себя раздел по оценке нормативного обеспечения работы ИТ-систем, а также раздел по существующему разграничению прав доступа.

В случае проведения **экспертизы по анализу защищенности во внесудебном порядке** экспертами RTM Group может быть проведена оценка последствий для бизнеса, включая правовые последствия. Это позволяет категорировать уязвимости по уровню угрозы.

Что входит в комплекс экспертиз по анализу защищенности? Экспертиза по анализу защищенности представляет собой **технический аудит информационной безопасности**. В отличие от стандартного аудита, перед началом работ должен быть определен перечень объектов исследований, формализована методика проведения экспертизы, описаны используемые материалы и оборудование.

В случае проведения судебной экспертизы все необходимые исходные данные, а также формулировки вопросов должны быть достаточными и корректными. Поэтому крайне желательно предварительное привлечение в судебное заседание специалиста еще до назначения судебной экспертизы.

В зависимости от поставленных вопросов могут применяться различные методики, материалы и оборудование. Информация относительно методик, материалов и оборудования может быть предоставлена суду заранее. Открытость методик, возможность повтора исследования и верификации выводов эксперта позволяют суду вынести обоснованное решение по рассматриваемому делу.

2. Экспертиза базы данных.

Экспертиза базы данных – один из вариантов компьютерно-технической экспертизы, которая может выполняться как на этапе разработки базы, так и в отношении уже созданной базы. В первом случае задачей экспертизы становится проверка соответствия базы критериям технического задания.

Также экспертиза может оценить реальную стоимость разработки базы данных в целом и отдельных ее частей. Если анализируются данные в существующей базе, то задачами экспертизы могут быть: выявление уязвимостей, обнаружение ошибок в обработке, соответствие требованиям закона в части обеспечения безопасности хранящихся в базе данных, а также исследование инцидентов.

Для чего нужна экспертиза баз данных? Независимая экспертиза дает возможность обнаружить ошибки и недочеты в работе с базами данных. Кроме того, она позволяет получить ряд критически важных для бизнеса сведений: о финансово-хозяйственных операциях, датах и времени совершения тех или иных действий и т. д. Независимое исследование дает возможность решить широкий круг проблем, связанных с работой системы хранения информации, авторскими правами и обеспечением нормативных требований к защите данных. Экспертиза, проводимая независимым беспристрастным специалистом, позволяет выявить:

– факт несанкционированного проникновения;

– время и дату внесения изменений в данные, хранящиеся в базе;

– общую последовательность выполненных операций;

– наличие ограничений на доступ и работу с базой и какие именно ограничения применялись;

– различия сведений в двух базах данных, если есть предположение, что данные из одной базы были скопированы в другую.

В каких еще случаях проводится экспертиза? Наиболее распространенные ситуации – это расследование правонарушений, связанных с вмешательством в работу базы данных предприятия, а также подготовка к проверкам по 152-ФЗ. Однако к помощи независимых экспертов прибегают и в том случае, если в базе хранятся особо ценные сведения, которые могут быть внесены в уставной капитал предприятия и использованы в качестве залога. Экспертиза также требуется, если базу нужно поставить на баланс компании. Зачастую процедуру заказывают и при оценке ущерба, понесенного предприятием после взлома сервера.

Как проводится экспертиза (аудит) базы данных? Общая схема проведения включает в себя следующие этапы (рис. 5.4):

1. Подбор алгоритма экспертизы (аудита). Алгоритм выбирается в зависимости от масштаба базы данных и стоящих перед экспертом вопросов и целей исследования.

2. Определение типа базы данных, изучение ее архитектуры, выявление электронных подписей, имеющихся прав на доступ и внесение изменений и т. д.

3. Непосредственно экспертиза, ставящая целью получение ответов на конкретные вопросы.

4. Подготовка экспертного отчета.

Рис. 5.4. Этапы проведения экспертизы

В ходе анализа эксперты могут ответить на следующие вопросы:

– Каков логический принцип размещения данных?

– В каком виде представлены данные – явные, скрытые, архивированные и т. д.?

– Как сторонний пользователь может получить доступ к базе?

– Предпринимались ли несанкционированные попытки доступа? Если да, то когда и предположительно кем?

– Как и когда была сформирована база?

– Могут ли быть внесены изменения в базу, если да – то как?

В частности, речь идет о внесении изменений при помощи простых средств, доступных рядовым пользователям, например текстового редактора.

Перечисленные выше вопросы представляют собой лишь общий перечень, который в каждом случае может быть изменен и расширен в зависимости от потребностей предприятия.

Стоит также отметить, что, как правило, заказчик экспертизы ставит перед специалистом одну-две общие задачи, например, выяснить, когда и как в базу было совершено проникновение. Задача эксперта заключается в том, чтобы корректно определить алгоритм действий и дать исчерпывающий ответ на поставленные вопросы. Именно от правильности подхода зависит, насколько полно будет проведена экспертиза и насколько точны будут полученные сведения. Поэтому подготовка и квалификация эксперта играют решающую роль.

3. Экспертиза электронной подписи.

Общепризнанная модель электронной цифровой подписи (ЭЦП) охватывает три процесса:

1. Генерация ключей (подпись и проверка).

2. Формирование подписи.

3. Проверка подписи.

Электронная подпись позволяет идентифицировать лицо, подписавшее сообщение или документ, контролировать целостность вышеуказанного документа или сообщения, защищать его от подделок и доказать авторство лица, написавшего сообщение или подписавшего документ. Алгоритмы формирования и проверки электронной цифровой подписи подробно изложены в стандарте ГОСТ Р 34.10-2012.

Различают несколько видов электронных подписей, наиболее часто применяются **простая электронная подпись** и **усиленная электронная**

подпись. Усиленная электронная подпись делится на усиленную неквалифицированную и усиленную квалифицированную электронную подпись.

Простой электронной подписью называют электронную подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Усиленная неквалифицированная электронная подпись – это подпись:

– которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

– позволяет определить лицо, подписавшее электронный документ;

– позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

– создается с использованием средств электронной подписи.

Понятие усиленной квалифицированной электронной подписи практически идентично неквалифицированной электронной подписи, но имеет следующие дополнительные признаки:

1. Ключ проверки электронной подписи указан в квалифицированном сертификате.

2. Для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.

Информация в электронном виде, подписанная квалифицированной электронной подписью, **признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью**. Такой документ согласно законодательству Российской Федерации может применяться в любых правоотношениях кроме случаев, в которых федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Документы и информация в электронном виде, подписанная неквалифицированной электронной цифровой подписью, должны предусматривать порядок проверки вышеуказанной подписи.

В случае с **простой электронной подписью** документ должен соответствовать требованиям, выдвинутым в ст. 9 Федерального закона

№ 63-ФЗ. На рис. 5.5 приведены условия, при соблюдении которых электронный документ считается подписанным простой электронной подписью.

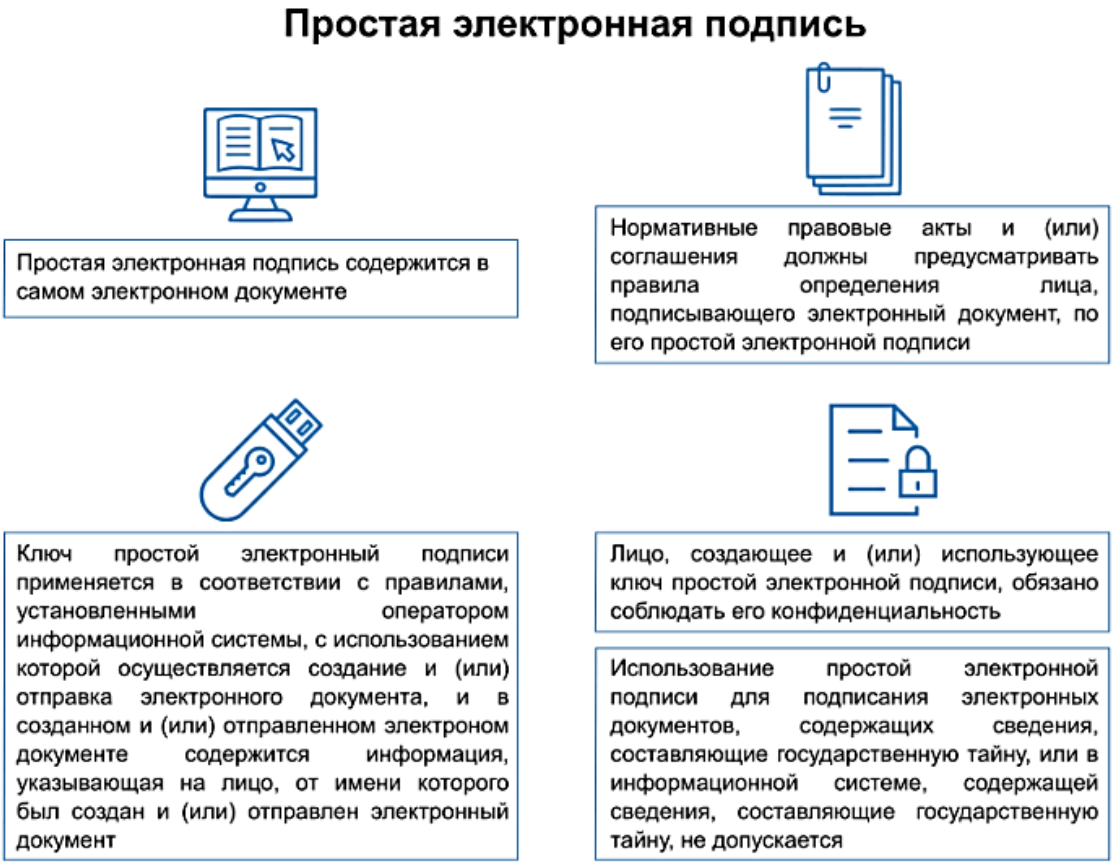

Рис. 5.5. Условия, при соблюдении которых электронный документ считается подписанным простой электронной подписью

Исследование электронной цифровой подписи назначается:

– при возникновении сомнения в оригинальности ЭЦП (имеются подозрения, что лицо, заверившее документ, пользуется не принадлежащей ему электронной подписью);

– для проверки подлинности ключа электронной цифровой подписи;

– для подтверждения того, что документ не был изменен в процессе доставки адресату (возникли подозрения, что документ редактировался после заверения электронной цифровой подписью);

– при необходимости проверки действительности сертификата ключа подписи на момент подписания документа (не был ли сертификат приостановлен или аннулирован).

Экспертиза электронной цифровой подписи осуществляется в том же порядке, что и любой другой вид экспертизы (независимо от объекта исследования). Экспертизу ЭЦП можно провести как внесудебное исследование, досудебную и назначенную судом экспертизу, а также на основании договора с частным или юридическим лицом.

Производство экспертизы электронной цифровой подписи требует специальных знаний и навыков в вышеуказанной области криптографической защиты информации. Требования к данной информационной технологии отражены в ГОСТ Р 34.10-2012.

Результат производства экспертизы оформляется в **заключении эксперта** – представленные в письменном виде содержание исследования и выводы по вопросам, поставленным перед экспертом лицом, ведущим производство, либо сторонами по делу.

Эксперту в исследовании электронной цифровой подписи обычно важно определить:

– принадлежность электронной цифровой подписи владельцу сертификата ключа;

– подлинность сертификата специальной организации, осуществляющей выдачу сертификатов ключей электронной цифровой подписи;

– совпадение хэш-функций на момент подписания и на момент проверки подлинности электронного документа;

– имеется ли сомнение в легитимности использования сертификата ключа по причине каких-либо искажений;

– не утратил ли силу сертификат ключа подписи на момент подписания документа;

– соответствуют ли полномочия лица, поставившего электронную подпись, правам подписанта;

– вносились ли какие-либо изменения в уже заверенный электронной цифровой подписью документ;

– какой вид электронной цифровой подписи использовался для заверения конкретного электронного документа.

Экспертиза электронной подписи – относительно новый вид исследования в рамках компьютерно-технической экспертизы. Однако данная область исследований уже стала одной из наиболее важных ввиду активного перевода банковских, бухгалтерских и множества экономических операций на электронный документооборот. Экспертиза

электронной цифровой подписи использует хеширование для дешифровки и сверки результатов хеш-функций, различия которых свидетельствуют о нарушении целостности документа, и обращается в реестр выдавшей сертификат ключа электронной подписи организации для исследования его подлинности.

Электронная цифровая подпись служит для идентификации человека, заверившего документ. В сущности, это алгоритм шифрования, обеспечивающий набор функций секретности, гарантии целостности документа и идентификации авторства, не допускающего отрицания лицом, подписавшим электронный документ. Цифровая подпись служит надежным инструментом информационной безопасности в области обмена данными.

Система электронных цифровых подписей зачастую подвергается атакам в области экономических интересов преступников. Экспертиза электронной подписи призвана пресекать любые сомнения в нарушении безопасности и целостности электронного документооборота.

5.2. Этапы проведения аудита

В экспертных аудитах план может содержаться в тексте технического задания на аудит. При этом некоторые стандарты в качестве обязательного элемента требуют разработку плана аудита ИБ по заранее определенной форме. Помимо плана аудита, который, как правило, служит планом одного конкретного аудита, некоторые стандарты вводят понятие программы аудита. Программа аудита обычно представляет собой план серии аудитов. Здесь необходимо быть внимательным, так как понятия плана и программы аудита могут существенно отличаться в разных стандартах.

Этапы аудита информационной безопасности

1. Инициация аудита (как правило, включает в себя разработку и подписание договора и ТЗ, в случае аудита по стандартам – ссылку на конкретный стандарт).

2. Сбор информации (проведение интервью, сбор технических данных и документации по информационной безопасности и пр.).

3. Обработка и анализ информации (этап, на котором полученная информация интерпретируется аудитором для достижения цели аудита).

4. Разработка отчета по результатам аудита (формат отчета зависит от технического задания или стандарта ИБ).

Это стандартные этапы, которые будут пройдены по результатам любого аудита ИБ. При этом в зависимости от конкретного проекта могут появиться дополнительные этапы, например:

– предварительное согласование отчета;

– разработка дополнительных документов (предварительная разработка политики или регламента аудита информационной безопасности);

– презентация по результатам работ.

Отчет по аудиту информационной безопасности

Форма и содержание отчета могут быть определены стандартом ИБ, например, ГОСТ 57580.2 содержит четкие требования к отчету. При этом большинство отчетов по аудиту информационной безопасности содержат следующее:

1. Информация о заказчике и исполнителе аудита.
2. Сведения об аудиторской группе.
3. Цели аудита.
4. Сроки аудита.
5. Информация о ходе аудита.
6. Информация о результатах аудита.
7. Рекомендации по результатам аудита.

