МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ
ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

ГРИГОРЬЕВ А.Н., ИВАНОВ П.Ю.,
КАСЬЯНОВ М.А., ФАДЕЕВА В.В.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Допущено Министерством внутренних дел
Российской Федерации в качестве учебного пособия
для курсантов и слушателей образовательных организаций
высшего образования системы МВД России

Москва
2018

УДК 004.056.5(075)
ББК Х.с51я73
Г83

Рецензенты:
В.А. Кемпф, кандидат технических наук, доцент
(Барнаульский юридический институт МВД России);
А.Н. Бабкин, кандидат технических наук, доцент
(Воронежский институт МВД России);
А.И. Горев, кандидат юридических наук, доцент
(Омская академия МВД России);
Д.В. Гоготова
(Департамент информационных технологий,
связи и защиты информации МВД России)

Авторский коллектив:
А.Н. Григорьев, доктор педагогических наук,
кандидат юридических наук, доцент;
П.Ю. Иванов;
М.А. Касьянов;
В.В. Фадеева, доктор педагогических наук, профессор

Г83 **Григорьев А.Н., Иванов П.Ю., Касьянов М.А., Фадеева В.В.** Основы информационной безопасности органов внутренних дел: учебное пособие. — М.: ДГСК МВД России, 2018. — 208 с.

Издание посвящено актуальным вопросам обеспечения информационной безопасности органов внутренних дел. В нем рассматриваются теоретические и практические аспекты обеспечения информационной безопасности органов правопорядка. Значительное внимание уделяется вопросам защиты информации от утечки по техническим каналам, обеспечения безопасности информации и информационных процессов в современных компьютерных системах и сетях.

Пособие предназначено для научно-педагогических работников, адъюнктов, курсантов и слушателей образовательных организаций системы МВД России, практических сотрудников органов внутренних дел Российской Федерации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время в связи с произошедшей коренной переоценкой ценностей многие традиционные ресурсы человеческого прогресса утрачивают свое первостепенное значение. Однако, информация по-прежнему остается одним из главных ресурсов научно-технического и социально-экономического прогресса мирового сообщества. В перспективе хорошо развитая информационно-телекоммуникационная сеть будет играть в повседневной жизни такую же роль, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Информация влияет не только на ускорение прогресса в науке и технике, но и на обеспечение охраны общественного порядка, сохранности собственности, общение между людьми и другие общественно значимые области. Она пронизывает все области жизнедеятельности современного общества, так как принятие любого решения основано, прежде всего, на анализе информации.

Информационная сфера играет всевозрастающую роль в обеспечении безопасности государства и общества. Именно через эту сферу реализуется значительная часть угроз национальной безопасности.

Одним из основных источников угроз информационной безопасности является деятельность криминальных группировок и организаций. В течение последних десятилетий отмечается неуклонная тенденция профессионализации преступности, которая приобретает все более организованный характер. Обладая значительными финансовыми возможностями и не будучи связанными требованиями закона, преступные формирования выстраивают свою, достаточно эффективную систему противодействия органам правопорядка. Нередко в этих целях они используют новейшие информационные технологии и технические средства.

Данные обстоятельства позволяют констатировать тот факт, что в своей практической деятельности сотрудники органов внутренних дел сталкиваются со все усиливающимся информационно-техническим противодействием со стороны криминального мира, осуществляемым, в том числе, и с использованием различных средств технической разведки. В этой связи сотрудники правоохранительных органов обязаны иметь представление о характере информационного противодействия их деятельности со стороны преступной среды. Это позволит своевременно и надежно перекрыть каналы утечки информации и в конечном счете защитить деятельность по выявлению, раскрытию и расследованию преступлений от противодействия криминальной среды.

Данное учебное пособие предназначено для использования при проведении занятий по курсу «Основы информационной безопасности в органах внутренних дел» с курсантами и слушателями образовательных организаций МВД России, обучающимися по специальностям 40.05.01 «Правовое обеспечение национальной безопасности» и 40.05.02 «Правоохранительная деятельность».

Пособие состоит из пяти глав. В первой главе содержится материал по общетеоретическим основам обеспечения информационной безопасности органов внутренних дел, который представлен с учетом специфики профес-

сиональной деятельности сотрудников полиции. Проведен подробный анализ информации не только как общенаучной категории, но и как объекта правового регулирования, защиты. Рассмотрено соотношение понятий «информационная безопасность» и «защита информации». Исследованы структура и содержание понятия «информационная безопасность органов внутренних дел».

Во второй главе учебного пособия рассмотрены методы и средства защиты информации в органах внутренних дел, понятие системы обеспечения информационной безопасности органов внутренних дел (ОВД) и обобщенный алгоритм ее построения, проведен анализ организационно-правовых основ обеспечения защиты информации, а также проблем обеспечения безопасности информации в сфере деятельности по борьбе с преступностью.

В третьей главе рассмотрены вопросы защиты информации на объектах информатизации органов внутренних дел. Основное внимание уделено анализу технических каналов утечки информации, а также вопросам организации инженерно-технической защиты информации. Даны практические рекомендации по оборудованию служебных помещений ОВД по требованиям защиты информации.

Четвертая глава посвящена защите информационных процессов в компьютерных системах. Рассмотрены основные угрозы безопасности информации в компьютерных системах, понятие, виды и общая характеристика преступлений в сфере компьютерной информации. Особое внимание уделено методам и средствам защиты компьютерной информации от несанкционированного доступа, а также антивирусной защите компьютерных систем.

В пятой главе пособия рассматриваются особенности защиты информации в информационно-телекоммуникационных системах.

1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

1.1. Понятие информации

«Я стремлюсь обладать информацией обо всем, что встречается на моем пути, и особенно о том, что является для меня наиболее важным». Это высказывание Эвфранора, одного из яростных защитников христианства, как нельзя лучше отражает значение информации в нашем быстроменяющемся мире. Информация как универсальная категория по праву играет очень важную роль в современном знании и в последние годы становится центральным объектом исследования в различных отраслях науки.

Как отмечает Г.В. Можаева, «…исторический опыт показывает, что общественное развитие невозможно вне информации и каналов ее распространения. Усложнение общественной жизни сопровождается расширением объемов информации, что, в свою очередь, ведет к увеличению потребности в обмене информацией. Чем шире потребность в информации и информационном обмене, тем больше информации распространяется в обществе. Она оказывает определяющее влияние на сознание, поведение людей, определяет их быт, лежит в основе принятия решений, формирования мировоззрения, коммуникативных отношений в обществе. Информация представляет собой фактор, управляющий общественным развитием»[1].

В этой связи вполне закономерным представляется то обстоятельство, что сегодня в научном сообществе существует определенное понимание необходимости изучения фундаментальных свойств информации и принципов информационного взаимодействия, которые лежат в основе наиболее важных законов эволюции живой и неживой природы, человеческого общества, а также того удивительного феномена, который мы называем сознанием. Все больше ученых считают, что ключевой идеей, связанной с поиском основополагающего порядка мироустройства, может стать переформулирование взглядов на природу не в терминах материи и энергии, а в терминах информации. Одним из первых об этом заговорил патриарх американской физики Джон Арчибальд Уиллер: «…Чем больше я размышляю…о нашей странной способности постигать тот мир, в котором мы живем, тем больше вижу фундаментальное… значение логики и информации…»[2].

Таким образом, осмысление роли информации в развитии природы и общества, а также освоение информации как стратегического ресурса и движущего

---

[1] Можаева Г.В. Роль исторической информации в современном источниковедении // Открытое и дистанционное образование. 2003. № 1. С. 35-46.

[2] Wheeler J.A. Geons, black holes & quantum foam: a life in physics. New York: W.W. Norton & Company, 1998. P. 63-64.

фактора дальнейшего развития цивилизации являются сегодня исключительно важными и актуальными проблемами, которые приобретают не только общенаучную, но и общецивилизационную значимость.

Термин «информация» происходит от латинского *informatio*, означающего «ознакомление, разъяснение, представление, понятие»[1] и первоначально был связан исключительно с коммуникативной деятельностью людей. В России он появился, по-видимому, в эпоху Петра I[2], однако, сколь-нибудь широкого распространения не получил. Вплоть до начала XX века под информацией понимались сведения (устные, письменные или иные), передаваемые одними людьми другим людям посредством различных способов, или собственно процесс передачи и получения сведений[3].

Стремительное развитие в 20-х годах прошлого века средств и систем связи, зарождение информатики и кибернетики настоятельно потребовали научного осмысления понятия информации и разработки соответствующей теоретической базы. Это привело к формированию и развитию целого «семейства» самых различных учений об информации и, соответственно, подходов к определению самого понятия информации.

Зарождение «классической» научной теории информации относят к 1948 году. Именно в этом году увидела свет основополагающая работа американского ученого Клода Шеннона «Математическая теория связи», в которой исследовались технические и количественные параметры информации и в которой им была предложена формула определения количества информации для совокупности событий с различными вероятностями.

Исходным пунктом шенноновского подхода является представление об информации как о некоторой самостоятельной категории, которую «…можно рассматривать как нечто, — писал К. Шеннон, — весьма схожее с такими физическими величинами, как масса или энергия»[4]. При этом, «…значимый аспект информации, с точки зрения ее передачи, состоит в том, что одно специфическое сообщение выбрано из набора возможных сообщений…Таким образом, …информация есть не что иное, как выбор одного сообщения из набора возможных сообщений»[5].

Отличный от взглядов К. Шеннона подход к определению количества информации предложил в 1965 году академик А.Н. Колмогоров, который он назвал алгоритмическим. В соответствии с этим подходом количество информации определяется как *минимальная длина программы, позволяющей пре-*

---

[1] См.: Советский энциклопедический словарь / гл. ред. А.М. Прохоров. — 3-е изд. М.: Сов. энциклопедия, 1985. С. 498.

[2] См.: Смирнов Н.А. Западное влияние на русский язык в Петровскую эпоху. СПб: Тип. Акад. наук, 1910. С. 123.

[3] См.: Алешин Л.И. Культура информации в информационном обществе: постановка проблемы//Информационная культура: процессы теоретического осмысления: Сб. ст. Краснодар, 2001. С. 87-101; Бубнов В.А. О толковании понятия «информация» и о количественной мере информации//Вестник Московского городского педагогического университета. Серия: Естественные науки. 2009. № 1. С. 69-75.

[4] Shannon C.E. Information Theory//Encyclopedia Britannica. 1972. Vol. 12. P. 246.

[5] Shannon C.E. Указ. соч. P. 247.

образовать один объект (*множество*) *в другой* (*множество*)[1]. Однако, в силу целого ряда причин данный подход не нашел своего широкого практического применения.

Сформулированная К. Шенноном теория информации оказала заметное влияние на самые различные области знаний. Помимо чисто прикладного, значение разработанного К. Шенноном подхода к исследованию информации заключалось и в том, что в его рамках было получено первое определение информации, удовлетворительное, в том числе, и с философской точки зрения: *информация есть устраненная неопределенность*. По замечанию А.Д. Урсула, «…если в наших знаниях о каком-либо предмете существует неясность, неопределенность, а получив новые сведения об этом предмете мы можем уже более определенно судить о нем, то это значит, что сообщение содержало в себе информацию»[2].

Однако выделение в информации только количественного ее аспекта оказалось явно недостаточно, что предопределило поиск иных, более универсальных подходов к определению понятия информации. Таким, по существу другим, дополнительным подходом, стал подход кибернетический, охватывающий структуры и связи систем.

Становление и развитие кибернетики как науки неразрывно связано с именем известного философа и мыслителя Норберта Винера, который предложил свое «информационное видение» кибернетики, как науки об управлении и связи в живых организмах, обществе и машинах. По мнению Н. Винера, информация — это «…обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших органов чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде…»[3].

Выработанный в рамках кибернетики подход к исследованию феномена информации оказал поистине неоценимое воздействие на интенсификацию научных исследований в этой области. В этой связи 60-70-е гг. прошлого столетия оказались весьма плодотворными для научных изысканий информационной проблематики. Понимание очевидной необходимости выхода за рамки частнонаучных представлений об информации привело к попыткам выработки еди-ного междисциплинарного подхода к изучению данной проблемы, в основу которого была положена философия, как своего рода краеугольная основа, фундамент научных представлений об окружающем мире.

В западной философской мысли в конце семидесятых — начале восьмидесятых годов двадцатого века широкое распространение получил подход к определению сущности информации, основанный на представлении о связи понятия «информация» с философской категорией «различие». Так, по мнению Грегори Бейтсона, «…то, что мы имеем в виду, когда говорим об информации... есть, фактически, различимое различие (*a difference that makes a*

---

[1] См.: Колмогоров А.Н. Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 1965. Т. 1. Вып. 1. С. 3-11.

[2] См.: Урсул А. Д. Отражение и информация. М.: Мысль, 1973. С. 32.

[3] Винер Н. Кибернетика и общество. М.: Изд. ин. лит., 1958. С. 31.

difference)...»[1]. При этом Г. Бейтсон придерживается точки зрения об исключительно ментальном характере категории «различие»[2].

Впоследствии данный подход к пониманию природы и сущности информации получил свое развитие в работах известного немецкого социолога Никласа Лумана, по мнению которого информация есть не что иное, как «*различие, порождающее различие*» (*a difference which finds a difference*), т.е. различие в сфере разума, порожденное различием во внешнем мире.

Используя материал статистической теории информации, в середине 50-х годов прошлого века У. Р. Эшби изложил концепцию разнообразия, суть которой заключается в утверждении, что теория информации изучает процессы «передачи разнообразия» по каналам связи, причем «информация не может передаваться в большем количестве, чем это позволяет количество разнообразия»[3]. Таким образом, согласно этой концепции, *природа информации заключается в разнообразии*, *а количество информации выражает количество разнообразия*.

Подход к определению информации, близкий к концепции разнообразия, имеется и в работах академика В.М. Глушкова, характеризующего информацию как «…меру неоднородности в распределении энергии (или вещества) в пространстве и во времени, меру изменений, которыми сопровождаются все протекающие в мире процессы»[4].

В отечественной науке развитие философского осмысления феномена информации до недавнего времени осуществлялось в рамках теории отражения. При этом, по мнению некоторых исследователей[5], категория отражения оказалась тем ключом, который позволил открыть тайну природы информации, именно эта философская категория оказалась методологически плодотворной для проникновения в ее сущность. По мнению А.Д. Урсула, «…природа информации заключается в отраженном разнообразии, а количество информации выражает количество разнообразия. Движение этого разнообразия (увеличение или уменьшение) представляет собой информационный процесс»[6].

Следует отметить, что отсутствие единого подхода к пониманию связи между информацией и отражением привело к появлению множества различных точек зрения по данному вопросу. Так, например, сторонники «атрибутивной» концепции информации полагают, что информация входит как компонент, аспект, сторона в любые отражательные процессы (Б.В. Ахлибининский, Л.Б. Баженов, Б.В. Бирюков, К.Е. Морозов, И.Б. Новик, Л.А. Петрушенко, А.Д. Урсул и др.).

По мнению же сторонников функционального подхода информация возникает только на уровне жизни и представляет собой не атрибут всей материи, а функциональное свойство самоуправляемых и самоорганизующихся систем

---

[1] Бейтсон Г. Экология разума: Избр. ст. по антропологии, психиатрии и эпистемологии / пер. с англ. М.: Смысл, 2000. С. 418.

[2] См.: Бейтсон Г. Указ. соч. С. 416-417.

[3] См.: Ashby W. Ross. An Introduction to Cybernetics/Second Impression. London: Chapman & Hall Ltd, 1957. P. 152.

[4] См.: Глушков В.М. Мышление и кибернетика//Вопросы философии. 1963. № 1. С. 36.

[5] См.: Урсул А.Д. Отражение и информация. М.: Мысль, 1973. С. 114.

[6] Урсул А.Д. Природа информации. М.: Политиздат, 1968. С. 12.

(В.В. Вержбицкий, Г.Г. Вдовиченко, И.И. Гришкин, Д.И. Дубровский, Н.И. Жуков, А.М. Коршунов, М.И. Сетров, Г.И. Царегородцев и др.).

Говоря о дальнейшем развитии представлений об информации, следует отметить, что в конце 80-х годов XX века можно было наблюдать новый всплеск интереса к данной научной категории. В этот период исследователями были предприняты попытки решения проблем информационного обеспечения всех сфер жизнедеятельности человека.

Не утихают научные споры о природе и сущности информации и в наши дни. Основная причина сложившейся ситуации заключается в фрагментарности современного научного знания, в отсутствии единых подходов к построению целостной и непротиворечивой картины мироздания. Вместе с тем, следует констатировать, что в настоящее время научной мыслью созданы предпосылки формирования единой научной картины мира на основе базисных принципов, имеющих общенаучный статус.

Если кратко охарактеризовать современные тенденции синтеза научных знаний, то они выражаются в стремлении построить общенаучную картину мира на основе принципов универсального эволюционизма, объединяющих в единое целое идеи системного и эволюционного подходов.

Усилиями ведущих ученых, среди которых отметим В.И. Вернадского, П. Тейяр де Шардена, А.Л. Чижевского, К.Э. Циолковского и др., была установлена дуальная (двойственная) структура материального мира, представляющего собой взаимодействие систем костного и живого вещества. В системе этого взаимодействия двух составляющих окружающей действительности центральное место занимает человек, который «…является ключевым звеном универсального и глобального эволюционного процесса и который рассматривается как объект космической эволюции, закономерного и естественного этапа в развитии нашей Вселенной, ответственный за состояние мира, в который он сам погружен»[1].

Понимание той роли, которую играет человек в современном мире, тесно связано с представлениями об активности субъекта, о принципах его созидательной и конструктивной деятельности в нем. В современном научном знании основным методологическим инструментом исследования данного вопроса является деятельностный подход, истоки которого берут свое начало еще в немецкой классической философии (Гегель, Л. Фейербах).

В рамках данного подхода субъект определяется через его деятельность, в процессе которой он создает предмет, опредмечивает свои замыслы[2]. В процессе реализации деятельности человек неизбежно осуществляет информационное взаимодействие со средой ее осуществления, результатом которого, в конечном итоге, является выработка ситуативно обусловленного (контекстнозависимого) отклика человека — субъекта деятельности на изменения окру-

---

[1] См.: Князева Е.Н., Курдюмов С.П. Коэволюция: человек как соучастник коэволюционных процессов // Устойчивое развитие. Наука и практика. 2002. № 1. С. 18.

[2] См.: Психология человека от рождения до смерти. Полный курс психологии развития / под ред. члена-корреспондента РАО А.А. Реана. СПб.: «Прайм-ЕВРОЗНАК», 2003. С. 18.

жающей среды. Механизм формирования этого отклика заключается в принятии того или иного решения, обусловленного как собственно целью, так и сложившейся ситуацией деятельности.

Такое представление о деятельности как форме взаимодействия человека с окружающим миром, позволяет сделать вывод о том, что с содержательной точки зрения информация — *это такое изменение в представлении об условиях деятельности, которое воспринимается субъектом этой деятельности как значимое с точки зрения ее конечных целей и выступает в этой связи основой для принятия многократных последовательных решений для их достижения*[1].

Данный подход к пониманию сущности информации позволяет констатировать, что именно информация является своего рода «пусковым механизмом» деятельности. Как отмечает Н.Н. Леонтьева, «…именно новая порция информации толкает людей на те или иные поступки. Отсутствие информации порождает беспокойство и желание эту информацию добыть, чтобы принять какое-то решение…»[2]. «Информацией является то, — пишет Н.И. Плотников, — что вызывает изменение поведения, принятие решения»[3].

Осуществляя деятельность, человек сам определяет, что для него является информацией, а что нет. То, что для одного человека может быть информацией, для другого лишь ненужные сведения. Исходя из этого, информацию можно рассматривать как продукт мыслительной деятельности, формируемый в процессе обработки и анализа полученных сведений, а также их соотнесения с поставленными целями и решаемыми задачами. Поскольку жизнедеятельность человека основана на целевых установках, носит поведенческий характер, то информация необходима ему для выработки и (или) корректировки целевых установок и поведения как совокупности действий, направленных на достижение поставленных целей.

Здесь можно только согласиться с точкой зрения выдающегося математика и мыслителя Н.Н. Моисеева, который в своей последней книге писал: «Информация сама по себе ничего не стоит и ничего не дает. Мне кажется бессмысленным говорить о ценности информации, как о некоторой абсолютной характеристике. Информация нужна субъекту для возможности выбора способа действий при стремлении к достижению некоторой цели»[4].

Таким образом, *роль информации, ее значение в системе профессиональной деятельности специалистов МВД России заключается в том, что информация, рассматриваемая как психический феномен, выступает регу-*

---

[1] См.: Григорьев А.Н. Информация и информационное взаимодействие в расследовании преступлений: теоретические аспекты: монография. Калининград: Калининградский ЮИ МВД России, 2006. С. 92.