Темы для обсуждения

1. Что является целями работ по аудиту состояния информационной безопасности автоматизированных систем хозяйствующих субъектов?

2. Что относится к внешнему и внутреннему аудиту ИБ?

3. Каковы основные этапы планирования аудита информационной безопасности?

4. Какие вопросы по аудиту информационной безопасности оговариваются на предварительном этапе организации аудита?

5. Какие существуют практические подходы к анализу и оценке текущего состояния информационной безопасности организации?

6. Каким требованиям по ИБ должна отвечать система защиты информации?

7. Какие используются категории несоответствия?

8. Что выносится на заключительный этап аудиторских процедур информационной безопасности?

Задание для самоконтроля

Выполните тест

1. Аудит информационной безопасности – это…
   а) оценка текущего состояния системы информационной безопасности;
   б) проверка используемых компанией информационных систем, систем безопасности;
   в) проверка способности успешно противостоять угрозам.
2. Расставьте этапы аудита ИБ в их логическом порядке:
   а) локализация потенциально опасных мест ИБ;
   б) разработка рекомендаций по повышению уровня безопасности ИС;
   в) составление и анализ списка рисков;
   г) оценка уровня защищенности информационной безопасности.
3. Активный аудит – это…
   а) исследование средств для определения соответствия их решениям задач информационной безопасности;
   б) исследование состояние системы сетевой защиты, использование которой помогает хакеру проникнуть в сети и нанести урон компании;
   в) исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий).
4. Что такое ЭЦП?
   а) электронно-цифровой преобразователь;
   б) электронно-цифровая подпись;
   в) электронно-цифровой процессор.
5. Какой принцип не относится к проведению анализа защищенности:
   а) принцип черного ящика;
   б) принцип зеленого ящика;
   в) принцип белого ящика.

Библиографический список

1. Аверченков, В. И. Аудит информационной безопасности : учеб. пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – М. : ФЛИНТА, 2016. – 269 с.

2. Анализ рисков в управлении информационной безопасностью // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenieriskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoibezopasnostyu (дата обращения: 22.05.2022).

3. Аудит безопасности информационных систем // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti (дата обращения: 22.05.2022).

4. Аудит информационной безопасности – основа эффективной защиты предприятия // ДиалогНаука [Электронный ресурс]. – Режим доступа: https://dialognauka.ru/press-center/article/4753/ (дата обращения: 01.04.2022).

5. Аудит информационной безопасности // IBS [Электронный ресурс]. – Режим доступа: https://www.ibs.ru/it-infrastructure/information-security/auditinformatsionnoy-bezopasnosti/ (дата обращения: 23.05.2022).

6. Аудит информационной безопасности // Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Аудит_информационной_безопасности (дата обращения: 22.05.2022).

7. Аудит информационной безопасности // Контур [Электронный ресурс]. – Режим доступа: https://kontur.ru/security/features/audit-ib/ (дата обращения: 23.05.2022).

Глава 6. ГОСУДАРСТВЕННОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Уровни информационной безопасности

Информационная безопасность – это глубоко изученный процесс, который принято подразделять на несколько уровней.

Уровни информационной безопасности – это методологическая основа, на которой базируется реализация информационной защиты организации. Без знания этих основ и их особенностей невозможно эффективно внедрять защитные механизмы в инфраструктуру компании. Существуют как глобальные проблемы, затрагивающие несколько «пластов» ИБ, так и локальные, характерные для конкретного уровня.

Выделяют следующие уровни защиты информации.

Уровень 1. Законодательный. К этому уровню относятся законы, нормативные акты и прочие документы Российской Федерации и международного сообщества.

Уровень 2. Административный. Включает в себя комплекс мер, предпринимаемых локально руководством организации.

Уровень 3. Процедурный. Представляет собой комплекс мер безопасности, реализуемых людьми.

Уровень 4. Технический. Уровень компьютерных программ, осуществляющих информационную безопасность.

Рассмотрим каждый из уровней защиты информации подробно.

Уровень 1 (законодательный) – это уровень правовых основ. Главным инициатором в лице своих законодательных органов и профильных ведомств выступает государство. На правовом уровне формируются регламенты и минимальные требования, которым должны соответствовать те или иные компании.

Перечислим основные правовые акты в области защиты информации.

Федеральные законы

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

5. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Указы Президента Российской Федерации

1. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

2. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

3. Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

Приказы Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ)

1. Приказ ФСТЭК РФ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приказы Федеральной службы безопасности Российской Федерации (ФСБ РФ)

1. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

2. Приказ ФСБ РФ и ФСТЭК РФ от 31 августа 2010 г. № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

Постановления Правительства Российской Федерации

1. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Информационные сообщения ФСТЭК РФ

1. Информационное сообщение ФСТЭК РФ от 30 июля 2012 г. № 240/24/3095 «Об утверждении Требований к средствам антивирусной защиты».

2. Информационное сообщение ФСТЭК России от 24 августа 2018 г. № 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».

Стандарты информационной безопасности

Международные стандарты

1. BS 7799-1:2005 – Британский стандарт BS 7799. Первая часть стандарта. BS 7799 Part 1 – Codeof Practice for Information Security Management (Практические правила управления информационной безопасностью). Описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определенных на основе лучших примеров мирового опыта (bestpractices) в данной области. Этот документ служит практическим руководством по созданию СУИБ.

2. BS 7799-2:2005 – Британский стандарт BS 7799. Вторая часть стандарта. BS 7799 Part 2 – Information Security Management – Specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

3. BS 7799-3:2006 – Британский стандарт BS 7799. Третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности.

4. ISO/IEC 17799:2005 – «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.

5. ISO/IEC 27000 – Словарь и определения.

6. ISO/IEC 27001 – «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования». Международный стандарт, базирующийся на BS 7799-2:2005.

7. ISO/IEC 27002 – «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности».

8. ISO/IEC 27005 – Сейчас: BS 7799-3:2006 – Руководство по менеджменту рисков ИБ.

9. ISO/IEC 31000 – Описание подхода к риск-менеджменту без привязки к ИТ/ИБ.

10. German Information Security Agency. IT Baseline Protection Manual – Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

Государственные (национальные) стандарты Российской Федерации

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

2. Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации.

3. ГОСТ Р 51188-98. Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

5. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.

6. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности.

7. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности.

8. ГОСТ Р ИСО/МЭК 15408. Общие критерии оценки безопасности информационных технологий. Это стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности, благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения ГОСТа – защита информации от несанкционированного доступа, модификации или утечки и другие способы защиты, реализуемые аппаратными и программными средствами.

9. ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования. Прямое применение международного стандарта – ISO/IEC 27001:2005.

10. ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты.

Руководящие документы

РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации. Архивная копия от 15 июля 2017 на Wayback Machine – содержит описание показателей защищенности информационных систем и требования к классам защищенности.

Нормативные документы ИБ

1. Стандарт Банка России СТО БР ИББС-1.0-2014 – Стандарт Банка России: Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

2. PCI DSS (Payment CardIndustry Data Security Standard) – Стандарт безопасности данных индустрии платежных карт.

Федеральные законы, регулирующие информационную безопасность, очень важны, поэтому они требуют дополнительных комментариев.

В российском законодательстве базовым законом в области защиты информации является **Федеральный Закон «Об информации, информационных технологиях и о защите информации»**. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

– осуществлении права на поиск, получение, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации, обеспечивающей обработку ее информационных технологий и технических средств.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В ст. 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. Свобода поиска, получения, передачи, производства и распространения информации любым законным способом.

2. Установление ограничений доступа к информации только федеральными законами.

3. Открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации кроме случаев, установленных федеральными законами.

4. Равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации.

5. Обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации.

6. Достоверность информации и своевременность ее предоставления.

7. Неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

8. Недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся информация делится на общедоступную и информацию ограниченного доступа. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. В Законе определяется информация, к которой нельзя ограничить доступ, например, информация об окружающей среде или деятельности государственных органов. Оговаривается также, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет четыре категории информации в зависимости от порядка ее предоставления или распространения:

1. Информацию, свободно распространяемую.

2. Информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях.

3. Информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению.

4. Информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

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

– своевременное обнаружение фактов несанкционированного доступа к информации;

– предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

– постоянный контроль за обеспечением уровня защищенности информации.

Итак, Федеральный Закон «Об информации, информационных технологиях и о защите информации» создает правовую основу информационного обмена в Российской Федерации и определяет права и обязанности его субъектов.

Ключевые моменты закона об информационной безопасности:

1. Нельзя собирать и распространять информацию о жизни человека без его согласия.

2. Все информационные технологии равнозначны, нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.

3. Есть информация, к которой нельзя ограничивать доступ, например, сведения о состоянии окружающей среды.

4. Некоторую информацию распространять запрещено, особенно ту, которая пропагандирует насилие или нетерпимость.

5. Хранитель информации обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

6. У государства есть реестр запрещенных сайтов. Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории Российской Федерации.

7. Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор – тогда его сайт разблокируют.

Федеральный закон № 152-ФЗ «О персональных данных» регулирует работу с персональными данными – личными данными конкретных людей. Закон обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников.

Ключевые моменты закона:

1. Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.

2. Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.

3. Если вы собираете персональные данные, то обязаны держать их в секрете и защищать от посторонних.

4. Если владелец персональных данных потребует их удалить, вы обязаны сразу же это сделать.

5. Если вы работаете с персональными данными, то обязаны хранить и обрабатывать их в базах на территории Российской Федерации. При этом данные можно передавать за границу при соблюдении определенных условий, прописанных в законе, – жесткого запрета на трансграничную передачу данных нет.

Серверы облачной платформы VK Cloud (бывш. MCS) находятся на территории Российской Федерации и соответствуют всем требованиям Федерального Закона № 152-ФЗ. В публичном облаке VK можно хранить персональные данные в соответствии с УЗ-2, 3 и 4. Для хранения данных с УЗ-2 и УЗ-1 также есть возможность сертификации как в формате частного облака, так и на изолированном выделенном гипервизоре в ЦОДе VK.

При построении гибридной инфраструктуры для хранения персональных данных на платформе VK Cloud (бывш. MCS) вы получаете облачную инфраструктуру, уже соответствующую всем требованиям законодательства. При этом частный контур нужно аттестовать, в этом могут помочь специалисты VK, что позволит быстрее пройти необходимые процедуры.

Федеральный закон № 98-ФЗ «О коммерческой тайне» определяет, что такое коммерческая тайна, как ее охранять и что будет, если передать ее посторонним. В нем сказано, что коммерческой тайной считается информация, которая помогает компании увеличить доходы, избежать расходов или получить любую коммерческую выгоду.

Ключевые моменты закона о защите информации компании:

1. Обладатель информации сам решает, является она коммерческой тайной или нет. Для этого он составляет документ – перечень информации, составляющей коммерческую тайну.

2. Некоторые сведения нельзя причислять к коммерческой тайне, например, информацию об учредителе фирмы или численности работников.

3. Государство может затребовать у компании коммерческую тайну по веской причине, например, если есть подозрение, что компания нарушает закон. Компания обязана предоставить эту информацию.

4. Компания обязана защищать свою коммерческую тайну и вести учет лиц, которым доступна эта информация.

5. Если кто-то разглашает коммерческую тайну, его можно уволить, назначить штраф или привлечь к уголовной ответственности.

Федеральный Закон № 63-ФЗ «Об электронной подписи» касается электронной подписи – цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки. Закон определяет, что такое электронная подпись, какую юридическую силу она имеет и в каких сферах ее можно использовать.

Ключевые моменты закона:

1. Для создания электронной подписи можно использовать любые программы и технические средства, которые обеспечивают ее надежность. Вы не обязаны использовать для этого какое-то конкретное государственное программное обеспечение.

2. Подписи бывают простые, усиленные неквалифицированные и усиленные квалифицированные. У них разные технические особенности, сферы применения и юридический вес. Самые надежные – усиленные квалифицированные подписи, они полностью аналогичны физической подписи на документе.

3. Те, кто работает с квалифицированной подписью, обязаны держать в тайне ключ подписи.

4. Выдавать электронные подписи и сертификаты, подтверждающие их действительность, может только специальный удостоверяющий центр.

Федеральный Закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» касается

компаний, которые работают в сферах, критически важных для жизни государства, когда сбой в их работе отразится на здоровье, безопасности и комфорте граждан России.

К таким сферам относятся здравоохранение, наука, транспорт, связь, энергетика, банки, топливная промышленность, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая, металлургическая и химическая промышленность. Сюда относят также компании, которые обеспечивают работу предприятий этих сфер, например, предоставляют оборудование в аренду или разрабатывают для них программное обеспечение.

Если на предприятии этих сфер возникнет простой, это негативно отразится на деятельности всего государства. Поэтому к ИТ-инфраструктуре и безопасности информационных систем на этих предприятиях предъявляют особые требования.

Ключевые моменты закона об информационной безопасности критически важных структур:

1. Для защиты критической инфраструктуры существует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

2. Объекты критически важной инфраструктуры обязаны подключиться к ГосСОПКА. Для этого нужно купить и установить специальное ПО, которое будет следить за безопасностью инфраструктуры компании.

3. Одна из мер предупреждения – проверка и сертификация оборудования, ПО и всей инфраструктуры, которая используется на критически важных предприятиях.

4. Субъекты критической информационной инфраструктуры обязаны сообщать об инцидентах в своих информационных системах и выполнять требования государственных служащих. Например, использовать только сертифицированное ПО.

5. Все ИТ-системы критически важных предприятий должны быть защищены от неправомерного доступа и непрерывно взаимодействовать с ГосСОПКА.

6. При разработке ИТ-инфраструктуры критически важные предприятия должны руководствоваться 239-м приказом ФСТЭК. В нем прописаны основные требования к защите информации на таких предприятиях.

7. Государство имеет право проверять объекты критически важной инфраструктуры, в том числе внепланово, например, после компьютерных инцидентов вроде взлома или потери информации.

Кратко остановимся на международных нормативно-правовых актах обеспечения информационной безопасности.

В международной практике обеспечения ИБ основными направлениями являются нормирование компьютерной безопасности по критериям оценки защищенности надежных систем и ИТ; стандартизация процессов создания безопасных информационных систем.

Так, уже в 1983 году Агентство компьютерной безопасности Министерства обороны США опубликовало отчет, названный TCSEC (Критерии оценки защищенности надежных систем), или «Оранжевую книгу» (по цвету переплета), где были определены семь уровней безопасности (A1 – гарантированная защита; B1, B2, B3 – полное удовлетворение доступом; Cl, C2 – избирательное управление доступом; D – минимальная безопасность) для оценки защиты грифованных данных в многопользовательских компьютерных системах. Для оценки компьютерных систем Министерства обороны США Национальный центр компьютерной безопасности Министерства обороны США выпустил инструкции NCSC-TG-005 и NCSC-TG-011, известные как «Красная книга» (по цвету переплета). В свою очередь, Агентство информационной безопасности Германии подготовило Green Book («Зеленая книга»), где в комплексе рассмотрены требования к доступности, целостности и конфиденциальности информации как в государственном, так и частном секторе.

В 1990 году «Зеленая книга» была одобрена Германией, Великобританией, Францией и Голландией и направлена в ЕС, где на ее основе были подготовлены ITSEC (Критерии оценки защищенности информационных технологий), или «Белая книга», как европейский стандарт, определяющий критерии, требования и процедуры для создания безопасных информационных систем, имеющий две схемы оценки: по эффективности (от E1 до E6) и по функциональности (доступность, целостность системы, целостность данных, конфиденциальность информации и передачи данных).

В «Белой книге» названы основные компоненты безопасности по критериям ITSEC:

– информационная безопасность;
– безопасность системы;
– безопасность продукта;
– угроза безопасности;
– набор функций безопасности;
– гарантированность безопасности;
– общая оценка безопасности;
– классы безопасности.

Согласно европейским критериям ITSEC информационная безопасность включает в себя шесть основных элементов ее детализации.

1. Цели безопасности и функции информационной безопасности.

2. Спецификация функций безопасности:

– идентификация и аутентификация – это не только традиционная проверка подлинности пользователя, но и функции для регистрации новых пользователей и удаления старых, а также функции для изменения и проверки аутентификационной информации, в том числе средств контроля целостности, и функции для ограничения количества повторных попыток аутентификации;

– управление доступом (в том числе функции безопасности, которые обеспечивают временное ограничение доступа к совместно используемым объектам с целью поддержания целостности этих объектов; управление распространением прав доступа; контроль получения информации путем логического вывода и агрегирования данных);

– подотчетность (протоколирование);

– аудит (независимый контроль);

– повторное использование объектов;

– точность информации (поддержка определенного соответствия между разными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникации));

– надежность обслуживания (функции обеспечения, когда действия, критичные по времени, будут выполнены именно тогда, когда нужно; некритичные действия нельзя перенести в разряд критичных; авторизованные пользователи за разумное время получат запрашиваемые ресурсы; функции обнаружения и нейтрализации ошибок; функции планирования для обеспечения коммуникационной безопасности, т. е. безопасности данных, передаваемых по каналам связи);

– обмен данными.

3. Конфиденциальность информации (защита от несанкционированного получения информации).

4. Целостность информации (защита от несанкционированного изменения информации).

5. Доступность информации (защита от несанкционированного или случайного удержания информации и ресурсов системы).

6. Описание механизмов безопасности.

В «Белой книге» декларируется разница между системой и продуктом. Под системой понимается конкретная аппаратно-программная конфигурация, созданная с вполне определенными целями и работающая в известном окружении, а под продуктом – аппаратно-программный пакет, который можно купить и по своему усмотрению вставить в ту или иную систему. Для объединения критериев оценки системы и продукта в ITSEC вводится единый термин – «объект» оценки. Каждая система и (или) продукт предъявляют свои требования к обеспечению конфиденциальности, целостности и доступности информации.

Для их реализации необходим и соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев, подотчетность, аудит, правила повторного использования объектов доступа, точность информации, надежность обслуживания, обмен данными. Например, для реализации функций идентификации и аутентификации могут использоваться такие механизмы, как специальный сервер KERBEROS, а для защиты компьютерных сетей – фильтрующие маршрутизаторы, сетевые анализаторы протоколов (экраны) типа FirewallPlus, Firewall-1, пакеты фильтрующих программ и т. д.

Для того чтобы объект оценки можно было признать надежным, необходима определенная степень уверенности, которая декларируется как гарантированность безопасности, включающая в себя два компонента: эффективность и корректность механизмов безопасности (средств защиты). В некоторых источниках гарантированность называют адекватностью средств защиты.

При проверке эффективности анализируется соответствие между задачами безопасности по конфиденциальности, целостности, доступности информации и реализованным набором функций безопасности – их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования

злоумышленниками слабых мест защиты. Кроме того, в понятие «эффективность» включается и способность механизмов защиты противостоять прямым атакам, которая называется мощностью механизмов защиты. По ITSEC декларируются три степени мощности: базовая, средняя, высокая. При проверке корректности анализируются правильность и надежность реализации функций безопасности. По ITSEC декларируется семь уровней корректности – от E0 до E6.

Общая оценка безопасности системы по ITSEC состоит из двух компонентов: оценки уровня гарантированной эффективности механизмов (средств) безопасности и оценки уровня их гарантированной корректности. Безопасность системы в целом оценивается отдельно для систем и продуктов. Защищенность их не может быть выше мощности самого слабого из критически важных механизмов безопасности (средств защиты).

В европейских критериях устанавливается 10 классов безопасности (F-Cl, F-C2, F-B1, F-B2, F-B3, F-1N, F-AV, F-DI, F-DC, F-DX). Первые пять из них аналогичны классам C1, C2, B1, B2, B3 американских критериев TCSEC. Класс F-1N предназначен для систем с высокими потребностями к обеспечению целостности, что типично для систем управления БД, и различает следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выделение объектов. Класс F-AV предназначен для систем с высокими требованиями к обеспечению их работоспособности за счет противодействия угрозам отказа в обслуживании (существенно для систем управления технологическими процессами). Класс F-DI ориентирован на системы с повышенными требованиями к целостности данных, которые передаются по каналам связи. Класс F-DC характеризуется повышенными требованиями к конфиденциальности информации, а класс F-DX предназначен для систем с повышенными требованиями одновременно по классам F-DI и F-DC.

Канада разработала CTCPEC, и, наконец, США разработали новые Федеральные критерии (Federal criteria)**.** Так как эти критерии являются несовместимыми между собой, было принято решение попытаться гармонизировать (объединить) все эти критерии в новый набор критериев оценки защищенности, названный Common criteria (Общие критерии). Общие критерии дают набор критериев по оценке защищенности и устанавливают требования к функциональным возможностям

и гарантиям; семь уровней доверия (уровни гарантий при оценке), которые может запросить пользователь (уровень EAL1 обеспечивает лишь небольшое доверие к корректности системы, а уровень EAL7 дает очень высокие гарантии); два понятия: «профиль защиты» и «цель безопасности».

На уровне правовых основ есть два глобальных риска, которые могут негативно сказаться на всей ИТ-инфраструктуре:

1. Бюрократизация. Часто ее называют «бумажной безопасностью», когда набор документов полностью соответствует требованиям регуляторов, но заявленный уровень защиты не соответствует реальности. Эта проблема перекликается с административным уровнем информационной безопасности, где формируются локальные нормативы и корпоративные правила работы с данными.

2. Неэффективная адаптация. Проблема интерпретации законодательных актов и их применения к конкретной компании обычно вскрывается на этапе ведомственных проверок. Риски здесь напрямую зависят от профессионализма подрядчика и профильных сотрудников.

Помимо этого всегда остается риск столкнуться с классическими проблемами любого законодательства: бюрократизацией процессов, отсутствием разъяснений по тем или иным частным случаям, неочевидностью правоприменительной и судебной практик. Обеспечение безопасности – это процесс, который нуждается в постоянном сопровождении. Система защиты должна регулярно корректироваться в соответствии с изменяющейся средой: появляются новые информационные активы, виды атак, изменяются модели нарушителей.

За законодательным уровнем защиты систем идет административный, на котором «универсальные» правовые нормы и требования адаптируются под специфику конкретной компании.

Это уровень управленческих решений. Основные инициаторы на административном уровне – это топ-менеджмент компании. В рамках этого уровня формируются должностные инструкции, назначаются ответственные лица и составляются регламенты реагирования, обучения персонала и внедрения других защитных механизмов.

Как и на предыдущем уровне, главной проблемой здесь остается формализм. В таком случае протоколы безопасности становятся формальными и не несут никакой практической пользы, поскольку не исполняются должным образом.

Чтобы правильно оценить уровень защищенности систем, в первую очередь нужно определить модель угроз компании и узнать, от кого защищаться. Без моделирования возможных угроз информационной безопасности невозможно построить защищенную систему.

При анализе угроз должны быть обязательно учтены:

1. Угрозы безопасности – это возможная реализация атак или нарушение главных принципов информации: целостности, доступности, конфиденциальности.

2. Модели нарушителя – это портреты хакеров, например, внешний злоумышленник со сканерами в арсенале, хакер в составе группировки, предприимчивый школьник или внутренний нарушитель.

3. Способы реализации угроз – сценарии атак.

4. Возможные уязвимости – бреши в ИТ-инфраструктуре компании: сайтах, приложениях, личных кабинетах и т. д.

5. Последствия от потери или компрометации информации.

При учете этих угроз становится ясно, как именно изменить системы, процессы и средства защиты, чтобы сократить риски и учесть максимум угроз информационной безопасности.

Успешность компании на административном уровне информационной безопасности напрямую зависит от зрелости руководства с позиции ИБ. Большую роль здесь играет осознанность основных принципов информационной безопасности, ее значение для функционирования компании.

Если руководство компании понимает, например, что незащищенность от DDoS-атак может стать причиной недоступности ресурсов компании на N времени и приведет к X финансовым потерям – оно с большей вероятностью придет к пониманию необходимости «закрыть» эту проблему превентивно до первого инцидента.

Законодательный и административный уровни – это этапы теоретико-инструментального обоснования. Их главная задача – это стандартизация процессов осуществления информационной безопасности. Создание комплекса привычных и понятных действий позволяет сформировать ощущение предсказуемости. А предсказуемость – это одно из главных условий безопасности.

Процедурный, или операционный, уровень ИБ является следующим, третьим уровнем, т. е. уровнем практической реализации тех регламентов и инструкций, которые были сформулированы на предыдущих этапах.

Этот уровень обеспечения информационной безопасности – один из самых высокорисковых. На это есть две главные причины:

1. Задействование большого количества людей. Фактически на этом уровне участвуют все сотрудники компании, которые имеют возможность доступа к корпоративным информационным системам.

2. Актуализация. Риск столкновения с киберугрозами существует в любой момент времени. Как правило, «на дистанции» сотрудники показывают разный уровень сопротивления методам социальной инженерии.

Одним из способов снижения рисков может стать массовое обучение персонала организации. Прежде всего необходимо проводить тренинги по противодействию методам социальной инженерии и фишинговым атакам. Причем приоритет стоит отдавать не только теоретическим, но и практическим занятиям с интервалом не более четырех недель.

Многие компании уже пришли к выводу, что успешность внедрения технических средств и ИБ-процедур напрямую зависит от уровня подготовки сотрудников. Новый тренд, к которому движется отрасль, – это обеспечение равномерной периодичности, а в лучшем случае – непрерывности обучения сотрудника.

Несмотря на то что компании с каждым годом все осознаннее относятся к обеспечению информационной безопасности, человеческий фактор продолжает оставаться одной из главных проблем систем безопасности.

Хакеры активно используют методы социальной инженерии, например, электронные письма, содержащие зараженные файлы или фишинговые ссылки. Чтобы уровень кибергигиены рос, компаниям нужно планомерно повышать осведомленность сотрудников о правилах безопасности: учить выявлять фишинговые сайты, рассказывать о психологических приемах и технологиях, которые используют мошенники, чтобы получить конфиденциальную информацию.

В этом компаниям помогают обучающие платформы. Например, в компании МегаФон это SecurityAwareness, на которой есть постоянно обновляющийся набор курсов по разным темам в сфере кибербезопасности и инструментов, позволяющих проверять и закреплять полученные знания. Прохождение обучения позволяет снизить угрозу фишинга почти в десять раз – до 3 – 5 %.

Актуальность такого подхода растет пропорционально росту числа атак, большинство из которых происходят с использованием методов социальной инженерии для получения «точки входа».

Что же включает в себя цифровая гигиена? Вот набор простых правил:

1) использовать сложные пароли;

2) никому не сообщать пароли и пин-коды;

3) использовать мультифакторную аутентификацию везде, где это возможно;

4) не хранить персональные данные (например, сканы паспортов) в облачных системах;

5) использовать социальные сети с умом – не стоит делиться слишком личной информацией;

6) не использовать рабочую почту для личных нужд;

7) не подключаться с рабочих компьютеров к открытым WiFi-сетям;

8) обращаться к сотрудникам службы безопасности при подозрении на кибератаку.

Еще один важный момент, который часто упускается на операционном уровне, – это выстраивание эффективных моделей взаимодействия между ИБ-специалистом и остальными сотрудниками. Если сотрудник считает, что получил фишинговое письмо, он должен четко понимать, как и кому нужно передать эту информацию. Такой подход позволяет выработать «коллективный иммунитет» и своевременно предупредить остальных сотрудников о возникшей угрозе.

Четвертый уровень информационной безопасности. Это уровень «боевых» информационных систем и технических решений, с помощью которых компания защищает свою инфраструктуру. В зависимости от конкретной компании, ее возможностей и масштабов могут быть использованы как SIEM-системы, так и обычные антивирусные программы.

Для начала компания должна определить, какую информацию она хочет защищать. В этом помогут тестовые вопросы: какая информация может обогатить конкурентов, утечка каких данных приведет к приостановке непосредственной деятельности компании и за что могут последовать штрафы от регуляторов.

Затем следует принять организационные меры по построению ИБ-системы: определить политику безопасности, разработать стандарты и

руководства; назначить ответственных. После этого необходимо подумать об обучении сотрудников основам кибербезопасности.

Следует понимать, что защита информации должна быть всесторонней – на уровне ИТ-инфраструктуры, приложений и данных. Если компания большая, скорее всего, понадобится установка системы мониторинга безопасности и сбора событий.

Поскольку одна из основных проблем в современной кибербезопасности – это нехватка специалистов, то стратегию защиты стоит выстраивать таким образом, чтобы затрачивать как можно меньше человеческих ресурсов.

На техническом уровне защиты информационной безопасности происходит определенный конфликт интересов: стремление бизнеса минимизировать затраты сталкивается со стремлением ИБ-специалистов максимально насытить инфраструктуру защитными инструментами.