[2] Леонтьева Н.Н. О содержании Информации // Научно-техническая информация. Сер. 2. Информационные системы и процессы. 1999. № 8. С. 11.

[3] Плотников Н.И. Информационная разведка: как создается закрытая информация из открытых источников. Новосибирск: Научно-издательский центр ОИГГМ СО РАН, 1998. С. 11.

[4] Моисеев Н.Н. Универсум, информация, общество. М.: Устойчивый мир, 2001. С. 51.

лятивной основой профессиональной деятельности, формирующей ее путем выбора необходимого сценария деятельности в зависимости от предметно-субъективных условий ее осуществления.

Отмеченное позволяет заключить, что любое реальное взаимодействие человека с окружающим миром предполагает использование информации об этом мире как основы для ориентации в нем и организации взаимоотношений с окружающей действительностью.

Вместе с тем, несмотря на свою многоаспектность и мно-гозначность, информация как универсальная категория не только играет очень важную роль в современном знании, но и является одним из важнейших факторов социального прогресса. По своей сути информация представляет собой фактор, управляющий общественным развитием. В этой связи вполне закономерным представляется то пристальное внимание, которое уделяется вопросам защиты информации в современном мире. А что же из себя представляет информация как объект защиты?

1.2. Информация как объект защиты

Существующие реалии таковы, что информация и современные информационно-телекоммуникационные технологии являются одним из наиболее важных факторов в формировании общества XXI века, фактором, пронизывающим все стороны и аспекты человеческой деятельности.

Информация как объект в современном мире и как предмет жизнедеятельности и жизнеобеспечения имеет свои специфические особенности. По мнению Ю.Н. Загинайлова[1], к ним можно отнести следующие:

1. Информация в форме сведений всегда связана с человеком (физическим лицом), а в форме сообщений и данных — с материальным носителем, на котором она фиксируется, хранится и переносится.

2. Информация может быть товаром и объектом рыночных отношений. Право собственности закреплено гражданским законодательством, включает имущественные права. Для реализации права необходимо документирование информации — фиксация на материальном носителе.

3. Информация как предмет жизнедеятельности и жизнеобеспечения имеет ценность (цену) и (или) важность, которые могут меняться во времени и приносить доход или другие материальные и нематериальные блага ее обладателям. Для сохранения ценности (важности) информации необходимо поддерживать ее потребительские свойства.

К основным потребительским свойствам информации относят ее достоверность, полноту, актуальность, своевременность, адекватность, избыточность, полезность, целостность, доступность, конфиденциальность[2].

---

[1] См.: Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. С. 18.

[2] См.: Душин В.К. Теоретические основы информационных процессов и систем: учебник. М.: Дашков и К, 2015. [Электронный ресурс]. — Режим доступа: http://www.knigafund.ru/ books/173695.

Достоверность информации — ее соответствие объективной реальности (как текущей, так и прошедшей) окружающего мира.

Полнота информации — ее достаточность для принятия решения.

Актуальность информации — степень соответствия информации текущему моменту времени. Нередко с актуальностью, как и с полнотой, связывают коммерческую ценность информации. Поскольку информационные процессы растянуты во времени, то достоверная и адекватная, но устаревшая информация может приводить к ошибочным решениям. Необходимость поиска (или разработки) адекватного метода для работы с данными может приводить к такой задержке в получении информации, что она становится неактуальной и ненужной. На этом, в частности, основаны многие современные системы шифрования данных и механизмы электронной подписи. Лица, не владеющие ключом (методом) для чтения данных, могут заняться поиском ключа, поскольку алгоритм метода обычно доступен, но продолжительность этого поиска столь велика, что за время работы информация теряет актуальность и, соответственно, связанную с ней практическую ценность.

Своевременность информации означает, что она получена в нужный момент принятия решения, без опоздания. Информация, поступившая после принятия решения, скорее всего, не нужна. С другой стороны, не всякая заблаговременность предоставления информации хороша: может быть утрачена ее актуальность.

Под *адекватностью информации* понимают степень соответствия информации, полученной потребителем, тому, что автор вложил в ее содержание.

Избыточность информации — это наличие информации в объеме сверх необходимого для реализации цели восприятия.

Полезность информации — степень необходимости информационного объекта для данного субъекта.

Среди рассматриваемых потребительских свойств следует выделить те свойства информации, которые определяют ее безопасность.

В нормативных правовых актах в области защиты информации под ***безопасностью информации*** понимается *состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность*[1]. Т.е. для обеспечения безопасности информации необходимо постоянно поддерживать конфиденциальность, целостность и доступность информации. При нарушении хотя бы одного из этих свойств ценность информации снижается, либо теряется вообще.

Конфиденциальность — свойство информации, указывающее на необходимость ограничения круга субъектов, имеющих доступ к данной информации.

Целостность — свойство информации существовать в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

---

[1] См.: Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Доступность — состояние информации (ресурсов инфор-мационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Как уже отмечалось ранее, при всей своей неопределенности и многозначности информация выступает в качестве системообразующего фактора общественной жизни, составляя содержание общественных отношений, складывающихся в процессе социогенеза. Необходимо осуществляемое правовое регулирование этих отношений обуславливает потребность рассмотрения и правового аспекта понятия информации, определяющего специфичность информации не только как объекта права, но и как объекта защиты.

В самом общем виде под информацией понимаются сведения о предметах, явлениях и процессах окружающего нас мира. Именно так определяется информация в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», направленном на регулирование взаимоотношений в информационной сфере. Согласно ст. 2 этого закона *информация — это сведения* (*сообщения, данные*) *независимо от формы их представления*.

В этом законе, наряду с «информацией», законодатель выделяет еще один объект права — *«документированную информацию» — документ — зафиксированную на материальном носителе путем документирования информацию с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.*

Вообще, сам термин «документ» имеет множество значений и в различных сферах деятельности трактуется неодинаково, но все (в том числе и законодатели) согласны с тем, что документ — *это материальный носитель, на котором зафиксирована информация*.

В зависимости от материальной основы, используемой для хранения и/или передачи информации, выделяют два вида документов:

– документ, материальная основа которого — вещество (бумага, металл, дерево и др.);

– документ, материальная основа которого — поле (в том числе звуковые волны, радиоволны, оптическое излучение).

Документирование информации — это фиксация информации на материальном носителе (*т.е. процесс создания документа*)*, осуществляемая по установленным правилам*[1]. При этом правила документирования устанавливаются либо правовыми актами, либо выработаны традицией. В системе министерства внутренних дел правила документирования устанавливаются приказами министра внутренних дел. Документы, созданные в органах внутренних дел по установленным правилам, приобретают статус служебных или *официальных документов*.

---

[1] См.: Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. С. 47.

Официальный документ — документ, созданный надлежащим субъектом органа внутренних дел, оформленный и удостоверенный в установленном порядке.

Служебный документ — официальный документ, используемый в текущей деятельности органа внутренних дел.

Документирование информации по своей сути имеет двоякую направленность. С одной стороны, оно служит средством распространения информации, например, передачи ее от человека человеку, а с другой, — средством вовлечения информации в регулируемые законодательством правоотношения. В последнем случае документ должен быть снабжен определенными реквизитами, которые позволяли бы его однозначно идентифицировать.

Под реквизитом документа понимается элемент его оформления[1]. К числу основных реквизитов документа относятся: наименование организации, наименование вида документа, дата регистрации документа, регистрационный номер документа, место составления или издания документа, адресат, резолюция, текст документа, подпись, гриф согласования документа, визы согласования документа, оттиск печати, отметка о заверении копии, отметка об исполнителе и др.[2]

В настоящее время с развитием систем электронного документооборота широкое распространение получили документы, которые хранятся и используются в электронном виде. Для их обозначения используется понятие «*электронный документ*», под которым понимается «…документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[3].

Отличительной особенностью данного подхода к определению понятия электронного документа является отсутствие жесткой привязки к конкретному материальному носителю. Один и тот же документ может существовать на разных носителях, поэтому к нему не применимы такие понятия, как оригинал и копия. Все идентичные по содержанию экземпляры электронного документа могут рассматриваться как оригиналы и отличаться друг от друга только датой создания. А в качестве копии электронного документа может рассматриваться только его копия на бумажном носителе.

---

[1] См.: Национальный стандарт РФ ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См.: ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов» (принят и введен в действие постановлением Госстандарта РФ от 3 марта 2003 г. № 65-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] См.: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Для подтверждения достоверности электронного документа используется электронная подпись, под которой понимается «*...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*» (ст. 2 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»).

Вышеупомянутый закон выделяет два вида электронной подписи: простая электронная подпись и усиленная электронная подпись. При этом различаются усиленная неквалифицированная электронная подпись (далее — неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее — квалифицированная электронная подпись).

Простая электронная подпись представляет собой комбинацию из логина и пароля и подтверждает, что электронное сообщение отправлено конкретным лицом.

Неквалифицированной электронной подписью является электронная 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.

Квалифицированной электронной подписью является электронная подпись, которая не только соответствует всем признакам неквалифицированной электронной подписи, но и подтверждается сертификатом от аккредитованного удостоверяющего центра.

Сообщение с простой или неквалифицированной электронной подписью может (по предварительной договоренности сторон и в специально предусмотренных законом случаях) быть приравнено к бумажному документу, подписанному собственноручно.

Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Таким образом, с позиций действующего законодательства документированная информация представляет собой такую организационную форму, которая может быть определена как единая совокупность[1]:

1) содержания информации;

2) реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры;

3) материального носителя информации, на котором ее содержание и реквизиты закреплены.

---

[1] См.: Копылов В.А. Информационное право: учебник. - Изд. 2-е, перераб. и доп. М.: Юристъ, 2005. С. 78.

Согласно ст. 5 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация может являться объектом публичных, гражданских и иных правовых отношений. Она может свободно использоваться любым лицом и передаваться одним лицом другому лицу. Однако, в определенных случаях свобода предоставления и распространения информации может ограничиваться.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на (рис. 1.1):

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.

Рис. 1.1. Виды информации в зависимости от порядка ее предоставления или распространения

Кроме того, информация как категория, имеющая действительную или потенциальную ценность, как и любой другой вид ценности, может, а в отдельных случаях и должна защищаться ее обладателем.

Защищаемая информация *— это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем информации*[1].

Обладатель защищаемой информации — это лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-

[1] Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

либо признакам. В качестве обладателя информации может выступать гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

Для обеспечения защиты информации ее обладатель может ограничивать доступ к ней третьих лиц.