В рамках этого «конфликта» значение имеют два ключевых фактора:

1. Бюджет. Специалисту по информационной безопасности предстоит на языке бизнеса обосновать, например, почему компании необходимо подключение к ИТ-платформе. Основная сложность заключается в том, что здесь нет конкретных метрик в стиле «окупаемости вложений».

2. Модель угроз. Важно понимать, какие данные и от чего предстоит защищать. На основе этой информации делаются выводы: хватает принятых мер или нужны новые.

При этом важно знать, что никакая система защиты не будет работать в компании, где сотрудники пренебрегают правилами цифровой гигиены. Это повышает актуальность простых решений, связанных с постоянным обучением сотрудников.

Человеческий фактор – самое слабое звено в системе информационной безопасности компании. Бизнесу крайне важно уделять внимание цифровой гигиене сотрудников, выделять на это ресурсы и время. В противном случае инвестиции в покупку технических средств защиты информации будут поставлены под угрозу элементарным незнанием основ кибербезопасности. Среди базовых знаний сотрудников должны быть понимание принципов создания и хранения паролей, умение вовремя распознать фишинговые письма, понимание того, к каким рискам может привести один клик по непроверенной ссылке.

Подведем итоги.

1. Главная цель разграничения уровней ИБ – это упрощение понимания процесса реализации информационной безопасности. На основе этой модели четко видна зависимость операционных решений и технологий от бумажной работы.

2. Понимание связей между этими уровнями дает компании ряд важных преимуществ:

– повышает осознанность всех участников процесса;

– позволяет оптимизировать затраты за счет проведения анализа и избирательного отношения к инструментарию ИБ;

– улучшает качество ИБ-процессов, что влечет снижение затрат на внедрение защитных инструментов.

3. Уровни не взаимозаменяют друг друга, и не получится прикрыть отсутствие работы с сотрудниками внедрением защитных ИС с сохранением их эффективности.

Таким образом, комплексный подход и осознанная работа на каждом из базовых уровней безопасности информации позволяет снизить себестоимость последующего уровня за счет эффективного выстраивания процессов.

6.2. Место информационной безопасности в структуре национальной безопасности

Важной проблемой можно назвать рассмотрение задач обеспечения информационной безопасности, являющейся неотъемлемой составной частью обеспечения национальной безопасности любого государства мирового сообщества на новом этапе своего развития – этапе формирования информационного общества. Известными характерными признаками такого общества является явная обусловленность экономического, социального, научного и всего развития страны широким внедрением новых информационных технологий, обеспечивающих эффективную информатизацию общества, которая, в свою очередь, обеспечивает информационную безопасность общества, в том числе качественной информацией, информационными продуктами, услугами и знаниями, являющимися сегодня важнейшим стратегическим ресурсом страны. Информатизация личности, общества – это важнейшее стратегическое направление деятельности государства,

определяющее стабильное и безопасное социально-экономическое и политическое развитие и приоритеты во всех сферах, в том числе в информационной, и видах деятельности в мировом сообществе.

Подтверждением этому служат практические шаги ведущих стран мира и России, что подтверждается принятием ими ряда нормативных правовых актов и иных документов:

1. 2000 год – Окинавская хартия глобального информационного общества (от имени России подписана Президентом).

2. 2000 год – Концепция национальной безопасности Российской Федерации (утверждена Указом Президента, в ред. от 10.01.2000).

3. 2000 г. – Федеральные целевые программы «Развитие единой образовательной информационной среды (2001 – 2005 годы)», «Электронная Россия».

4. 2002 год – Федеральная целевая программа «Электронная Россия на 2002 – 2010 годы» (утверждена Постановлением Правительства России от 28 января 2002 года № 65).

5. 2007 год – Стратегия развития информационного общества в России (утверждена 25 июля 2007 года Советом Безопасности Российской Федерации) и др.

Национальная безопасность включает безопасность государства, общества, личности. Информационная безопасность в цифровую эпоху играет в системе национальной безопасности ключевую роль, ведь именно от нее зависят сохранность данных и возможность коммуникации и координации между органами власти и обществом.

Под системой национальной безопасности, или системой обеспечения национальной безопасности (СОНБ), понимается совокупность органов, сил и средств. Она является многоуровневой и предполагает взаимодействие государственных органов, общественных институтов, бизнеса и граждан с целью сохранения суверенитета страны, предотвращения посягательств на ее интересы, сбережения национального богатства. Реализуется система внутри страны во взаимодействии между регионами и в рамках международных отношений, предполагая одновременную и в равной степени защиту интересов государства, общества и личности.

Информационная безопасность в системе национальной безопасности занимает одну из ведущих позиций. В России принимаются основополагающие документы в наиболее важных сферах жизнеобеспечения

страны. Наряду с Доктриной продовольственной безопасности разработана и действует Доктрина информационной безопасности, ставшая краеугольным камнем в разработке современной системы защиты от цифровых угроз. Она дала определение информационной сферы, в которой должны применяться внедряемые принципы безопасности. Под информационной сферой понимается совокупность информации, объектов информационной инфраструктуры, сетей связи и Интернета, технологий, участников цифровых отношений, государственных органов и иных организаций, работающих в сфере разработки технологий, защиты данных. Кроме того, к этой сфере относится система регулирования взаимоотношений между ее субъектами.

Доктрина информационной безопасности Российской Федерации

Вторая редакция Доктрины была принята в 2016 году, до этого действовал более ранний документ 2000 года. Она разработана Советом Безопасности РФ и стала теоретической и концептуальной основой для создания нормативно-правовых актов и внедрения проектов, целью которых стала защита интересов России от кибератак и иных цифровых угроз.

Доктрина рассматривает всю работу в информационной сфере на основе и в интересах Концепции национальной безопасности Российской Федерации и выделяет четыре основные составляющие национальных интересов России в информационной сфере.

Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения и пользования информацией, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для ее реализации необходимо:

1) повысить эффективность использования информационной инфраструктуры в интересах общественного развития;

2) усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала России;

3) обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить

и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

4) обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

5) укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

6) гарантировать свободу массовой информации и запрет цензуры;

7) не допускать пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

8) обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов в информационной сфере включает в себя информационное обеспечение государственной политики страны, связанное с доведением до российской и международной общественности достоверной информации о ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам. Для этого требуется:

1) укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

2) интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов в информационной сфере включает в себя развитие современных информационных технологий, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка этой продукцией и выход ее на мировой рынок, а также обеспечение

накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Для достижения результата на этом направлении необходимо:

1) развивать и совершенствовать инфраструктуру единого информационного пространства России;

2) развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

3) развивать в стране производство конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

4) обеспечить государственную поддержку фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем. В этих целях требуется:

1) повысить безопасность информационных систем (включая сети связи), прежде всего первичных сетей связи и информационных систем органов государственной власти, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

2) интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля их эффективности; обеспечить защиту сведений, составляющих государственную тайну; расширять международное сотрудничество России в области безопасного использования информационных ресурсов и противодействия угрозе противоборства в информационной сфере.

Угрозы, изложенные в Доктрине информационной безопасности:

1) рост научного и технического потенциала ряда государств, стремящихся закрепить свой приоритет на международной арене и использующих для этого информационные ресурсы. Применяются такие

методы, как прямое цифровое вторжение в инфраструктуру жизнеобеспечения и применение ресурсов научно-технической разведки;

2) усиление информационно-психологического воздействия на население, использование информационных технологий для изменения менталитета и поведения граждан;

3) использование технологий цифровых атак и хакерского потенциала национальными и международными экстремистскими и террористическими группировками;

4) возрастание масштабов кибератак на объекты инфраструктуры, финансовую сферу, бизнес и граждан;

5) недостаточный уровень развития собственного научного и кадрового потенциала.

Понимание перечисленных угроз привело к реализации проектов национального масштаба, призванных минимизировать риски, возникающие в сфере информационной безопасности как неотъемлемой составляющей национальной безопасности.

Защита суверенитета государства в цифровом мире требует существенных усилий. Роль государства в усилении информационной безопасности в системе национальной безопасности выражается в следующих направлениях:

1) нормативно-правовом регулировании на законодательном и подзаконном уровнях;

2) реализации национальных проектов;

3) регулировании на уровне исполнительной власти;

4) организации взаимодействия государства и общества.

Если регулирование и взаимодействие носят системный и непрерывный характер, то национальные проекты направлены на прорывное решение наиболее значимых задач.

Национальный проект «Цифровая экономика»

Национальный проект «Цифровая экономика», реализуемый Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, предусматривает выполнение нескольких подпрограмм:

1. Кадры.
2. Безопасность.
3. Технологии.
4. Государственное управление.

Их реализация рассчитана на период до 2024 года. В рамках подпроекта «Информационная безопасность» планируется решить ключевые задачи, призванные обеспечить устойчивое развитие национальной информационной инфраструктуры, подготовку кадров и развитие технологий, повысить экспортный потенциал отрасли, гарантировать полную защиту интересов государства и общества.

На период реализации программы предусмотрено:

– предоставить поддержку 100 экспортно ориентированным компаниям, что должно обеспечить устойчивое присутствие национальных информационных технологий на международной арене;

– добиться маршрутизации на территории России не менее 90 % сетевого трафика (концепция суверенного Рунета);

– обеспечить использование не менее чем 97 % населения средств защиты информации;

– снизить долю иностранного программного обеспечения, покупаемого или арендуемого государственными организациями, до 10 % в структуре общей цены закупок.

В рамках подпроекта с осени 2019 года началось предоставление субсидий ряду исполнителей. На его реализацию до 2024 года планируется затратить 167 млрд руб.

Показатели в цифровом выражении, которых предполагается достичь к 2024 году:

– снизить среднее время простоев ГИС (государственных информационных систем) в результате информационных атак с 65 часов на конец 2018 года до 1 ч в 2024 году, что должно сыграть ключевую роль в сфере защиты информации;

– повысить процент населения, применяющего отечественные средства защиты информации, с 86 до 97 %;

– увеличить количество специалистов, подготовленных по направлению защиты информации, с 7 до 24 тыс.;

– снизить долю иностранного ПО в общей цене закупок ПО государственными органами и компаниями с 50 до 10 %.

Помимо планируемых показателей определены конкретные действия, которые уже достигнуты и должны быть реализованы в рамках нацпроекта:

1. Предполагается, что безопасность информационного пространства и сети Интернет недостаточно отрегулирована на уровне

международного права, отсутствуют документы, которые позволяют устранить перевес сил в пользу отдельных государств. В рамках решения этой задачи в международные организации (ООН) внесены проекты соглашений и конвенций, направленных на реализацию принципа паритетности в сфере информационных технологий, равного участия государств в управлении Интернетом. Так, Россия стала инициатором первой резолюции Генеральной Ассамблеи ООН «О достижениях в области информатизации и телекоммуникаций в контексте международной безопасности в 1998 году» и намерена продолжить движение в этом направлении.

2. Нападения иностранных хакеров на сети электрообеспечения страны признаны одной из основных угроз национальной и экономической безопасности. Были проанализированы угрозы, составлена их модель и внесены предложения по изменению отраслевых стандартов и нормативно-правовых актов с целью создания единой устойчивой системы защиты объектов электросистемы, принадлежащих различным собственникам, что усложняет задачу создания единого пространства регулирования системы защиты от сетевых атак.

3. Обеспечение информационной безопасности требует преимущественной маршрутизации трафика в пределах границ Российской Федерации. Разработаны концепция и основные нормативные акты по созданию суверенного Рунета, началось их внедрение. Правовой статус российского сегмента Интернета законодательно закреплен.

4. От устойчивости сетей связи зависит качество управления и взаимодействия государственных органов. Были законодательно закреплены требования к устойчивости и безопасности сетей связи и оборудования как для ГИС, так и для компаний различных организационно-правовых форм.

5. Сети общего пользования могут стать объектами направленных атак. Разработана и внедряется система мониторинга состояния сетей общего пользования. Изменены требования к проектированию сетей связи общего пользования с учетом действующей модели угроз. Новые общие и частные сети могут создаваться только при условии их соответствия разработанным параметрам.

6. Информационная безопасность призвана решать задачи обеспечения правопорядка. Разработан и вводится комплекс решений по внедрению отечественных информационных технологий при реализации программы «Умный город».

Государственный центр обнаружения и предотвращения компьютерных атак

Среди уже внедренных проектов, обеспечивающих защиту интересов государства и общества, особое значение имеет ГосСОПКА – государственный центр обнаружения и предотвращения компьютерных атак. Его поддержкой занимается ФСБ РФ, ведомство выполняет ключевые задачи обеспечения национальной безопасности в информационной сфере.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, созданная по указу Президента РФ № 620, предназначена для решения четырех основных задач в сфере информационной безопасности как части национальной безопасности:

1) прогнозирование рисков атак в информационном пространстве;

2) взаимодействие между собой и с государством компаний, которым принадлежат значимые информационные ресурсы, особенно обслуживающие критические объекты инфраструктуры, для выявления, предупреждения и ликвидации последствий цифровых атак;

3) контроль и мониторинг уровня защищенности инфраструктуры от цифровых атак;

4) расследование инцидентов информационной безопасности.

За общее рабочее состояние системы отвечает ФСБ РФ. Все организации любой формы собственности, имеющие в распоряжении объекты критической информационной инфраструктуры (КИИ), обязаны создать у себя центры ГосСОПКА и оборудовать их в соответствии с требованиями ФСБ и ФСТЭК РФ. Отказ от выполнения этих требований ввиду их важности для жизнеобеспечения страны и создания необходимого уровня информационной безопасности в системе национальной безопасности предусматривает ответственность вплоть до уголовной.

С точки зрения информационной архитектуры ГосСОПКА выглядит как единый, но территориально распределенный комплекс центров управления и мониторинга, обменивающихся между собой информацией о кибератаках. Задача системы – объединение критически важной инфраструктуры в единую сеть с целью обмена информацией о кибератаках. Если такая атака совершается на один из объектов, он

передает ее параметры другим, и те имеют возможность подготовиться к нападению. Совместная система предупреждения уже доказала свою эффективность.

Система состоит из центров трех уровней – федерального, регионального и местного, которые делятся на территориальные, ведомственные и корпоративные центры. Для борьбы с компьютерными атаками все они должны иметь следующие программные и аппаратные средства:

1. Средства обнаружения выявляют не инциденты, а именно значимые события информационной безопасности, чаще всего они реализуются по модели SIEM.

2. Механизм предупреждения, инвентаризации и мониторинга реализуется программными средствами класса VulnerabilityScanner или сканерами защищенности. В большинстве компаний с КИИ такие средства уже внедрены согласно рекомендациям ФСТЭК РФ.

3. Ликвидация последствий. Здесь реализуется совместная работа участников системы по ликвидации последствий компьютерных атак, реализуемая в виде IncidentResponsePlatform.

4. Расшифровка.

5. Обмен информацией.

6. Криптографическая защита каналов связи. В данном случае дополнительной разработки средств шифрования именно для ГосСОПКИ не потребовалось.

Разработка программных средств для их внедрения в центрах ГосСОПКА ведется крупнейшими компаниями – производителями программного обеспечения в стране, что является одним из проявлений взаимодействия государства и общества в сфере информационной безопасности как части национальной безопасности.

Зона совместного регулирования

Государство уполномочено принимать нормативные акты и рекомендации в сфере обеспечения компьютерной безопасности, но они непосредственно влияют на общество и бизнес, вынуждая корректировать планы и бюджеты. Современная концепция взаимодействия власти и общества в сфере информационной безопасности предполагает, что практически все нормативные акты, существенно затрагивающие

общественные интересы, должны пройти стадию предварительного общественного обсуждения.

Особенно это касается значимых законопроектов. Так, законопроект о суверенном Рунете проходил длительное общественное обсуждение, пока не были учтены основные замечания. Это же касается ряда рекомендаций ФСТЭК РФ, относящихся к сертификации программного обеспечения, ведомство прислушивается к аргументам бизнеса и вносит корректировки в свои проекты. Невозможно решать вопросы такого уровня, как ограничение пользования Интернетом, без учета интересов личности, поэтому в обсуждении концепции цифровой безопасности принимали участие не только Ростелеком и «Лаборатория Касперского», но и общественность. Законопроект был размещен в Интернете для открытого обсуждения, что позволило скорректировать ряд направлений государственной политики, так как состояние информационной защищенности гражданина предполагает и его информированность о тех действиях государства, которые могут повлиять на его интересы.

Международно-правовое взаимодействие государства и общества

Государство не может действовать в одиночку, ему нужно стабильное взаимодействие с институтами гражданского общества и бизнесом; это позволяет достичь синергии в создании информационной безопасности в системе национальной безопасности Российской Федерации. Крупнейшие производители компьютерных технологий понимают, что в современном мире силовой инструментарий государства зачастую стоит на службе у крупных корпораций и кибероружие иностранных государств во многом будет задействовано против российского бизнеса. Так, в начале 2019 года Франция приняла новую доктрину кибербезопасности, разрешающую «превентивные кибератаки», тем самым признав факт разработки кибероружия. Она оказалась не первой, ранее факт таких разработок признавал Китай.

Исходя из представленного Минкомсвязи паспорта проекта «Информационная безопасность» критическая инфраструктура пока не готова к целенаправленному отражению массированной атаки на системы жизнеобеспечения, энергосеть, крупнейшие промышленные предприятия. Бизнес полностью готов к сотрудничеству с государством, видя

общую опасность. Наиболее существенной проблемой стала возможность внешнего проникновения в системы АСУ предприятий. Евгений Касперский утверждает, что в 2018 году такие попытки осуществлялись в отношении 48 % систем АСУ. Это побуждает к выработке новых защитных решений; авария на нефтепроводе способна полностью парализовать регион. Бизнес, стремясь к защите своих интересов, активнее включается в общегосударственную работу в области информационной безопасности.

На сегодня частно-государственное взаимодействие в области кибербезопасности развивается в различных направлениях. Несмотря на режим санкций идет активное общение между учеными и предпринимателями России и стран Европы. Общество стремительно реализует модель «сетевой дипломатии», в которой бизнесмены нашей и зарубежных стран активно договариваются о создании кодекса этики, в рамках которого информационные атаки на экономическую инфраструктуру окажутся неприемлемым и не признаваемым экономическим сообществом мира методом конкурентной борьбы.

Риск киберинцидентов, инспирируемых международными террористическими группировками и опасных для общества и бизнеса, привел к возникновению компьютерных групп реагирования на чрезвычайные ситуации и команд компьютерной безопасности по реагированию на инциденты (CERTs / CSIRTs). Глобальный форум по управлению Интернетом в 2017 году показал, что корпоративные CERTs из различных стран активно идут на сотрудничество друг с другом, выстраивая собственную трансграничную систему взаимодействия и борьбы государств с глобальными компьютерными угрозами. В России участником глобального тренда стал RU-CERT – российский центр реагирования на компьютерные инциденты.

Бизнес выдвигает идеи создания некой общей среды кибербезопасности, в которой реализовывались бы переплетенные интересы государства и общества. Так, в октябре 2019 года состоялось заседание Клуба «Безопасность информации в промышленности», в котором приняли участие лидеры бизнеса России – «Норникель», «Северсталь», «Лукойл», «Юнипро», «Газпромнефть», «Фосагро», «НЛМК». Примером такого взаимодействия стало рассмотрение на международном уровне разработанной компанией «Норникель» Хартии информационной безопасности критических объектов промышленности в ОБСЕ и в Совете Баренцева/Евроарктического региона.

Признаваемая потенциальными участниками Хартии информационная безопасность в системе национальной безопасности выступает гарантом отказа не только бизнеса, но и государств от конфликтов с использованием кибероружия, последствия которых могут оказаться критическими. Хартия «Норникеля» осуждает использование информационных технологий в целях недобросовестной конкуренции и нанесения ущерба объектам промышленности и «приветствует усилия международного сообщества по приданию опорным информационно-коммуникационным инфраструктурам, формирующим основу глобальной сети, статуса демилитаризованной зоны, свободной от силового противоборства политических субъектов».

Этот документ не единственный, бизнес уже несколько лет выступает с инициативами усилить совместное регулирование борьбы с кибероружием.

1. В 2014 году Microsoft предложил Цифровую Женевскую конвенцию, включающую шесть основных принципов международной кибербезопасности, применяемых в мирное время. Компания потребовала от государств ограничить гонку кибервооружений.

2. Соглашение о кибербезопасности (предложено Cybersecurity TechAccord в 2018 году).

3. Хартия доверия Siemens (CharterofTrust) – 2018 год. Компания сформулировала основные принципы организации совместной политики кибербезопасности.

4. Глобальная комиссия по киберстабильности (GCCS) в 2018 году предложила два документа, они касаются защиты «публичного ядра» Интернета и обеспечения безопасности инфраструктуры, используемой для проведения выборов и референдумов.

Пока ни один из названных документов не вышел из стадии обсуждения, это касается и схожих документов в сфере международного права, предлагаемых иными международными субъектами.

Вопросы информационной безопасности Российской Федерации могут быть решены только в тесном взаимодействии государства, бизнеса и общества, где заинтересованными участниками диалога становятся крупные корпорации и разработчики программного обеспечения. Цифровая эра создает новые вызовы, в которых за государством остается роль организатора и регулятора, а бизнес становится соисполнителем задач.

Темы для обсуждения

1. Национальные интересы в информационной сфере.
2. Источники и содержание угроз в информационной сфере.
3. Соотношение понятий «информационная безопасность» и «национальная безопасность».
4. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
5. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
6. Система обеспечения информационной безопасности.
7. Обеспечение информационной безопасности Российской Федерации.
8. Понятие информационной войны. Проблемы информационной войны.
9. Информационное оружие и его классификация.
10. Цели информационной войны, ее составные части и средства ее ведения. Объекты воздействия в информационной войне.
11. Уровни ведения информационной войны. Информационные операции. Психологические операции.
12. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
13. Основные положения государственной информационной политики Российской Федерации.
14. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
15. Виды защищаемой информации в сфере государственного и муниципального управления.
16. Обеспечение информационной безопасности организации.
17. Характеристика эффективных стандартов по безопасности.
18. Требования к полноте эффективных стандартов по безопасности.
19. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
20. Информация – фактор существования и развития общества.
21. Обеспечение информационной безопасности: содержание и структура понятия.
22. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
23. Обеспечение информационной безопасности Российской Федерации.

24. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности.

25. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

26. Административный уровень обеспечения информационной безопасности.

27. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).

28. Корпоративная нормативная база по защите информации.

29. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).

30. Нормативно-методические документы по обеспечению безопасности информации.

31. Информация как объект гражданских прав предпринимателя.

32. Хакеры как феномен информационного пространства.

33. Правонарушения в сфере информационных технологий.

Задание для самоконтроля

Выполните тест

Выберите один или несколько правильных ответов.

1. Информация – это:

а) визуальное восприятие объекта;

б) сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии;

в) фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира;

г) обыденное восприятие действительности.

2. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам:

а) источник информации;

б) уничтожитель информации;

в) обладатель информации;

г) носитель информации.

3. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя:

а) электронное сообщение;

б) распространение информации;

в) конфиденциальность информации;

г) предоставление информации.

4. Отношения, связанные с обработкой персональных данных, регулируются законом:

а) «Об информации, информационных технологиях»;

б) «О персональных данных»;

в) «О защите информации»;

г) «О конфиденциальной информации».

5. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и так далее – это:

а) исправление персональных данных;

б) работа с персональными данными;

в) преобразование персональных данных;

г) обработка персональных данных.

6. Федеральный закон «Об информации, информационных технологиях и о защите информации» направлен:

а) на регулирование взаимоотношений в информационной сфере совместно с Гражданским кодексом РФ;

б) регулирование взаимоотношений в гражданском обществе Российской Федерации;

в) регулирование требований к работникам служб, работающих с информацией;

г) формирование необходимых норм и правил работы с информацией.

7. К принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» относятся:

а) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

б) всеобщий неограниченный доступ к любой информации;

в) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

г) достоверность информации и своевременность ее предоставления.

8. Информацией, составляющей государственную тайну, владеют:

а) государство;

б) только образовательные учреждения;

в) граждане Российской Федерации.

9. Информацией, составляющей коммерческую тайну, владеют:

а) государство;

б) различные учреждения;

в) Государственная Дума;

г) граждане Российской Федерации.

10. Персональными данными владеют:

а) государство;

б) различные учреждения;

в) министерство здравоохранения;

г) граждане Российской Федерации.

11. Федеральный Закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» регулирует сферы:

а) здравоохранения;

б) культуры;

в) металлургической промышленности;

г) связи.

12. Под информационной безопасностью Российской Федерации в Доктрине национальной безопасности понимается:

а) совокупность действий государства для обеспечения информационной безопасности;

б) действия общества и государства по сохранности информации Российской Федерации;

в) состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

г) безопасность информации государства, общества, личности.

13. Когда была утверждена действующая Доктрина информационной безопасности Российской Федерации?

а) 2000 год;

б) 1998 год;

в) 2016 год;

г) 2020 год.

14. Основные цели национального проекта «Цифровая экономика»:

а) повышение внутренних затрат на развитие цифровой экономики за счет всех источников;

б) интеграция импортного и отечественного программного обеспечения для широкого использования;

в) использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями;

г) создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств.

15. Основные задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы:

а) контроль и мониторинг уровня защищенности инфраструктуры от цифровых атак;

б) расследование инцидентов информационной безопасности;

в) прогнозирование рисков атак в информационном пространстве;

г) помощь пользователям в доступе к информационным ресурсам при цифровых атаках.

Библиографический список

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 18.11.2022).

2. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 18.11.2022).

3. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 18.11.2022).

4. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 18.11.2022).

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

[Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 18.11.2022).

6. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/02ede4153cefcb2787580144c4bd05be466415f9/ (дата обращения: 18.11.2022).

7. Цифровая экономика РФ [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fyandex.ru%2f (дата обращения: 18.11.2022).

Глава 7. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ

7.1. Влияние цифровизации на информационную безопасность хозяйствующих субъектов

В современных условиях влияние технологий носит глобальный характер, и правительство России стремится стимулировать цифровую инклюзивность и трансформацию во многих отраслях в рамках целей по развитию цифровой экономики. Так, бюджетные ассигнования на финансовое обеспечение реализации национального проекта «Цифровая экономика» запланированы в объеме 210,7 млрд руб. в 2022 году, в 2023 году – более 190 млрд руб., 2024 году – более 188 млрд руб. На финансирование проекта «Информационная безопасность» запланировано выделить в 2022 году – 8,465 млрд руб., в 2023 году – 8,324 млрд руб., в 2024 году – 6,539 млрд руб.[90]

Интенсивное развитие информационных, электронных и цифровых технологий, их повсеместное внедрение (в первую очередь на производстве) повлекли за собой серьезные структурные изменения в экономической и социальной сферах жизни общества, возникновение совершенно новых рынков и развитие новых форм бизнеса.

---

[90] URL: https://tass.ru/ekonomika/12465313https://tass.ru/ekonomika/12465313 (дата обращения: 18.12.2022).

Вместе с тем компьютеризация и глобальные вычислительные сети, новейшие информационные технологии создают для экономической среды новые риски и источники угроз. Ведущие эксперты в ИТ-индустрии по направлению «Информационная безопасность» в качестве рисков внедрения цифровой экономики выделяют:

− зависимость от западных технологий, замедление развития собственных компетенций;

− угрозу потери тайны личной жизни, утечки персональных данных, различные виды «отслеживания»;

− риск быстрого захвата новых образующихся рынков, связанных с развитием цифровизации, транснациональными компаниями;

− социальную напряженность, связанную с сокращением рабочих мест;

− юридическую неопределенность, этические проблемы, рост мошенничества, «роботизацию» людей;

− исчезновение приватности, навязчивая реклама, новый цифровой тоталитаризм, утечка персональных данных граждан за границу;

− захват экономики более сильными и богатыми иностранными игроками[91].

При владении информацией, особенно если она представляет особую ценность, немаловажной задачей становится ее защита. Темпы развития современных информационных систем и технологий опережают темпы развития средств, обеспечивающих информационную защиту. Незащищенность информации от искажения, нарушения целостности, кражи, потери может нанести непоправимый урон любому субъекту или объекту цифровой экономики. Особенно это касается таких сфер, как оборона, военно-промышленный комплекс, космические разработки, медицина, финансы, банки и т. д. Растущая информатизация экономических процессов требует повышения степени ее безопасности. Эти вопросы обсуждаются на уровне предприятий, а также законодательных и исполнительных органов городов, регионов, государства.

---

[91] Касперская Н. И. Необходимо минимизировать риски цифровой экономики для граждан, общества и государства. 2018 г. URL: https://agenda-u.org/news/natalyakasperskaya-neobhodimo-minimizirovat-riski-cifrovoy-ekonomiki-dlya-grazhdan-obshchestva (дата обращения: 18.12.2022).