Правовой режим доступа к информации может быть:

– *общим*, выражающим общие, исходные способы правового регулирования;

– *специальным*, являющимся модификацией общего режима и вносящим либо особые льготы и преимущества, либо особые ограничения, которые заключаются в дополнительных запретах и обязываниях[1].

Общим правовым режимом доступа к информации является режим открытой информации, то есть информация может быть сообщена любому лицу. Данное положение закреплено в Конституции Российской Федерации, в п. 4 ст. 29 которой, например, говорится, что «*...каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом*».

Общедоступная информация является общественно значимой информацией для граждан и общества. В первую очередь это относится к государственным информационным ресурсам, создаваемым специально для обеспечения государственной политики России и информирования граждан и общества по этим и другим вопросам. К таким ресурсам, в частности, относятся Интернет-порталы и интернет-сайты федеральных органов государственной власти, министерств и ведомств, Государственной Думы, органов государственной власти субъектов Российской Федерации, муниципальных органов.

Несмотря на открытый характер информации, размещенной на подобного рода площадках, ее общественная значимость, важность требуют поддержания целостности (неискаженности) и постоянной доступности для граждан и организаций через информационно-телекоммуникационные сети общего пользования (Интернет).

Наряду с отмеченным, значительная часть общедоступной информации (общедоступных информационных ресурсов) включает объекты интеллектуальной собственности, определенных в качестве таковых гражданским законодательством. И в первую очередь это объекты авторского и смежного права. К ним, в частности, относятся произведения науки, литературы и искусства, программы для ЭВМ и базы данных — объекты авторского права, объекты смежного права с авторским — исполнения, фонограммы, сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания), объекты патентного права — изобретения, полезные модели, промышленные образцы и др. Гражданский кодекс Российской Федерации, наряду с правовыми методами защиты объектов авторского и смежного права, предусматривает возможность защиты этих объектов техническими (программно-аппаратными) средствами[2].

---

[1] Магдилов М.М., Магдилова Л.В. Особенности и виды правового режима информации [Электронный ресурс]. — Режим доступа: http://www.rusnauka.com/1_NIO_2014/Pravo/ 11_153760.doc.htm. — Загл. с экрана.

[2] См.: Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. С. 94-96.

В установленных законодательством случаях в отношении информации могут быть введены специальные режимы доступа, направленные на охрану сведений, свободное распространение которых нарушает права и законные интересы общества, государства, личности.

В соответствии с отмеченным, *вся информации, в зависимости от правового режима доступа к ней, подразделяется на общедоступную и с ограниченным доступом* (ст. 5 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Под **информацией с ограниченным доступом** *понимается информация, доступ к которой ограничен в соответствии с законом с целью защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов правообладателей этой информации, обеспечения обороны страны и безопасности государства.*

Перечень информации с ограниченным доступом законом не определен, однако, основываясь на положениях закона, а также в соответствии с Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», к информации с ограниченным доступом относятся:

1. Сведения, составляющие *государственную тайну.*

2. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (*персональные данные*), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

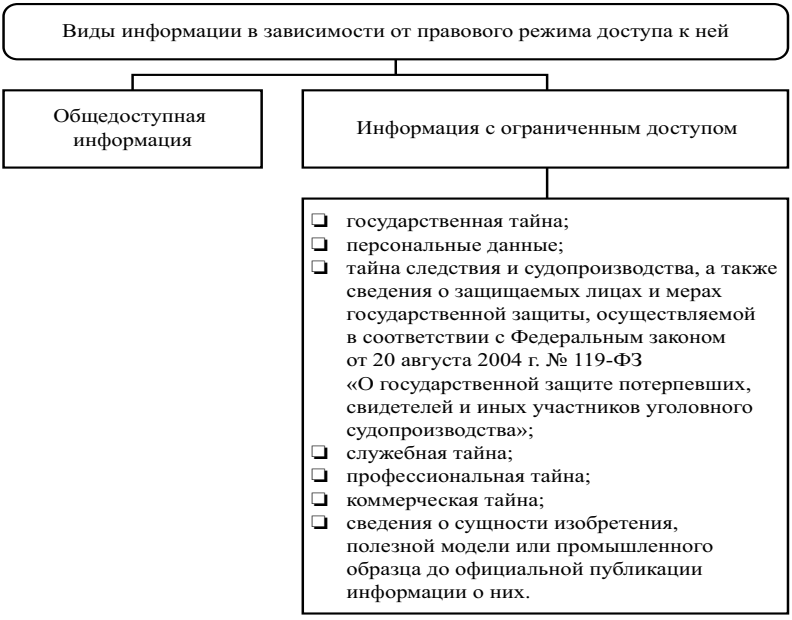


Рис. 1.2. Виды информации в зависимости от правового режима доступа к ней

3. Сведения, составляющие т*айну следствия и судопроизводства*, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации.

4. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским Кодексом Российской Федерации и федеральными законами (служебная тайна).

5. *Сведения, связанные с профессиональной деятельностью*, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телефонных или иных сообщений и т. д.).

6. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским Кодексом Российской Федерации и федеральными законами (*коммерческая тайна*).

7. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

8. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

Однако защита информации не сводится только лишь к правовому регулированию режима доступа к ней. Защита информации — это совокупность правовых, организационных и технических мер, направленных на (ст. 16 Закона «Об информации, информационных технологиях и о защите информации»):

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Как можно заметить, защита информации — довольно емкая и многогранная проблема, не сводящаяся только к собственно защите информации от несанкционированного доступа. Именно поэтому в настоящее время проблема обеспечения защищенности информации рассматривается как проблема информационной безопасности, заключающаяся в комплексном ее решении по нескольким направлениям.

1.3. Информационная безопасность и защита информации

В настоящее время наша цивилизация находится на очень сложном этапе своего развития, который многие ученые характеризуют как глобальный системный кризис. Человечество оказалось перед лицом целого ряда взаимос-

вязанных проблем, которые не просто оказывают негативное воздействие на мировое развитие, но и угрожают самому существованию человека как биологического вида. Это и глобальное изменение климата, истощение природных ресурсов, угроза краха мировой экономики.

В этих условиях многим ученым выход из сложившейся ситуации видится в кардинальном переосмыслении дальнейших путей развития человечества, в отказе от экстенсивной модели развития, основанной на безудержном потреблении материальных благ, и переходе к новой парадигме развития, которая должна быть основана на эффективном использовании последних достижений в области науки и техники. Возможность реализации этого во многом зависит от того, насколько человечество сможет освоить и эффективно использовать информацию как новый и практически неисчерпаемый ресурс развития, а информационные технологии — как мощный фактор и катализатор этого развития.

В этой связи следует констатировать, что минувший век вошел в историю как период поистине тектонических изменений в информационной сфере общества, способных изменить облик цивилизации.

Прежде всего, речь идет о значительном увеличении используемых современным обществом знаний. Накопленные человечеством информационные ресурсы растут, особенно в последние годы, невиданными доселе темпами. Так, по данным исследователей из Калифорнийского университета (США), в 2002 году общий объем произведенной человечеством информации составил порядка 5 экзабайт[1].

По результатам же исследования, проведенного Global Information Industry Center (США)2 в 2008 году, во всем мире только лишь серверы обработали 9,57 зеттабайт информации (1 зеттабайт равен 1024 экзабайтам). Это примерно 12 гигабайт информации в среднем на одного работника, или приблизительно 3 террабайта информации на одного работника в год.

Таким образом, новые информационно-телекоммуникационные технологии стали неотъемлемой частью жизни современного общества, ведущей к изменению социально-экономических, геополитических контуров цивилизации. Происходит постепенное размытие национальных границ, стремительно растет сектор экономики, связанный с производством и потреблением информационных услуг, снимаются информационные барьеры, формируется единое мировое информационное пространство. Все это знаменует собой переход человечества к качественно новому типу общественной формации — переход от общества индустриального к обществу информационному.

В настоящее время в научной среде существуют различные подходы к пониманию природы информационного общества, несмотря на то, что сама идея информационной эволюции социума была сформулирована еще в конце 60-х — начале 70-х годах прошлого века.

---

[1] 1 экзабайт — 1018 байт. Для примера, объем произведенной в 1999 году информации составил 2 экзабайта.

[2] См.: How Much Information? 2010. Report on Enterprise Server Information [Электронный ресурс]. — Режим доступа: http://hmi.ucsd.edu/pdf/HMI_2010_EnterpriseReport_Jan_ 2011.pdf. — Загл. с экрана.

Впервые контуры информационного общества, как общества будущего, были отчетливо обрисованы в отчетах, представленных японскому правительству рядом организаций: «Японское информационное общество: темы и подходы» (1969 г.), «План информационного общества» (1971 г.). В этих отчетах *информационное общество определялось как такое, где процесс компьютеризации даст людям доступ к надежным источникам информации, избавит их от рутинной работы, обеспечит высокий уровень автоматизации производства*. При этом изменится и само производство — продукт его станет более «информационно емким», что означает увеличение доли инноваций, дизайна и маркетинга в его стоимости[1].

Последние десятилетия проблема формирования информационного общества неизменно находит свое отражение в различных правовых актах как национального, так и международного уровня. Данные обстоятельства со всей очевидностью свидетельствуют о том, что в настоящее время среди политических элит большинства стран существует четкое понимание того, что построение информационного общества — это не просто абстрактная футурологическая концепция, а необходимое условие поступательного развития государства, обеспечения его конкурентоспособности в условиях глобальной информатизации.

Таким образом, как отмечает Т.А. Мешкова, «…являясь одной из закономерностей современного социального прогресса, информатизация, по сути, представляет собой процесс преобразования человеком среды своего существования, биосферы в ноосферу, результатом которого будет создание высокоразвитой инфосферы. Этот процесс затрагивает как среду обитания, так и общество, самого человека»[2].

Однако глубина совершаемых преобразований, происходящих как в нашей стране, так и во всем мире, не только дает новые возможности для устойчивого развития России в XXI веке, но и влечет за собой возникновение угроз, способных оказать негативное воздействие на обеспечение безопасности государства.

Прежде всего, это получившие значительное ускорение в последнее время процессы поляризации мира не только по политическим, но и по социально-экономическим, технологическим основаниям, маргинализация отдельных стран и регионов. Кроме того, доступность и широкое использование информационных технологий является важнейшим фактором, создающим почву для качественной трансформации преступной деятельности, ее «виртуализации», перехода от традиционных иерархических к сетевым формам ее организации[3].

И, наконец, произошло кардинальное переосмысление той роли, которую играет информация и СМИ в управлении современным обществом. Пришло понимание того, что смысл информационного сообщения определяется не столько объективными сведениями о произошедшем, сколько тем контекстом,

---

[1] См.: Луценко Л.М. Информационное общество и его социально-философский аспект: монография. М.: Галлея-Принт, 2011. С. 38.

[2] См.: Мешкова Т.А. Безопасность в условиях глобальной информатизации: новые вызовы и новые возможности: автореф. дисс. … канд. полит. наук. М., 2003. С. 4.

[3] См.: Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями Вена, 10-17 апреля 2000 г. Положение в мире в области преступности и уголовного правосудия. Доклад генерального секретаря A/CONF.187/5.

в котором эти сведения подаются. Именно контекст и придает этим сведениям необходимый смысл. Это привело к появлению различных технологий манипулирования индивидуальным, групповым и даже общественным сознанием, которые с успехом используются для организации «цветных революций», государственных переворотов, массовых беспорядков, других кризисных событий и явлений[1]. Не случайно в последнее время большое внимание уделяется вопросам использования «информационного оружия» при ведении так называемых «гибридных войн» — операций, в которых применение вооруженной силы сочетается с интенсивным информационно-психологическим воздействием на противника. Данная проблема особо актуальна для нашей страны, поскольку, как отмечает А.И. Бастрыкин, «…последнее десятилетие Россия, да и ряд других стран, живут в условиях так называемой гибридной войны … Эта война ведется по разным направлениям — политическому, экономическому, информационному, а также правовому. Причем в последние годы она перешла в качественно новую фазу открытого противостояния»[2].

По оценке специалистов, данные проблемы носят вовсе не конъюнктурный характер, а представляют собой тектонический процесс глобальной трансформации[3]. Это зримое проявление перехода в новую культурную, экономическую, технологическую, геополитическую эпоху, новое представление о безопасности личности, общества, государства и методах ее осуществления.

В настоящее время основой государственной политики по обеспечению безопасности России является **Стратегия национальной безопасности Российской Федерации** (утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683), представляющая собой базовый документ стратегического планирования, определяющий национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление *национальной безопасности* Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу. При этом, в качестве одного из важнейших объектов обеспечения безопасности России Стратегия выделяет информационную сферу общества. Таким образом, речь идет о необходимости обеспечения информационной безопасности страны, как одной из важнейших составляющих обеспечения ее национальной безопасности.

---

[1] См.: Григорьев А.Н. Проблемы обеспечения информационной безопасности России в условиях глобализации и информатизации современного общества // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2013. № 4(34). С. 52.

[2] «Пора поставить действенный заслон информационной войне». Председатель Следственного комитета РФ Александр Бастрыкин — о методах борьбы с экстремизмом в России [Электронный ресурс]. — Режим доступа: http://www.kommersant.ru/Doc/2961578. — Загл. с экрана.

[3] См.: Мокшанов М.Г. Актуальные вопросы противостояния гибридным войнам в условиях современной действительности // Наука. Мысль. 2015. № 3. С. 60-63; Романова В.А. Информационная составляющая гибридных войн современности // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 2. С. 293-299.

В рамках существующих подходов безопасность традиционно понимается как *состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз*[1].

Безопасность проявляется как невозможность нанесения вреда функционированию и свойствам объекта безопасности, либо его структурных составляющих. Это положение служит методологическим основанием для выделения видов безопасности. В качестве одного их них выделяют информационную безопасность, которая до недавнего времени рассматривалась преимущественно с точки зрения защиты (поддержания) только лишь количественных и качественных характеристик информации.

Вместе с тем, как уже отмечалось, в настоящее время пришло понимание того, что, выполняя важные функции по обеспечению социума сведениями и знаниями, информация в то же время может причинить ему определенный ущерб. Опасные информационные воздействия могут быть двух видов. Первый заключается в утрате информации, что может привести, с одной стороны, к снижению эффективности собственной деятельности, а с другой, — к повышению эффективности деятельности противника, предоставлению ему дополнительных возможностей и преимуществ. Второй — неконтролируемое распространение «вредной информации», способной привести к принятию ошибочных решений, оказать негативное влияние на индивидуальное и массовое сознание.

Все это привело к расширению понятия информационной безопасности и его рассмотрению как проблемы, не сводящейся лишь к защите (поддержанию параметров качества) информации, но и включающей вопросы защиты от негативных информационных воздействий.

Защита информации, как составляющая процесса обеспечения информационной безопасности, с содержательной точки зрения представляет собой *деятельность, направленную на предотвращение утечки защищаемой информации, несанкци-онированных и непреднамеренных воздействий на защищаемую информацию*[2].

Защита от негативных информационных воздействий предполагает выполнение комплекса мероприятий по обеспечению защиты как государства, так и отдельных граждан, общества в целом от различного рода манипулятивных воздействий, которые могут осуществляться государством (в том числе иностранным), различными государственными и общественно-политическими структурами, социальными группами, отдельными личностями через средства массовой информации, искусство, образование, воспитание, личное общение и приводят к искажению информационно-ориентировочной основы жизнедеятельности, снижению психологического потенциала человека и другим негативным последствиям.

---

[1] См.: Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / под ред. В.А. Садовничего и В.П. Шерстюка. М.: МЦНМО, 2002. С. 46.

[2] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, информационная безопасность определяется способностью государства, общества, личности решать следующие задачи:

– обеспечивать с определенной вероятностью защищенность информационных ресурсов и информационных потоков, необходимых для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;

– противостоять информационным угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

– вырабатывать личностные и групповые навыки и умения безопасного поведения;

– поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Исходя из перечисленных задач, в наиболее общем виде *информационная безопасность* может быть определена как *состояние защищенности интересов личности, общества и государства в информационной сфере от воздействия на них различного рода угроз*. При этом составляющими информационной безопасности являются:

– *состояние безопасности информационного пространства*, при котором обеспечивается его формирование и развитие в интересах граждан, общества и государства;

– *состояние безопасности информационной инфраструктуры*, при котором исключается возможность негативного воздействия на объект безопасности при ее использовании;

– *состояние безопасности информации и информационных ресурсов*, при котором исключается или существенно затрудняется возможность причинения им ущерба (вреда) вследствие проявления внутренних или внешних угроз.

В полной мере такой подход нашел свое выражение в принятой в 2016 г. **Доктрине информационной безопасности Российской Федерации** (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646). Как отмечается в данном документе, «…Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации». Исходя из этого, разработчиками Доктрины ***информационная безопасность Российской Федерации*** определяется как *состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.*

Признавая крайне важную роль информационной сферы в обеспечении реализации стратегических национальных приоритетов Российской Федерации, Доктрина выделяет следующие национальные интересы в информационной сфере:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Как констатируется в Доктрине, «…расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы». К числу таковых авторы Доктрины относят:

1. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

2. Расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического

воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности. Также наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

3. Широкое использование различными террористическими и экстремистскими организациями механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

4. Возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

На основе национальных интересов Российской Федерации в информационной сфере, анализа современного состояния информационной безопасности в различных сферах жизнедеятельности государства и общества формируются стратегические цели обеспечению информационной безопасности:

– *в области обороны страны* — защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

– *в области государственной и общественной безопасности* — защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры;

– *в экономической сфере* — сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств

обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

– *в области науки, технологий и образования* — поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности;

– *в области стратегической стабильности и равноправного стратегического партнерства* — формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

В условиях продолжающейся научно-технической революции в области вычислительной техники и телекоммуникаций, глобализации процессов экономического и политического развития человеческого общества проблемы безопасности развития личности, функционирования общественных структур и органов государства в информационной сфере становятся все более актуальными, затрагивая широкий круг субъектов информационных отношений. Это обуславливает то внимание, которое уделяется в настоящее время выработке государственной политике обеспечения информационной безопасности Российской Федерации, основывающейся на следующих принципах (Доктрина информационной безопасности Российской Федерации):

– законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

– конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

– соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

– достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

– соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Рассмотрев основные вопросы, связанные с обеспечением информационной безопасности Российской Федерации, остановимся подробнее на проблемах обеспечения информационной безопасности органов внутренних дел.

1.4. Понятие информационной безопасности органов внутренних дел и ее структура

В общеметодологическом плане в структуре понятия «безопасность» выделяют:

– объект безопасности;

– угрозы объекту безопасности;

– обеспечение безопасности объекта от проявлений угроз.

Ключевым элементом определения содержания понятия «безопасность» является объект безопасности, то есть то, что защищается от угроз. Выбирая

в качестве объекта безопасности информацию, циркулирующую в органах внутренних дел, а также деятельность служб и подразделений органов внутренних дел, связанную с производством и потреблением информации, мы можем говорить об их *информационной безопасности* — безопасности их «информационного измерения».

В соответствии с **Концепцией обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года** (утв. приказом МВД России от 14 марта 2012 г. № 169) *под информационной безопасностью органов внутренних дел понимается «…состояние защищенности информации, информационных ресурсов и информационных систем органов внутренних дел, при котором обеспечивается защита информации* (*данных*) *от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования».* Структура данного понятия приведена на рис. 1.3. Рассмотрим ее подробнее.

Рис. 1.3. Структура понятия «информационная безопасность органов внутренних дел»

Объект информационной безопасности органов внутренних дел

Как мы уже отмечали, в качестве объекта информационной безопасности выступают:

– *информационные ресурсы* органов внутренних дел, используемые при решении служебных задач, в том числе содержащие информацию ограниченного доступа, а также специальные сведения и оперативные данные служебного характера.

Информация, используемая в органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. Эти сведения используются при организации работы подразделений, при принятии практических мер по борьбе с преступностью и правонарушениями.

Кроме указанных сведений широко используется научная и техническая информация, необходимая для совершенствования деятельности органов внутренних дел.

Помимо отмеченного, защите также подлежит информация ограниченного доступа физических и юридических лиц, к которой должностные лица служб и подразделений органов внутренних дел получают доступ при выполнении служебных обязанностей, в частности, при раскрытии и расследовании преступлений;

– *информационная инфраструктура* органов внутренних дел, под которой понимается *совокупность методов, средств и технологий реализации информационных процессов (то есть процессов создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации), необходимо осуществляемых в органах внутренних дел при выполнении возложенных на них законом задач.*

К информационной инфраструктуре органов внутренних дел относятся, прежде всего, используемые в практической деятельности правоохранительных органов *информационные системы*, составляющие основу информационного обеспечения правоохранительной деятельности.

Все многообразие информационных систем, используемых в органах внутренних дел, можно условно разделить на несколько основных групп:

1) информационно-справочные системы;

2) экспертные системы (системы поддержки принятия решений);

3) автоматизированные системы обработки изображений.