В настоящее время особое внимание уделяется проблеме управления информационной безопасностью. Система управления информационной безопасностью создается с использованием следующих основных принципов:

– использование одной системы защиты для выявления (предотвращения) нескольких угроз и нескольких систем защиты для выявления (предотвращения) одной угрозы;

– принцип автоматизации задач информационной безопасности – автоматизированное выявление и противодействие угрозам, автоматизация расследования инцидентов;

– принцип экономической целесообразности – стоимость системы защиты должна быть адекватна возможному ущербу от реализации угрозы;

– принцип непрерывности – обеспечение безопасности в соответствии с данным принципом выполняется непрерывно как бизнес-процесс;

– интеграция процессов безопасности с основными бизнес-процессами компании. Выполнение данного принципа позволяет учитывать требования безопасности на всех этапах принятия решений, этапах жизненного цикла продукции, обеспечивает присутствие специалистов по безопасности на ключевых совещаниях, позволяет разрабатывать меры защиты на стадии разработки продуктов[92].

Управление информационной безопасностью должно обеспечить реализацию следующих постоянно действующих процессов:

– выявление угроз на разных стадиях атаки (планирование, реализация атаки);

– противодействие, включая проактивное. Внедрение технических средств и систем защиты, организационных мероприятий, направленных на предупреждение и блокирование атак. Средства защиты выбираются для актуальных угроз исходя из принципа экономической целесообразности;

– фиксирование действий пользователей и нарушителей с целью формирования информационной базы для расследования инцидентов;

– реагирование на инциденты в моменте (в процессе атаки);

---

[92] Развитие цифровой экономики как фактор повышения уровня экономической безопасности страны : монография / под ред. А. К. Моденова. СПб. : С.-Петерб. гос. архитектурно- строит. ун-т, 2020. 316 с.

– расследование инцидентов;

– анализ методов, средств защиты, оценка рисков и ранжирование угроз;

– мониторинг эффективности системы безопасности компании, планирование и внедрение новых методов и средств защиты;

– документирование процессов обеспечения информационной безопасности;

– обучение руководства компании, администраторов информационной безопасности, сотрудников компании – пользователей информационных систем;

– оценка информационной безопасности (периодически, на постоянной основе).

Цифровизация используется практически в каждой сфере бизнеса. В последнее время утечки данных все чаще происходят в процессе развития технологий. Это вынуждает предприятия принимать необходимые меры для обеспечения информационной безопасности, которая призвана стать приоритетной для его развития и становится первостепенной структурой предприятия. Киберугрозы не несут в себе опасности для здоровья и жизни, но являются угрозой для целостности всего предприятия. Каждое действие, связанное с использованием цифровых технологий, оставляет свой след. Злоумышленники могут воспользоваться любой уязвимостью на предприятии, связанной с несоблюдением стандартных правил безопасности: несвоевременное обновление программного обеспечения; использование устаревших антивирусных баз; несвоевременное обучение персонала новым технологиям.

Даже при соблюдении всех базовых условий безопасности присутствуют риски информационной безопасности организаций, среди которых:

– фишинг – вид интернет-мошенничества, нацеленный на получение критически важных данных, учетных записей и т. д.;

– APT-угрозы – сложная постоянная угроза, является высокоточной кибератакой, с помощью которой происходит кража конфиденциальных данных;

– вымогательское ПО – программа-вымогатель, блокирующая доступ к ПК, выводящая на экран надпись с требованием выкупа в обмен на его разблокировку;

– DDOS-атаки – внешнее воздействие на вычислительные источники сервера или рабочей станции с целью выведения их из строя[93].

Для обеспечения безопасности от базовых киберугроз можно использовать как базовые правила информационной безопасности, так и специализированные правила и программы, предотвращающие добычу злоумышленниками необходимых данных. Противодействие киберугрозам становится приоритетной целью для организаций в условиях цифровизации.

Первостепенная задача любой организации – усилить образованность сотрудников в области информационной безопасности. Появление новых угроз требует своевременного реагирования со стороны сотрудников структуры информационной безопасности[94]. При этом необходимо заметить, что разработка комплекса мер должна осуществляться параллельно с процессом создания информационной системы. Решение данной проблемы, ставшей уже мировой, невозможно осуществить только в одном государстве, для этого необходимы усилия международного сотрудничества[95].

7.2. Информационная безопасность в финансовой сфере

Развитие технологий влечет за собой новые проблемы, связанные с обеспечением безопасности. Одна из самых больших угроз связана с экономической безопасностью. В соответствии с Указом Президента от 13 мая 2018 года № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» основными угрозами являются:

– деятельность межгосударственных экономических объединений, созданных без участия Российской Федерации, которая ставит под угрозу национальные интересы России и может нанести им ущерб;

---

[93] Пырчев С. В. Тенденции организованной преступности в развивающемся цифровом мире // Труды Академии управления МВД России. 2020. № 2. С. 142 – 153.

[94] Диканова Т. А. К вопросу углубления интеграции в рамках Евразийского экономического союза при решении проблемы цифровизации и информационной безопасности // Международное сотрудничество евразийских государств: политика, экономика, право. 2019. № 4. С. 102 – 110.

[95] Проблемы информационной безопасности : тр. VIII Междунар. науч.-практ. конф. (Симферополь – Гурзуф, 17 – 19 февраля 2022 г.) / под ред. проф. О. В. Бойченко. – Симферополь : Издат. дом КФУ им. В. И. Вернадского, 2022. С. 18 – 19.

– уязвимость российской финансовой системы перед глобальными рисками;

– низкий объем инвестиций в развитие российской экономики и реального сектора, который обусловлен неблагоприятным инвестиционным климатом;

– низкая активность в инновационной сфере, в том числе слабый уровень внедрения и разработки новых технологий, невысокий уровень квалификации отечественных специалистов;

– недостаточный уровень эффективности государственного управления;

– криминализация экономической сферы и высокий уровень коррупции;

– высокий уровень теневой экономики;

– отсутствие равномерного пространственного развития России, высокий уровень разрыва в развитии темпов и уровня социально-экономического развития регионов и муниципальных образований Российской Федерации [96].

У каждой транзакции существует своя защита. Любая информация должна быть защищена от рук злоумышленников. Защита информации осуществляется с помощью криптографических методов шифрования, аутентификации или определенного аппаратного обеспечения. От длины ключа зависит, насколько тяжело его будет расшифровать и получить желаемую информацию.

При проведении транзакций имеется риск утечки информации, разрушения и потери ценных данных и искажения информации. Для минимизации этих рисков в банках необходимо, чтобы программы по информационной безопасности банка составлялись с учетом следующих особенностей:

– организационной структуры банка;

– направленности информационных потоков;

– количества и характера операций;

– численности клиентов;

– банковские операции проводятся на основе компьютерной информации.

---

[96] Проблемы информационной безопасности.

Для базового обеспечения безопасности транзакций следует проводить тщательный анализ и оптимизацию средств защиты информации, использовать различные уровни обеспечения безопасности в зависимости от рисков и потребностей клиента.

Самая распространенная защита транзакции – это протокол SSL – «Secure Socked Layer», который осуществляет безопасную передачу зашифрованной информации от пользователя к серверу, и технология 3-D Secure. Ее смысл заключается в том, что при каждой операции необходимо подтверждать личность держателя карты в реальном времени, что позволит предотвратить неконтролируемые банком операции.

Быстро развивающаяся и все более опасная среда информационных угроз сегодня повышает необходимость обеспечения безопасности для бизнеса, что в сочетании с более открытым характером современных организаций является испытанием даже для самых обеспеченных ресурсами корпораций.

В середине декабря 2021 года стало известно о первой за три года успешной хакерской атаке на корреспондентский счет Банка России. Согласно данным Group-IB (разработчик решений для детектирования и предотвращения кибератак), кибератака была направлена на систему межбанковских переводов АРМ КДБ (автоматизированное клиентское рабочее место Банка России; через эту систему банки проводят расчеты между собой с корреспондентских счетов, открытых в ЦБ).

Как и все финансовые учреждения, банки подвержены различным операционным и транзакционным рискам, включая преступность, мошенничество со стороны сотрудников и стихийные бедствия. Из-за характера собираемой информации о финансовых операциях и широкого использования технологий для обработки этой информации банки подвержены определенным информационным и технологическим рискам.

Политика информационной безопасности (ПИБ) – это заявление или набор правил, предназначенных для руководства поведением сотрудников в отношении безопасности данных, активов и ИТ-систем компании. ПИБ организаций должна отражать среду риска для конкретной отрасли, определять желаемое поведение и играть важную роль в общем состоянии безопасности организации.

Целью создания эффективной ПИБ является предоставление соответствующих рекомендаций для организации. Политика информаци-

онной безопасности для банков должна охватывать все данные, приложения, системы, сети, клиентов, объекты и инфраструктуру, которые находятся под контролем.

Существуют основные принципы, согласно которым обеспечивается информационная безопасность банка:

– своевременное обнаружение проблемы;

– организация проекта по развитию структуры;

– актуальность и эффективность предпринимаемых решений.

Банки, как и другие компании, используют системный подход, который фокусируется на осведомленности пользователей, разрушая разрозненные технологии и системы, а также объединяя системы безопасности для единого предоставления информации о состоянии разведывательной информации. Организации во всех секторах внедряют новые системы и технологии в свою среду безопасности, в том числе используют собственные устройства для удаленного управления и решения оперативных задач; устройства для мониторинга безопасности в домашних сетях; умные счетчики в инженерных сетях.

Коммерческие банки уделяют особое внимание устойчивости и ситуационной осведомленности. Эти шаги охватывают весь спектр деятельности организации: от требования доступа пользователей к корпоративным ресурсам через виртуальную частную сеть (VPN) и блокировки USB до шифрования жестких дисков и использования центрального «золотого» образа операционных систем с предопределенной программой для добавления или ограничения доступа. Специфика и особенности системы безопасности индивидуальны для каждой банковской организации, поэтому комплексная и профессиональная система безопасности – обязательное условие для всей банковской системы.

В связи с повышением уровня киберпреступности и мошенничества одной из главных целей любого банка стало предотвращение рисков и защита от угроз собственных клиентов в условиях повышения качества обслуживания.

Биометрия – это форма измерения физических характеристик для проверки личности с помощью таких опций, как голос, отпечатки пальцев, лицо, сетчатка или радужная оболочка глаза, инфракрасная термограмма вены или комбинация этих идентификаторов.

Методы биометрической идентификации могут быть достигнуты на мобильных устройствах либо через встроенные биометрические

датчики путем прикрепления к ним портативного биометрического оборудования через USB-кабель либо через соединение Wi-Fi. Вот несколько методов биометрической аутентификации, которыми банки уже пользуются[97]:

– сканирование радужной оболочки глаза;

– распознавание голоса;

– распознавание лица;

– сканирование отпечатков пальцев;

– аутентификация шаблона вен.

Эти режимы биометрической аутентификации могут использоваться в различных банковских сценариях, включая снятие и депонирование наличных в банкоматах, проверку личности при обращении в свой банк и (чаще всего) аутентификацию мобильных банковских приложений[98].

Еще одной возможностью предотвращения развития мошенничества стала поведенческая биометрия. Это инновационный подход к аутентификации пользователей, основанный на создании уникального профиля для каждого клиента.

Сегодня, применяя передовые технологии больших данных и машинного обучения, поведенческая биометрия использует богатое сочетание личных и аппаратных характеристик, чтобы отличать законных клиентов от мошенников.

Как правило, наиболее часто используемый тип поведенческой биометрии включает в себя автоматическое распознавание шаблонов, таких как нажатия на экран устройства или на его клавиши. Кроме того, эти человеческие черты усиливаются устройствами, такими как IP-адреса и геолокация. Затем к каждой транзакции могут применяться правила оценки рисков, гарантируя, что всегда предлагается соответствующий уровень аутентификации[99].

---

[97] Моногарова А. А., Курзанов И. Д., Николайчук О. А. Биометрия как способ удаленной идентификации в банковском секторе // Научный формат. 2019. № 3 (3). С. 89 – 90.

[98] Шаманина Е. И., Захаренко Ю. С. Биометрические технологии как перспективное направление совершенствования дистанционного банковского обслуживания // Вестник ГУУ. 2020. № 5. С. 193 – 199.

[99] Винокуров А. В. Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству // Финансы и кредит. 2016. № 22. Вып. 21. С. 15 – 23.

Соответственно, если обнаружен повышенный риск операции, такой как необычное местоположение или неизвестный IP-адрес, транзакция может быть заблокирована или будет произведен запрос дополнительной аутентификации.

Биометрические технологии, такие как поведенческая биометрия и биометрические карты, дают банкам возможность оставаться на шаг впереди мошенников, которые продолжают совершенствовать свои действия с точки зрения масштаба, сложности и амбиций. Помимо этого российские банки производят сбор биометрических данных клиента с целью снижения собственных рисков, а также повышения скорости обслуживания клиентов.

Единая биометрическая система была запущена Банком России и «Ростелекомом» летом 2018 года. В обоих случаях сдача биометрии для клиентов является добровольной. Биометрическая идентификация позволяет развивать дистанционное обслуживание, что расширяет спектр возможностей клиента, а также повышает уровень доступности и скорости проведения банковских операций.

Например, в конце 2021 года Российский национальный коммерческий банк (РНКБ) первым в Крыму провел дистанционную сделку по выдаче ипотечного кредита с использованием биометрических данных клиента для идентификации. Житель Екатеринбурга получил ипотечный кредит на приобретение квартиры в Крыму без посещения банковского офиса.

С развитием биометрических технологий пароли, PIN-коды и контрольные вопросы становятся менее безопасным вариантом для мобильного банкинга. Существует множество факторов, которые следует учитывать при внедрении биометрии в банковскую систему, чтобы в полной мере оптимизировать качество обслуживания клиентов. Это включает в себя дальнейшее сокращение и смягчение ошибок в технологии, поиск идеального баланса между обслуживанием клиентов и безопасностью, а также обеспечение согласованности и полной интеграции всех услуг и процессов. Биометрические технологии с успехом применяются в преобразовании клиентского опыта в банковской сфере, сделав ее более плавной, быстрой и безопасной, чем когда-либо прежде.

Безопасность финансовых учреждений не гарантируется каким-либо определенным методом, необходимо выбирать лучшие доступные решения для защиты своих клиентов, а также повышения качества обслуживания и уровня доступности собственных услуг.