1. *Информационно-справочная система* — это автоматизированная система, предназначенная для сбора и хранения больших объемов данных и оперативного получение информации по запросам пользователей в интерактивном режиме. К ним относятся:

– автоматизированные информационно-справочные системы (АИСС);

– автоматизированные информационно-поисковые системы (АИПС);

– автоматизированные информационные системы (АИС);

– автоматизированные банки данных (АБД);

– справочно-правовые системы.

Кратко отметим некоторые информационно-справочные системы, применяемые в структурных подразделениях МВД России[1].

Так, например, АИСС «Кадры» предназначена для автоматизации процесса управления кадровым составом, содержит удобные средства задания конфигурации, имеет возможность графического представления исходных данных.

АИСС «Картотека-Регион» предназначена для работы с пофамильными учетами осужденных, разыскиваемых и задержанных за бродяжничество лиц.

АИСС «Сводка» обеспечивает сбор поступающей в Министерство внутренних дел оперативной информации о событиях, происшествиях и преступлениях, позволяет осуществлять поиск документов и реквизитов по запросам, контролировать прохождение и исполнение документов, вести статистическую обработку имеющихся данных, составлять отчеты и т.п.

АИПС «Автопоиск» содержит информацию об угнанных, задержанных, похищенных и бесхозных автотранспортных средствах.

АИПС «Антиквариат» осуществляет автоматизированный учет утраченных и выявленных предметов, представляющих историческую, художественную или научную ценность (археологические находки, предметы древности, исторические реликвии, художественные произведения и предметы прикладного искусства и др.).

АИПС «Аэропорт» предназначена для выявления в аэропортах на основе паспортных данных разыскиваемых преступников и других лиц, представляющих оперативный интерес, а также утраченных паспортов.

АИПС «Досье» позволяет получить сведения об особо опасных рецидивистах, «ворах в законе», «авторитетах» преступного мира и т.д. (например, установочные данные, приметы, место работы, место жительства, связи, привычки).

Для учета правонарушений, совершенных иностранцами и лицами без гражданства, разработана и функционирует АИПС «Криминал-И», включающая пять подсистем:

– АИПС «Криминал-И Адмпрактика» содержит сведения об иностранцах и лицах без гражданства, совершивших административные правонарушения;

– АИПС «Криминал-И Преступление» выдает сведения о происшествиях и преступлениях с участием иностранцев и лиц без гражданства;

– АИПС «Криминал-И ДТП» обеспечивает сведениями об иностранцах и лицах без гражданства, участниках дорожно-транспортных происшествий (ДТП) на территории России;

– АИПС «Криминал-И Розыск» содержит данные о находящихся в розыске или разысканных иностранцах;

– АИПС «Криминал-И Наказание» содержит сведения об иностранцах и гражданах России, постоянно проживающих за границей, находящихся под следствием, арестованных или отбывающих наказание на территории Российской Федерации.

---

[1] Григорьев А.Н., Фадеева В.В. Использование автоматизированных информационных систем в деятельности органов внутренних дел: учебное пособие. Калининград: Калининградский филиал СПбУ МВД России, 2012; Рак И.П. Информационные технологии в деятельности правоохранительных органов // Инновационная наука. 2016. № 2. С. 132-135.

Так же разработано большое количество АИПС по различным видам судебно-экспертных и криминалистических исследований: «Марка» (содержит эталонные образцы лакокрасочных материалов и покрытий), «Спектр» (содержит спектры красителей письма), «Волокнистые материалы», «Смазочные материалы», «Металлы», «Автоэмали», «Волокно» (текстиль), «Красители» (волокна), «Помада» (губная), «Бумага», «Оружие», «Патрон», «Гильза», «Клинок» и др. Эти системы могут работать самостоятельно или совместно с другими информационно-вычислительными комплексами.

2. *Экспертная система* — это программа, которая объединяет знания специалистов в конкретных предметных областях и оперирует ими с целью выработки рекомендаций или решения проблем, специфичных для этой области.

Так, например, экспертная система «Автоэкс» предназначена для экспертизы дорожно-транспортных происшествий и позволяет, в том числе, установить, мог ли водитель транспортного средства предотвратить происшествие.

Экспертная система «Спрут» позволяет на основании знаний о преступных формированиях, связей между лицами, экономических составляющих и фактов, представляющих оперативный интерес, устанавливать связи субъектов преступного формирования.

А экспертная система «Ущерб» на основе российского трудового законодательства обеспечивает юридический анализ ситуации привлечения рабочих и служащих к материальной ответственности при нанесении предприятию материального ущерба действием или бездействием.

3. *К автоматизированным системам обработки изображений относятся*: автоматизированные системы составления композиционных портретов, автоматизированные дактилоскопические информационные системы (АДИС).

Автоматизированные системы составления композиционных портретов предназначены для создания экспертами при участии очевидцев субъективных портретов лиц, подозреваемых в совершении преступлений (например, системы «Фоторобот» и «FaceManager», АИПС «Портрет»).

АДИС позволяют создавать и хранить в электронном виде большие массивы дактилоскопической информации, производить по ним поиск с использованием папиллярных узоров пальцев (или ладоней) рук. Для ввода изображений (дактилокарт) в таких системах используются сканеры и телекамеры (например, системы «Папилон» и «Сонда»).

К информационной инфраструктуре органов внутренних дел, помимо информационных систем, относятся также и*нформационные сети* и *сети связи* (в том числе и общего пользования), *информационные технологии*.

Здесь необходимо отметить, что в марте 2012 года МВД России была разработана концепция создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Создание ИСОД пришло на смену проекту по созданию единой информационно-телекоммуникационной системы (ЕИТКС) органов внутренних дел, которое велось с 2005 года.

ИСОД ОВД представляет собой совокупность используемых в Министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и комплексов программно-технических средств, а также систем связи и передачи данных, необходимых для эффективного обеспечения

служебной деятельности МВД России. В процессе создания Системы были решены задачи автоматизации основных видов деятельности подразделений МВД России, организации централизованного хранения и обработки данных. Система должна стать единым источником информации для всех сотрудников подразделений МВД России, служить для организации электронного взаимодействия между ними, обеспечения разграниченного доступа к информационным ресурсам. Также ИСОД будет способствовать повышению эффективности принимаемых решений за счет улучшения качества подготавливаемых отчетов, основанных на актуальных и достоверных данных, обеспечения оперативного и своевременного анализа ключевых показателей деятельности МВД России[1].

Основным элементом инфраструктуры ИСОД ОВД является единая информационная система центров обработки данных (ЕИС ЦОД), которая создается на нескольких территориально удаленных площадках. Она предназначена для размещения централизованных информационных систем и сервисов МВД и предоставления доступа к ним с использованием облачных технологий.

За счет создания ЕИС ЦОД в МВД становится возможным унифицировать используемые в ведомстве программно-технические решения и привести архитектуру основных автоматизированных информационных систем в соответствие с современными требованиями к доступности и надежности. ЕИС ЦОД должна обеспечить консолидацию разнородных данных, содержащихся в различных системах МВД России и обеспечить единую точку доступа к ним для использования в оперативно-служебной деятельности МВД России.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД России, реализуемые в рамках ИСОД, включают:

– сервис электронного документооборота (СЭД);
– сервис электронной почты (СЭП);
– ведомственный информационно-справочный портал (ВИСП);
– систему видеоконференцсвязи.

Прикладные сервисы обеспечения оперативно-служебной деятельности включают:

– информационно-поисковый сервис «Следопыт-М»;
– сервис обеспечения охраны общественного порядка (СООП);
– сервис обеспечения деятельности дежурных частей (СОДЧ);
– сервис обеспечения деятельности подразделений материально-технического обеспечения МВД России (СОМТО);
– федеральную информационную систему ГИБДД (ГИБДД-М);
– сервис обеспечения экономической безопасности (СОЭБ);
– сервис НЦБ Интерпола (СОДИ);
– сервис экспертно-криминалистической деятельности (ЕАИС ЭКП);
– сервис обеспечения государственной защиты лиц (СУОГЗ);
– сервис оформления проезда сотрудников (СОПС);
– сервис ГУ собственной безопасности МВД России (СОПД ГУСБ);
– сервис статистической отчетности (МОСТ);
– банк отпечатков пальцев (ЦИАДИС).

[1] Деятельность информационных служб МВД России / Н.В. Ходякова и др. Волгоград: ВА МВД России, 2012.

Подсистема поддержки взаимодействия с населением, а также межведомственного взаимодействия с целью предоставления госуслуг включает:

– сервис предоставления госуслуг (СПГУ);

– систему централизованного учета оружия (СЦУО);

– единый банк данных архивной информации (Ретроспектива);

– интегрированный банк данных.

Завершая рассмотрение объектов информационной безопасности органов внутренних дел, следует отметить, что к числу объектов информационной инфраструктуры относятся и помещения, в которых протекают информационные процессы, осуществляемые в ходе осуществления служебной деятельности, обработки информации на компьютере и др.

Угрозы объекту информационной безопасности

Организация обеспечения информационной безопасности органов внутренних дел должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как следствие, определение актуальных угроз информационной безопасности органов внутренних дел.

Источники угроз. В теории защиты информации под *источниками угрозы безопасности информации понимают субъектов* (*физические лица, материальные объекты или физические явления*), *являющихся непосредственной причиной возникновения угрозы безопасности информации*[1].

В зависимости от своей природы источники угроз подразделяют на *антропогенные* (вызванные деятельностью человека), *техногенные* или *стихийные*. По отношению к самому объекту безопасности источники угроз подразделяются на внешние и внутренние.

Анализ положений Доктрины информационной безопасности Российской Федерации, Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года, а также иных нормативно-правовых документов в области информационной безопасности позволяет выделить следующие основные источники угроз информационной безопасности органов внутренних дел:

– *внешние*: международные преступные сообщества, организации и группы; иностранные государственные и частные коммерческие структуры; отечественные преступные группировки и коммерческие организации; стихийные бедствия и природные явления (пожары, землетрясения, наводнения и др. непредвиденные обстоятельства); различного рода техногенные аварии и др.;

– *внутренние*: аппаратное и программное обеспечение информационных и телекоммуникационных систем органов внутренних дел, а также персонал, непосредственно занятый их обслуживанием; сами сотрудники органов внутренних дел и др.

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Факторы, воздействующие на защищаемую информацию *— явления, действия или процессы, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней*[1].

В своей совокупности факторы, воздействующие или могущие воздействовать на безопасность защищаемой информации, по признаку отношения к природе возникновения подразделяют на *объективные* и *субъективные*.

По отношению к объекту безопасности факторы, воздействующие на безопасность защищаемой информации, подразделяют на *внутренние* и *внешние.*

В общем виде перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации, можно представить следующим образом:

1. *Объективные факторы, воздействующие на безопасность защищаемой информации*:

а) *внутренние*:

– передача сигналов (по проводным, оптико-волоконным линиям связи и др.);

– излучения сигналов, функционально присущие техническим средствам (устройствам);

– побочные и паразитные электромагнитные излучения, наводки;

– наличие акустоэлектрических преобразователей в элементах технических средств;

– дефекты, сбои и отказы, аварии технических средств и систем объекта информатизации;

дефекты, сбои и отказы программного обеспечения.

б) *внешние:*

– явления техногенного характера (сбои, отказы и аварии систем обеспечения объекта информатизации и т.п.);

– природные явления, стихийные бедствия (пожары, наводнения, землетрясения и т.п.).

2. *Субъективные факторы, воздействующие на безопасность защищаемой информации*:

а) *внутренние*:

– разглашение защищаемой информации лицами, имеющими к ней право доступа (через передачу информации по открытым линиям связи, опубликование информации в открытой печати и других средствах массовой информации, утрату носителей информации и т.п.);

– неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации (путем: несанкционированного изменения информации; несанкционированного копирования защищаемой информации);

– несанкционированный доступ к информации (путем подключения к техническим средствам и системам объекта информатизации; использования закладочных устройств и т.п.);

– недостатки организационного обеспечения защиты информации;

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

– ошибки обслуживающего персонала (при эксплуатации технических и программных средств, систем защиты информации);

б) *внешние:*

– доступ к защищаемой информации с применением технических средств разведки или съема информации;

– несанкционированный доступ к защищаемой информации;

– блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

– действия криминальных групп и отдельных преступных субъектов (диверсии в отношении объекта информатизации или его элементов);

– искажение, уничтожение или блокирование информации с применением технических средств.

Угрозы информационной безопасности органов внутренних дел

Безопасность информационных ресурсов и информационной инфраструктуры органов внутренних дел проявляется через безопасность их наиболее важных свойств, к числу которых, как уже отмечалось, относят: целостность, доступность и конфиденциальность. Нарушение этих свойств и представляет собой угрозу информационной безопасности органов внутренних дел. В соответствии с отмеченным, *под угрозой информационной безопасности органов внутренних дел понимается совокупность условий и факторов*, *создающих потенциальную или реальную опасность утечки*, *хищения*, *утраты*, *уничтожения*, *искажения*, *модификации*, *подделки*, *копирования*, *блокирования информации и несанкционированного доступа к ней*[1].

К *внешним угрозам*, представляющим наибольшую опасность для объектов обеспечения информационной безопасности органов внутренних дел, следует отнести:

– деятельность международных преступных сообществ, организаций и групп, связанную со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

– деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

– нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

– недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

---

[1] См.: Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (утв. приказом МВД России от 14 марта 2012 г. № 169) [Электронный ресурс]. Доступ из СТРАС «Юрист».

– отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;

– отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

– преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Обеспечение информационной безопасности

Как уже отмечалось, информационная безопасность органов внутренних дел — это состояние защищенности информационных ресурсов и поддерживающей информационной инфраструктуры органов внутренних дел от угроз, то есть невозможность нанесения им какого-либо ущерба, вреда. Поскольку и информационные ресурсы и информационная инфраструктура органов внутренних дел не существуют сами по себе, вне практической деятельности органов внутренних дел, а, собственно говоря, являются одними из средств этой деятельности, то вполне очевидно, что их защищенность может быть обеспечена только лишь путем создания таких условий деятельности органов внутренних дел, при которых потенциально опасные для объектов безопасности воздействия либо предупреждались, либо сводились к такому уровню, при котором они не способны нанести им ущерб.

Таким образом, ***обеспечение информационной безопасности органов внутренних дел*** *— это процесс создания таких условий осуществления деятельности органов внутренних дел, при которых потенциально опасные для информационных ресурсов и информационной инфраструктуры органов внутренних дел воздействия на них либо предупреждались, либо сводились к уровню, не препятствующему решению стоящих перед органами внутренних дел задач*[1].

Из данного определения ясно видно, что обеспечение информационной безопасности носит вспомогательный характер в системе деятельности органов внутренних дел, поскольку направлено на создание условий достижения целей и успешной реализации задач, стоящих перед органами внутренних дел — прежде всего, выявление, раскрытие, расследование и профилактика преступлений. Иными словами, она создает предпосылки для успешного выполнения стоящих перед органами внутренних дел задач[2].

Являясь видом обеспечения безопасности, обеспечение информационной безопасности обладает сложной структурой, включающей *цели, средства* и *субъектов этой деятельности*.

---

[1] См.: Григорьев А.Н. Понятие, сущность и структура информационной безопасности органов внутренних дел // Актуальные проблемы правоохранительной деятельности: Труды Калининградского юридического института МВД России. Выпуск X. Калининград: Калининградский ЮИ МВД России, 2004. С. 67-82.

[2] См.: Ишин А.М., Григорьев А.Н. Информация и расследование преступлений (технические меры обеспечения информационной защищенности деятельности по раскрытию и расследованию преступлений): научно-практическое пособие. Калининград: КЮИ МВД России, 2002. С. 37.

Целью обеспечения информационной безопасности органов внутренних дел является достижение необходимого уровня защиты информации от специальных программно-технических воздействий, средств технических разведок, несанкционированного доступа, а также утечки информации по техническим каналам[1].

При этом *основными задачами обеспечения информационной безопасности органов внутренних дел* являются[2]:

– совершенствование правовых, научно-практических, норма-тивно-технических, организационно-методических и иных основ информационной безопасности органов внутренних дел;

– реализация комплекса организационных (режимных) и технических мероприятий, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем органов внутренних дел от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования;

– создание и развитие системы информационной безопасности органов внутренних дел с учетом реализации «облачной архитектуры»;

– формирование и совершенствование системы мониторинга состояния информационной безопасности органов внутренних дел;

– организация и совершенствование профессиональной подготовки и переподготовки сотрудников органов внутренних дел в области обеспечения информационной безопасности.

Средства обеспечения информационной безопасности — это совокупность правовых, организационных и технических средств, предназначенных для обеспечения информационной безопасности.

Субъектами обеспечения информационной безопасности являются органы, организации и лица, уполномоченные законом на осуществление соответствующей деятельности. К ним относятся, прежде всего, руководители органов внутренних дел, сотрудники соответствующих подразделений органов внутренних дел, занимающиеся вопросами обеспечения информационной безопасности (например, сотрудники технических отделов, осуществляющие техническую защиту объектов органов внутренних дел), федеральные органы исполнительной власти, осуществляющие надзорные функции в пределах их компетенции (например ФСБ России, в части обеспечения сохранности сведений, составляющих государственную тайну) и др.

Завершая рассмотрение вопросов, затронутых в данном разделе учебного пособия, подведем некоторые итоги.

В современном мире информация является одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. В этой связи вполне закономерно то внимание, которое уделяется исследованию феномена информации в различных областях научного знания.

---

[1] См.: Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (утв. приказом МВД России от 14 марта 2012 г. № 169) [Электронный ресурс]. Доступ из СТРАС «Юрист».

[2] Там же.

Анализ существующих представлений об окружающем нас мире и месте человека в нем позволяет сделать вывод о том, что информация неразрывно связана с психическими процессами, осуществляемыми человеком в процессе взаимодействия с этим миром. Информация в этом взаимодействии выступает как средство регуляции и управления собственным поведением, что обеспечивает адекватные взаимоотношения с действительностью. Исходя из отмеченного, роль информации, ее значение в системе профессиональной деятельности специалистов МВД России заключается в том, что информация, рассматриваемая как психический феномен, выступает регулятивной основой профессиональной деятельности, формирующей ее путем выбора необходимого сценария деятельности в зависимости от предметно-субъективных условий ее осуществления.

Информация как объект в современном мире и как предмет жизнедеятельности и жизнеобеспечения имеет свои специфические особенности, к числу которых относится и ценность (важность) информации. Для сохранения ценности (важности) информации необходимо поддерживать ее потребительские свойства: достоверность, полноту, актуальность, своевременность, адекватность, избыточность, полезность, конфиденциальность, доступность и целостность. Последние три свойства информации являются ключевыми с точки зрения обеспечения ее безопасности.

Несмотря на свою неопределенность и многозначность информация выступает в качестве системообразующего фактора общественной жизни, составляя содержание общественных отношений, складывающихся в процессе социогенеза. Необходимо осуществляемое правовое регулирование этих отношений обуславливает выделение информации в качестве одного из объектов права, что имеет крайне важное значение с точки зрения анализа информации как объекта защиты.

Информация как объект правового регулирования представляет собой такую организационную форму, которая может быть определена как единая совокупность: содержания информации; реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры; материального носителя информации, на котором ее содержание и реквизиты закреплены.

Информация как категория, имеющая действительную или потенциальную ценность, как и любой другой вид ценности, может, а в отдельных случаях и должна защищаться ее обладателем.

Анализ действующего законодательства позволяет отнести к защищаемой информации: информацию с ограниченным доступом, общедоступную информацию, объекты интеллектуальной собственности.

Признание той роли, которую играет информацию в современном мире, привело к осознанию необходимости обеспечения информационной безопасности личности общества, государства, то есть обеспечения состояния защищенности их интересов в информационной сфере от воздействия различного рода угроз. При этом обеспечение информационной безопасности рассматривается как проблема, не сводящаяся лишь к защите (поддержанию параметров качества) информации, но и включающая вопросы защиты от негативных информационных воздействий.

В настоящее время условия осуществления правоохранительной деятельности характеризуются все возрастающей профессионализацией преступных сообществ, активным информационно-техническим противостоянием организованных преступных групп деятельности органов внутренних дел. Отмеченное актуализирует проблему обеспечения информационной безопасности органов внутренних дел, под которой понимается состояние защищенности информации, информационных ресурсов и информационных систем органов внутренних дел, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования.

В сложившихся условиях задача обеспечения информационной безопасности органов внутренних дел обусловлена необходимостью создания условий успешности реализации возложенных на органы внутренних дел функций по обеспечению законности и правопорядка, безопасности государства, общества и личности и носит системный характер, а ее решение возможно лишь путем принятия комплекса мер, затрагивающих различные аспекты данной задачи.