7.3. Особенности обеспечения информационной безопасности мобильных и интернет-систем

Эпидемия коронавируса, карантин и режим домашней изоляции показали неготовность многих предприятий к организации эффективной удаленной работы своих сотрудников. Новые вспышки заболеваний вызвали массовый переход на «удаленку», сделав процесс обеспечения перехода на удаленный режим работы для организаций и предприятий актуальным и востребованным.

Статистические данные, предоставленные аналитиками Gartner, в очередной раз подтверждают тенденцию устойчивого роста расходов на информационную безопасность в связи с возросшим спросом на технологии для обеспечения удаленной работы, вызванным пандемией коронавируса. Рост расходов на информационную безопасность в 2020 году достиг 133,78 млрд дол., что на 6,4 % больше, чем в 2019 году. В 2021 году, по данным аналитиков Astute Analytica, мировой рынок кибербезопасности достиг 162,9 млрд дол.[100].

При распределении бюджета на информационную безопасность принято рассматривать три ключевые составляющие: защитные меры, технические средства и людей. Важно анализировать потенциальные возможности использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации. Проводить регулярное тестирование на проникновение и инвентаризацию ресурсов необходимо в комплексе с мониторингом инцидентов безопасности, учитывая при этом ретроспективный анализ системных событий и непрерывную защиту веб-приложений и серверов.

В условиях пандемии неравномерность влияния на индустрию информационной безопасности отразилась в повышении спроса на средства защиты конечных точек (антивирусы, EDR/XDR-системы), востребованными стали средства удаленного подключения и контроля удаленных сотрудников (VPN, MFA, PAM/PUM). Отмечено снижение спроса на периметральную защиту, межсетевые экраны/NGFW и системы мониторинга безопасности. Переход на дистанционный формат

---

[100] Gartner / Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide- security-and-risk-managem (дата обращения: 18.12.2022).

работы вызвал необходимость проведения разработки эффективной системы контроля-учета рабочего времени и поиска новейших решений для предотвращения утечек данных. Особый интерес у компаний вызывает тестирование на проникновение. При этом замораживаются долгосрочные и крупные проекты развития информационной безопасности[101].

Проведенный анализ положительных и отрицательных сторон удаленной работы позволяет сделать вывод, что основными отрицательными моментами для руководителей предприятия становятся сложность осуществления контроля за действиями сотрудников в рабочее время, а также сложность контроля защиты информации, которую они обрабатывают и впоследствии передают через интернет коллегам или в офис. Таким образом, при удаленной работе возникает необходимость осуществления:

– контроля доступа к информации – обеспечение контроля взаимодействия, доступа к информации и передачи информации;

– аутентификации – обеспечение контроля надежности доступа и контроля доступа к учетной записи[102].

Создание безопасного удаленного доступа предполагает безопасное VPN-подключение, своевременное определение кибератак и молниеносную реакцию на них, введение двухфакторной аутентификации, поддержание в актуальном состоянии программно-аппаратного комплекса защиты, актуализацию подхода к построению MDM-решений, расширение возможностей стандартных антивирусов, облачные решения.

Конечно, предприятия не располагают таким средствами, чтобы для работы на «удаленке» обеспечить каждого сотрудника служебным ноутбуком и набором средств защиты для него. Однако тренд удаленной работы в ближайшее время вряд ли пойдет на спад, работать и учиться будем все больше удаленно, поэтому разработка и применение приложений, обеспечивающих удаленный доступ к компьютерам, должны быть направлены на облегчение данного процесса, включая повышенный уровень безопасности.

---

[101] Бойченко О. В., Бахши Д. Г. Механизмы защиты данных сетевых информационных технологий // Проблемы информационной безопасности : тез. докл. III Междунар. науч.-техн. конф., 16 –18 февр. 2017 г. Симферополь, 2017. С. 153 – 154.

[102] Бойченко О. В., Журавленко Н. В. Информационная безопасность : учеб. пособие для студентов высш. учеб. заведений. Симферополь, 2016. 248 с.

Понимая, что массовый и быстрый перевод сотрудников на удаленную работу может привести к серьезным угрозам информационной безопасности как самих информационных систем, так и всех корпоративных и персональных данных компании, необходимо искать решение таких проблем в создании комплексных средств обеспечения информационной безопасности при удаленной работе.

Комплексное решение обеспечения информационной безопасности должно включать:

– своевременное обнаружение и предотвращение угроз информационной безопасности;

– организацию расследования инцидентов;

– проведение анализа деятельности сотрудников;

– инвентаризацию программного и аппаратного обеспечения;

– удаленное администрирование машин пользователей.

Таким образом, применение комплексного подхода при создании систем информационной безопасности должно обеспечить как применение технических средств защиты, так и решение вопросов по управлению и упорядочению информационной безопасности, гарантируя защиту информационных активов и снижая информационные риски[103].

В дальнейшем индустрия систем безопасности будет неуклонно развиваться, несмотря на влияние на рынок различных социальных и экономических факторов, поэтому для малого и среднего бизнеса важно освоить и внедрить высокотехнологичные решения, основанные на искусственном интеллекте, облачных вычислениях, интернете вещей, уделяя при этом особое внимание вопросам обеспечения информационной безопасности. Важно понимать, что сфера безопасности в перспективе будет не только обеспечивать защиту, но и способствовать повышению эффективности бизнеса, создавать дополнительную ценность для пользователей, компаний и общества. В таких условиях всегда востребованы квалифицированные кадры, дефицит которых ощущается постоянно.

Отметим, что полностью исключить вероятность взлома всей корпоративной сети или отдельного персонального компьютера

---

[103] Бойченко О. В., Федосеева К. Н. Место и роль интернет-технологий в современной экономике // Актуальные проблемы социально-экономического развития общества : тез. докл. II науч.-техн. конф., 21 февр. 2017 г. Феодосия, 2017. С. 195 – 199.

нельзя. Приведем закон Мерфи: «Если есть вероятность того, что какая-нибудь неприятность может случиться, то она обязательно произойдет». Наша задача сделать так, чтобы вероятность такого взлома была минимальной.

Мобильные приложения можно отнести к широко используемым сервисам, которые, в свою очередь, осуществляют сбор, хранение и передачу информации[104]. Таким образом, возможность эксплуатации программных уязвимостей в таких мобильных приложениях может привести к серьезному ущербу как для разработчиков таких мобильных приложений, так и для самих пользователей. В связи с этим актуальным становится вопрос по разработке комплекса мер по осуществлению анализа, выявлению и предупреждению возможных угроз в мобильных приложениях. Для того чтобы анализировать мобильные приложения на предмет наличия угроз и уязвимостей с частично либо полностью недоступным исходным кодом на таких платформах, как Android и IOS, применяют следующие методы:

1. Анализ программного кода на наличие стороннего программного кода исходя из открытых источников. В контексте исследования программных компонентов исходный код, который является недоступным, наличие стороннего программного кода можно определить на основании символьной информации в двоичном образе данных компонентов. При наличии стороннего программного кода можно проводить его анализ на наличие уязвимостей.

2. Метод обратной разработки. В процессе данного метода проводят обратную компиляцию, дизассемблирование программного кода, а также используют другие инструменты и методы для декомпиляции.

3. Статический анализ на выявление потенциальных угроз в работе исходного кода в случае успешного процесса декомпиляции кода.

4. Ручной анализ исходного кода для выявления угроз, которые потенциально могли быть не выявлены с помощью средств статического анализа[105].

---

[104] Александров Я. А., Сафин Л. К., Трошина К. Н. Статический бинарный анализ мобильных приложений для платформы Android по требованиям информационной безопасности // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2016. № 3. С. 44 – 49.

[105] Сафин Л. К., Чернов А. В., Александров Я. А. Исследование информационной защищенности мобильных приложений // Вопросы кибербезопасности. 2015. № 4 (12). С. 28 – 37.

Мобильные и интернет-системы постоянно подвергаются угрозам[106]. Можно выделить наиболее острые киберугрозы и создать условия для решения задач противодействия современным деструктивным вызовам, связанным с киберпреступностью.

1. Недооценка количества существующего на сегодняшний день вредоносного ПО абсолютным большинством российских компаний (91 %) наряду с тем, что число «зловредов» постоянно увеличивается, а целенаправленность воздействия совершенствуется (таргетированные атаки). Среди внешних киберугроз наибольшее опасение у бизнеса по-прежнему вызывает вредоносное ПО (77 %), затем следуют проблема спама (74 %), фишинговые атаки (28 %), корпоративный шпионаж (26 %) и сетевые вторжения (23 %), а также распространение DDoS-атак, кража мобильных устройств и крупного оборудования (финальная сумма ущерба для крупных компаний в среднем составила 20 млн руб. за каждую успешную кибератаку, а для предприятий среднего и малого бизнеса — почти 800 тыс руб.).

2. Рост инцидентов, обусловленных внутренними угрозами организаций (87%). В первую очередь это уязвимости в ПО, затем случайная или намеренная утечка данных, утечка данных через мобильные устройства, что связано с потерей мобильных устройств сотрудниками и мошенничеством работников (20 %).

3. Несовершенство разработанных политик безопасности, ориентированных на запрещение; отсутствие соответствующих инструментов контроля, которые позволят гарантировать соблюдение всех требований. При этом следует выделить ошибочное акцентирование типов информации, интересующей злоумышленников. Так, для компании наиболее важной считается информация о клиентах, финансовых и операционных данных, интеллектуальной собственности, а также информация по анализу деятельности конкурентов, платежная информация, персональные данные сотрудников и данные о корпоративных счетах в банках. При этом киберпреступники чаще всего крадут внутреннюю операционную информацию компаний (56 %), персональные данные сотрудников (26 %) и финансовые данные (19 %).

---

[106] Проблемы информационной безопасности. С. 83 – 84.

На основании анализа исследований в данной сфере можно сформулировать наиболее эффективные меры защиты от киберугроз:

– антивирусное ПО наряду с организацией защиты от таргетированных атак;

– построение комплексной системы защиты, охватывающей всю ИТ-инфраструктуру предприятия для предотвращения утечки данных и противодействия DDoS-атакам, делающим недоступными веб-ресурсы компании;

– управление обновлениями для своевременного закрытия уязвимостей в ПО наряду с практикой контроля приложений, позволяющей ограничивать использование некритичных для бизнеса программ, избегая ряда уязвимостей.

7.4. Обеспечение информационной безопасности данных и систем электронного документооборота

Big Data, или большие данные, – область знаний, которая включает в себя наборы разнообразных данных, способы их извлечения и методы анализа. Массивы таких данных довольно многообразные, неструктурированные, зачастую содержат некачественные участки. Большие данные – это не база данных (БД), в отличие от БД большие данные быстро накапливаются и самый обычный компьютер просто не справляется с их обработкой.

Постоянный рост и увеличение данных приводит к мысли о необходимости существования платформы или механизма, позволяющего собирать и хранить информацию без потери конфиденциальности и надлежащего вида. В конечном итоге отсутствие подходящей инфраструктуры создает проблему информационной безопасности больших данных.

Существует несколько проблем с обеспечением защиты Big Data, которые могут поставить под угрозу их безопасность.

1. Расширенные аналитические инструменты для неструктурированных больших данных и нереляционных БД (NoSQL). На практике – это новейшие технологии, которые до сих пор находятся в активной разработке, поэтому программному обеспечению и процессам информационной безопасности достаточно сложно защитить эти новые наборы инструментов.

2. Большие данные характеризуются размерами от терабайтов до петабайтов, что слишком велико для обычных проверок безопасности. Важно учитывать, что большая часть платформ основана на кластерах, что создает множество уязвимостей на узлах и серверах.

3. Имеет большое значение и то, что зачастую владельцы больших данных не проводят плановое обновление ПО безопасности, что подвергает его риску потери и раскрытия данных. Инструменты ИБ также должны быть настроены на отслеживание и предупреждение подозрительных действий[107].

4. Помимо постоянно растущего количества данных существует проблема того, что довольно часто эти данные могут находиться в открытом доступе[108]. Например, они могут быть использованы в коммерческих целях любым заинтересованным лицом без ограничений, авторских прав и патентов.

По этим причинам необходима реализация безопасности Big Data независимо от того, требуется ли в компании обновление системы безопасности или она нуждается в первоначальных решениях для обеспечения защиты больших данных.

К основным инструментам безопасности больших данных можно отнести следующие: шифрование, контроль учетных записей пользователя, обнаружение и предотвращение кибератак, физическая безопасность, регулярный плановый мониторинг и аудит системы. Благодаря вышеперечисленным мерам данные будут защищены в ходе передачи и хранения, аудит безопасности в реальном времени даст специалисту возможность оценить положение в целом, прежде чем оно станет критическим, а обучение сотрудников предотвратит их от случайных ошибок, что служит также одной из наиболее серьезных уязвимостей для злоумышленников[109].

---

[107] What is Big Data Security? Challenges & Solutions / Datamation [Электронный ресурс]. URL: https://www.datamation.com/big-data/big-data-security/#types (дата обращения: 18.12.2022).

[108] Титаренко Д. В., Исмайлов Э. И. Безопасность больших данных // Проблемы информационной безопасности социально-экономических систем : тез. докл. VII Всерос. междунар. науч.-практ. конф. Симферополь : Крым. федер. ун.-т им. В. И. Вернадского, 2021. С. 121 – 122.

[109] What is Big Data Security? Challenges & Solutions / Datamation.

На данный момент не представляется возможным назвать один универсальный и результативный инструмент по обеспечению информационной безопасности Big Data. Однако важно учитывать, что если своевременно не предпринимать соответствующие меры, то в будущем можно столкнуться с глобальной утечкой данных, которая может повлечь за собой материальный ущерб[110].

Обнаружение корпоративных данных в открытом доступе может привести не только к потере доверия клиентов, но и конкурентного преимущества для организации. В связи с этим защита больших данных от внешних и внутренних угроз считается первостепенной задачей для аналитика в области информационной безопасности на предприятии.

В связи с широкой человеческой деятельностью в электронных базах данных, а также в пространстве сети Интернет следует использовать концепции информационной безопасности в корпоративных информационных системах. Они строятся на принципах и положениях по созданию и функционированию информации в защищенной среде, заложенных в требованиях, ГОСТах, указах Президента Российской Федерации, постановлениях Правительства Российской Федерации, в Доктрине информационной безопасности Российской Федерации, а также международных договорах и соглашениях, заключенных или признанных Российской Федерацией и др.

Таким образом, прежде чем создавать корпоративную информационную систему, нужно разработать концепцию информационной безопасности, включающую в себя телекоммуникацию и информационную часть, которые образуют инфокоммуникационную среду. Первый этап состоит в выделении объекта защиты и состава информационной инфраструктуры, которая будет опираться на эту систему. Второй шаг – определение реестра защищаемых ресурсов и составление их списка, а также какого класса информационная система должна быть установлена.

---

[110] Шакиров А. А., Зарипова Р. С. Проблемы обеспечения информационной безопасности больших данных // Информационные технологии в строительных, социальных и экономических системах. 2019. № 3 – 4(17 – 18). С. 150 – 152.

Говоря о системах отечественного документооборота, можно привести несколько примеров. Лидерами индустрии СЭД в России являются компании Documentum и «ДокументумСервисиз». Система стоится на управлении документами, знаниями, бизнес-процессами и используется для крупных предприятий и организаций; имеет довольно высокую стоимость внедрения, так как является своего рода конструктором, собирающим в себя необходимую функциональность, и далека от коробочной системы, поэтому имеет смысл внедрять ее в больших компаниях с наличием квалифицированных кадров, знающих тонкости работы. Платформа представляет собой готовый продукт, предназначенный для создания распределенных архивов, динамического управления содержимым корпоративных интернет-порталов, управления проектами в распределенных проектных группах, для организации корпоративного делопроизводства, а также стандартов поддержки качества.

Другой крупной системой можно назвать «Евфрат», которая является простым электронным архивом с базовыми возможностями контроля исполнения. Система разработана компанией «CognitiveTechnologies», предлагающей продукты различного масштаба. Одним из вариантов для крупных компаний является «Евфрат Клиент-сервер», в нем в качестве клиентской части разработан самостоятельный продукт, независимый от серверного компонента «Евфрат-Офис» и представляющий собой ярлык на рабочем столе, имеющий неограниченное количество папок с ссылками на различные файлы. Особенность системы состоит в возможности открыть файл любого вида, недостаток – невозможно отследить получение и возврат документа.

Таким образом, система выступает средством для сканирования, регистрации, распознавания документа, присвоения реквизитов, поиска и незначительного контроля за исполнением; в отличие от предыдущей системы «Евфрат» – это недорогой продукт, который будет полезен и в малом офисе.

Если говорить о полностью российских разработках, то система CompaniMedia, разработанная на основе LotusNotes, является продуктом компании «Интертраст»; содержит набор сервисов, обеспечивающих

контроль исполнения, управление персоналом и проектами, коллективное создание документов и др. Особенность системы в том, что, независимо от территориальной структуры и качества передачи связи, она обеспечивает доставку документов, может служить как базой для делопроизводства, так и средством поддержки между сотрудниками.

Продукт «Эффект-Офис» петербургской компании «Гарант Интернешнл» имеет невысокую цену и ориентирован на небольшие компании, которые нуждаются в решении задач начального уровня. При этом содержит электронный архив со средствами поиска информации, регулирует доступ к архиву, имеет средства автоматизации делопроизводства и собственную электронную почту, что очень упрощает процесс, и все операции происходят в самой системе. Таким образом, современные системы совершенствуют сервисные возможности, так как базовые были уже реализованы ранее. Следует отметить, что разработчиков таких систем в России очень много, и они производят качественный готовый продукт для разного рода организаций. Если говорить о развитии СЭД в управлении различного вида мультимедийными технологиями, то спрос на нее в нашей стране начал формироваться недавно.

На основании изученных систем электронного документооборота, которые применяются как в государственной и архивной сферах, так и в частной, можно сделать вывод, что в современном мире объем информации, хранящейся в электронном виде в связи с внедрением компьютеров во все сферы жизни человека вырос в тысячу раз, а вместе с ним и возросло количество несанкционированных вмешательств в корпоративную информационную сеть. Перечислим методы проникновения в систему и меры их профилактики. Один из самых простых способов взломать систему и получить доступ к базе данных – это использование перехватчиков ввода с клавиатуры. Метод защиты прост: использование только одного компьютера для работы системы. Подбор или расшифровка пароля также наблюдаются довольно часто. Методом защиты служит постоянная смена паролей в личных кабинетах. Можно выделить и более широкомасштабную операцию: применение сетевых вирусов. В данном случае защититься от мошенников будет

намного сложнее, однако если проводить фильтрацию и мониторинг, регулярное сканирование сети, то риски существенно снизятся. Защищаются не только шифрованием и частой сменой пароля, но и аппаратными средствами, например, сетевыми адаптерами от угрозы перехвата пакетов. Сложнее использовать подмену IP-адреса, или спуфинг, который невозможно отследить из-за входа в систему без пароля. Методом защиты от такого рода воздействия со стороны может служить фильтрация пакетов, поступающих из Интернета.

Таким образом, нужно применять все предложенные способы защиты систем современного электронного документооборота как на государственном уровне, так и в корпоративных структурах.

Темы для обсуждения

1. Расскажите, насколько важно сформировать концепцию информационной безопасности организации?
2. Назовите наиболее значимые угрозы информационной безопасности.
3. Оцените значение Центрального банка РФ при обеспечении информационной безопасности операций.
4. Какие угрозы информационной безопасности можно выделить в финансовом секторе?
5. Проанализируйте эффективность биометрической идентификации.
6. Какие угрозы информационной безопасности создает удаленная работа сотрудников?
7. Раскройте методы защиты мобильных приложений, которые следует использовать.
8. Какие возможности и угрозы создает использование СЭД в организации?

Задание для самоконтроля

1. Охарактеризуйте основные принципы построения системы информационной безопасности.
2. Опишите основные этапы построения системы информационной безопасности.

3. Приведите примеры угроз, характерных для банковского сектора.

4. Охарактеризуйте особенности биометрической идентификации.

5. Дайте характеристику системы обеспечения информационной безопасности мобильных систем.

6. Дайте характеристику системы обеспечения информационной безопасности интернет-систем.

7. Проанализируйте систему информационной безопасности СЭД.

Библиографический список

1. Новости в России и мире [Электронный ресурс]. – Режим доступа: https://tass.ru/ekonomika/12465313 (дата обращения: 18.11.2022).

2. Касперская, Н. И. Необходимо минимизировать риски цифровой экономики для граждан, общества и государства. 2018 г. [Электронный ресурс]. – Режим доступа: https://agenda-u.org/news/natalyakasperskaya-neobhodimo–minimizirovat-riski-cifrovoy-ekonomiki-dlya-grazhdan-obshchestva (дата обращения: 18.11.2022).

3. Развитие цифровой экономики как фактор повышения уровня экономической безопасности страны : монография / под ред. А. К. Моденова. – СПб. : С.-Петерб. гос. архитектурно-строит. ун-т, 2020. – 316 с.

4. Проблемы информационной безопасности : тр. VIII Междунар. науч.-практ. конф. (Симферополь – Гурзуф, 17 – 19 февраля 2022 г.) / под ред. проф. О. В. Бойченко. – Симферополь : Издат. дом КФУ им. В. И. Вернадского, 2022. – 126 с.

5. Моногарова, А. А. Биометрия как способ удаленной идентификации в банковском секторе / А. А. Моногарова, И. Д. Курзанов, О. А Николайчук // Научный формат. – 2019. – № 3 (3). – С. 89 – 90.

6. Шаманина, Е. И. Биометрические технологии как перспективное направление совершенствования дистанционного банковского обслуживания / Е. И. Шаманина, Ю. С. Захаренко // Вестник ГУУ. – 2020. – № 5. – С. 193 – 199.

7. Винокуров, А. В. Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству / А. В. Винокуров // Финансы и кредит. – 2016. – № 22. – Вып. 21. – С. 15 – 23.

8. Gartner / Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021 [Электронный ресурс]. – Режим

доступа: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide– security-and-risk-managem (дата обращения: 18.11.2022).

9. Бойченко, О. В. Механизмы защиты данных сетевых информационных технологий / О. В. Бойченко, Д. Г. Бахши // Проблемы информационной безопасности : тез. докл. III Междунар. науч.-техн. конф., 16 – 18 февраля 2017 г. – Симферополь, 2017. – С. 153 – 154.

10. Бойченко, О. В. Информационная безопасность : учеб. пособие для студентов высш. учеб. заведений / О. В. Бойченко, Н. В. Журавленко. – Симферополь, 2016. – 248 с.

11. Бойченко, О. В. Место и роль интернет-технологий в современной экономике / О. В. Бойченко, К. Н. Федосеева // Актуальные проблемы социально-экономического развития общества : тез. докл. II науч.-техн. конф., 21 февраля 2017 г. – Феодосия, 2017. – С. 195 – 199.

12. Статический бинарный анализ мобильных приложений для платформы Android по требованиям информационной безопасности / Я. А. Александров [и др.] // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. – 2016. – № 3. – С. 44 – 49.

13. Исследование информационной защищенности мобильных приложений / Л. К. Сафин [и др.] // Вопросы кибербезопасности. – 2015. – № 4 (12). – С. 28 – 37.

14. What is Big Data Security? Challenges & Solutions / Datamation [Электронный ресурс]. – Режим доступа: https://www.datamation.com/big-data/big-data-security/#types (дата обращения: 18.11.2022).

15. Титаренко, Д. В. Безопасность больших данных / Д. В. Титаренко, Э. И. Исмайлов // Проблемы информационной безопасности социально-экономических систем : VII Всерос. междунар. науч.-практ. конф., Гурзуф, 18 – 20 февраля 2021 г. – Симферополь : Крым. федер. ун-т им. В. И. Вернадского, 2021. – С. 121 – 122.

16. Шакиров, А. А. Проблемы обеспечения информационной безопасности больших данных / А. А. Шакиров, Р. С. Зарипова // Информационные технологии в строительных, социальных и экономических системах. – 2019. – № 3 – 4(17 – 18). – С. 150 – 152.

ЗАКЛЮЧЕНИЕ

Переход современной экономики к цифровому типу развития приводит к усложнению методов и механизмов управления компаниями. Это требует новых решений, так как старые подходы теряют свою актуальность и перестают быть эффективными. Сегодня предприятиями и организациями нужно управлять точнее и быстрее, так как сам объект управления усложняется, обретая все новые технологические свойства.

Настоящие реалии функционирования компаний, особенно крупных, таковы, что в условиях цифровой экономики наиболее рентабельным оказывается использование информационных технологий. Их применение определяет в конечном итоге успешность работы и конкурентоспособность организации, формирует и удерживает клиентскую и партнерскую базы, обеспечивает возврат производимых компанией инвестиций.

По мере постепенного превращения информационных технологий в неотъемлемый атрибут любого предприятия или организации, в эффективный инструмент конкурентной борьбы к ним и формируемым на их основе информационным системам и платформам начали предъявлять особые требования. Это обстоятельство, в свою очередь, повлекло за собой необходимость разработки новых подходов к обеспечению информационной безопасности.

В учебном пособии в краткой форме изложен материал, содержащий систему научных знаний, которая составляет теоретическую основу информационной безопасности в различных экономических системах. Раскрывается широкий спектр вопросов: угрозы информационной безопасности: понятия, виды, классификация и риски; основы защиты информации; построение системы защиты информации и ее со-

держание (обеспечение информационной безопасности); преднамеренные и непреднамеренные угрозы информационной безопасности и борьба с ними (непреднамеренный человеческий фактор, вредоносные программы и компьютерные вирусы: виды и способы борьбы, типовые удаленные атаки в глобальных компьютерных сетях); элементы аудита системы информационной безопасности; вопросы государственного обеспечения системы информационной безопасности; аспекты информационной безопасности в социально-экономических системах.

Представленный в книге материал формирует у студентов:

– способность применять правовые, организационные, технические и программные средства защиты информации;

– понимание сущности информационной безопасности;

– знание основных моделей и принципов защиты информации от несанкционированного доступа;

– умение создавать программные средства защиты информации.

Авторы пособия ставили перед собой задачи пробуждения у студентов интереса к проблемам обеспечения информационной безопасности в организациях, понимания важности оценивания уровня информационной безопасности и активного овладения обучающимися методами защиты информации.

РЕКОМЕНДАТЕЛЬНЫЙ БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Вострецова, Е. В. Основы информационной безопасности [Электронный ресурс] : учеб. пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с. – Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 26.10.2022).

2. Гафнер, В. В. Информационная безопасность [Электронный ресурс] : учеб. пособие. В 2 ч. Ч. 1 / В. В. Гафнер. – Екатеринбург : Урал. гос. пед. ун-т, 2009. – 155 с. – Режим доступа: http://elar.uspu.ru/bitstream/uspu/4122/1/uch00029.pdf (дата обращения: 26.10.2022).

3. Голиков, А. М. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / А. М. Голиков. – Томск : Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 288 с. – Режим доступа: https://edu.tusur.ru/publications/1024/download (дата обращения: 26.10.2022).

4. Зенков, А. В. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие для вузов / А. В. Зенков.– М. : Юрайт, 2022. – 104 с. – (Высшее образование). – Режим доступа: https://urait.ru/bcode/497002 (дата обращения: 26.10.2022).

5. Информационная безопасность [Электронный ресурс] : учеб. пособие / В. Н. Ясенев [и др.] / под общ. ред. проф. В. Н. Ясенева. – Н. Новгород : Нижегород. гос. ун-т им. Н. И. Лобачевского, 2018. – 182 с. – Режим доступа: http://www.iee.unn.ru/wp-content/uploads/sites/9/2018/09/Yasenev_posobie_ isecurity.pdf (дата обращения: 26.10.2022).

6. Партыка, Т. Л. Информационная безопасность [Электронный ресурс] : учеб. пособие / Т. Л. Партыка, И. И. Попов. – 3-е изд., перераб. и доп. – М. : ФОРУМ, 2010. – 432 с. – (Профессиональное образование). – Режим доступа: http://kfilial.mggeu.ru/wp-content/uploads/2021/02/Partyka-T.L.-Popov-I.I.-Informatsionnaya-bezopasnost-1.pdf (дата обращения: 26.10.2022).

7. Сухостат, В. В. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / В. В. Сухостат, И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с. – Режим доступа: https://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informaczionnoj-bezopasnosti.pdf (дата обращения: 26.10.2022).

8. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 26.10.2022).

Учебное издание

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Авторы-составители:

ТЕСЛЕНКО Ирина Борисовна
ВИНОГРАДОВ Дмитрий Викторович
ГУБЕРНАТОРОВ Алексей Михайлович
и др.

Редактор А. П. Володина
Технические редакторы Ш. Ш. Амирсейидов, Н. В. Пустовойтова
Компьютерная верстка Е. А. Герасиной
Выпускающий редактор А. А. Амирсейидова

Подписано в печать 04.10.23.
Формат 60×84/16. Усл. печ. л. 12,32. Тираж 30 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.