Контрольные вопросы

1. Что понимается под информацией в действующем законодательстве?
2. Приведите понятие документированной информации. В чем заключается сущность процесса документирования информации?
3. Перечислите основные реквизиты документов.
4. Перечислите виды информации в зависимости от порядка ее предоставления или распространения.
5. Что в действующем законодательстве понимается под информацией с ограниченным доступом?
6. Что понимается под защитой информации, каковы ее цели?
7. Раскройте понятие информационной безопасности, ее роль и место в современном мире, в обеспечении национальной безопасности России.
8. В чем заключаются национальные интересы Российской Федерации в информационной сфере?
9. Перечислите угрозы информационной безопасности России.
10. Приведите понятие информационной безопасности органов внутренних дел и раскройте его содержание.

2. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

2.1. Система обеспечения информационной безопасности органов внутренних дел

Для обеспечения информационной безопасности в органах внутренних дел проводятся различные мероприятия, объединяемые понятием «система обеспечения информационной безопасности органов внутренних дел».

Система обеспечения информационной безопасности органов внутренних дел *— это совокупность правовых, организационных и технических мероприятий, средств и методов защиты, органов управления и исполнителей, направленных на противодействие угрозам информационной безопасности с целью предотвращения или существенного затруднения утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней*[1].

Основой для построения системы обеспечения информационной безопасности органов внутренних является использование комплексного и системного подхода.

Комплексный и системный подход к организации обеспечения информационной безопасности предполагает, с одной стороны, выявление и анализ возможных каналов утечки защищаемой информации с учетом объемов такой информации и носителей, на которых она накапливается, ее важности. С другой стороны, изучаются и анализируются возможности предполагаемого злоумышленника по собиранию и добыванию защищаемой информации не вообще, а в каждом конкретном случае в отношении определенного подразделения органов внутренних дел, сотрудника или проблемы. Системный подход позволяет создать органически взаимосвязанную совокупность сил, средств и специальных методов по оптимальному ограничению сферы обращения засекреченной информации, предупреждению ее утечки. При создании системы защиты информации и осуществлении мероприятий по защите секретов от разглашения или новейших технических средств разведки важно предусматривать разносторонние комплексные защитные меры, направленные на предупреждение утечки информации из сферы ее обращения.

При этом основное требование к системе обеспечения информационной безопасности органов внутренних дел — это ее комплексность и адаптивность.

Требование комплексности подразумевает, что при создании системы обеспечения информационной безопасности будут учитываться все возможные каналы утечки информации, даже если некоторые из них и кажутся на пер-

[1] См.: Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (утв. приказом МВД России от 14 марта 2012 г. № 169) [Электронный ресурс]. Доступ из СТРАС «Юрист».

вый взгляд труднореализуемыми. Однако система — это «живой» организм, который должен быть способен реагировать на изменения оперативной обстановки, внешних условий деятельности объекта защиты, адаптироваться к ним. Это значит, что система обеспечения информационной безопасности должна предусматривать механизмы, позволяющие оперативно реагировать на возникновение новых угроз за счет перераспределения имеющихся сил и средств.

В настоящее время существуют различные подходы к построению системы обеспечения информационной безопасности организации. Их анализ позволяет сформулировать следующий обобщенный алгоритм построения системы обеспечения информационной безопасности органов внутренних дел.

1. Определение целей создания системы обеспечения информационной безопасности.

При принятии управленческих решений в процессе создания системы обеспечения информационной безопасности ведущим является процесс целеполагания. Он означает, что необходимо определится с целями, которые ставятся перед конкретной системой, и убедиться, что они соответствуют целям осуществления данного вида деятельности в системе МВД России.

Как уже отмечалось, в соответствии *с Концепцией обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года* «Целью обеспечения информационной безопасности органов внутренних дел является достижение с использованием методов технической, в том числе криптографической, защиты информации необходимого уровня защиты от специальных программно-технических воздействий, средств технических разведок, несанкционированного доступа, а также утечки информации по техническим каналам»[1].

Проецирование вышесказанного на уровень конкретного органа внутренних дел позволяет *в качестве основной цели построения системы обеспечения информационной безопасности выделить обеспечение целостности, доступности и конфиденциальности используемой в органах внутренних дел информации, достижение устойчивого функционирования используемых в практической деятельности органа внутренних дел информационных систем*.

2. Построение обобщенной модели возможного нарушителя.

Модель вероятного нарушителя информационной безопасности необходима для систематизации информации о типах и возможностях субъектов, целях несанкционированных воздействий и выработки адекватных мер противодействия. При разработке модели нарушителя учитываются: предположения о категориях лиц, к которым может принадлежать нарушитель; тип нарушителя; предположения о мотивах действий нарушителя (преследуемых нарушителем целях); предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах); ограничения и предположения о характере возможных действий нарушителей; характер информационных угроз[2].

---

[1] См.: Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (утв. приказом МВД России от 14 марта 2012 г. № 169) [Электронный ресурс]. Доступ из СТРАС «Юрист».

[2] См.: Миронова В.Г., Шелупанов А.А. Модель нарушителя безопасности конфиденциальной информации // Информационная безопасность систем. 2012. № 1(31). С. 28-34.

По отношению к системе нарушители могут быть не только внутренними, из числа персонала, но и внешними, посторонними лицами.

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и другие характеристики — важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы обеспечения информационной безопасности.

3. Построение модели угроз информационной безопасности.

Моделирование угроз является крайне необходимым условием построения эффективной системы обеспечения информационной безопасности. По сути, моделирование угроз безопасности представляет собой описание источников и характера угроз, их негативного воздействия на объект и находящихся в нем людей, структуры инженерно-технической системы защиты информации, порядка работы служб безопасности по предотвращению, выявлению и реагированию на угрозы. Модель должна иллюстрировать основные факторы, определяющие задачи, состав подразделений по обеспечению безопасности и структуру систем инженерно-технической защиты объекта.

Задача построения модели угроз требует учета наиболее существенных связей объектов и параметров процессов внутри организации. Исходя из этого, основными этапами моделирования являются: оценка потенциальных внутренних и внешних угроз, их ранжирование друг относительно друга по уровню вероятности реализации угроз, выработка предложений по организации реагирования на угрозы с целью поддержания нормального функционирования организации[1].

Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала[2]:

низкая вероятность — отсутствуют объективные предпосылки к реализации угрозы безопасности информации, отсутствует требуемая статистика по фактам реализации угрозы безопасности информации (возникновения инцидентов безопасности), возможная частота реализации угрозы не превышает 1 раза в 5 лет;

средняя вероятность — существуют предпосылки к реализации угрозы безопасности информации, зафиксированы случаи реализации угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на возможность реализации угрозы безопасности информации, возможная частота реализации угрозы не превышает 1 раза в год;

высокая вероятность — существуют объективные предпосылки к реализации угрозы безопасности информации, существует достоверная статистика

---

[1] См.: Моделирование угроз — ключевой аспект построения системы безопасности [Электронный ресурс]. — Режим доступа: http://www.cleper.ru/articles/description.php?n=354. — Загл. с экрана.

[2] См.: ФСТЭК России. Методика определения угроз безопасности в информационных системах (проект) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/ attachments/download/812. — Загл. с экрана.

реализации угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на высокую возможность реализации угрозы безопасности информации, частота реализации угрозы — чаще 1 раза в год.

4. Анализ фактического состояния существующей системы обеспечения информационной безопасности.

На данном этапе необходимо проанализировать существующую систему обеспечения информационной безопасности, выявить ее уязвимости и недостатки. Иными словами, — те слабые места системы, которые могут способствовать реализации угроз безопасности информации, используемой в деятельности органов внутренних дел. К числу таких слабых мест можно отнести: неэффективную систему контроля доступа в служебные помещения органов внутренних дел, использование открытых каналов связи, фактическое отсутствие необходимых технических средств защиты информации и т.д.

5. Оценка возможных рисков информационной безопасности.

Согласно ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» под *риском информационной безопасности* понимается возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Для определения количественных или качественных показателей ущерба проводится процедура оценки рисков информационной безопасности.

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

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

Методы первой и второй группы могут использовать количественные или качественные шкалы для определения величины риска информационной безопасности. В первом случае риск и все его параметры выражаются в числовых значениях. При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определенный интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от применяемых методик оценки рисков.

6. Вывод о необходимости создания системы обеспечения информационной безопасности, предполагаемых методах и средствах защиты информации.

Важно подчеркнуть, что создание системы обеспечения информационной безопасности не заканчивается внедрением средств и методов защиты инфор-

мации в технологию функционирования объекта защиты. В процессе эксплуатации системы проводится регулярный контроль ее эффективности, при необходимости осуществляется доработка системы обеспечения информационной безопасности, вызванная изменениями состава и характеристик средств защиты информации, а также оперативной обстановки и внешних условий деятельности объекта защиты[1].

С практической точки зрения реализация системы обеспечения информационной безопасности подразумевает комплексное использование различных методов, средств и способов защиты информации. Рассмотрим их подробнее.

2.2. Защита информации в обеспечении информационной безопасности органов внутренних дел

Изложенные ранее подходы к определению содержания понятия информационной безопасности позволяют выделить два основных направления обеспечения информационной безопасности органов внутренних дел:

– защита личного состава органов внутренних дел от негативных информационных воздействий;

– защита (поддержание параметров качества) информации, используемой в деятельности органов внутренних дел.

Реализация первого направления предполагает организацию выполнения мероприятий по обеспечению информационной безопасности личного состава органов внутренних дел с использованием всех возможных сил и средств: информационно-пропагандистской, психологической, социальной работы путем эффективного применения различных средств воспитания и использования потенциала ведомственных средств массовой информации. Иными словами, задача информационно-психологической защиты — через информацию таким образом воздействовать на психику и психологию личного состава, чтобы обеспечить достаточный уровень его морально-психологического состояния.

Реализация второго направления (***защита информации***) предполагает осуществление целого комплекса мероприятий, *направленных на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию*[2].

Сущность защиты информации раскрывается через ее предметную область, определяющую: виды, направления и соответствующие им способы, цели и задачи защиты информации. В рассмотрении указанного будем опираться на положения национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

---

[1] См.: Балановская А.В. Концептуальный подход к построению системы информационной безопасности промышленного предприятия // Вестник Самарского государственного университета. 2015. № 5(127). С. 14-20.

[2] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Виды защиты информации:

– правовая защита информации;

– техническая защита информации;

– криптографическая защита информации;

– физическая защита информации.

Правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации — защита информации с помощью ее криптографического преобразования.

Физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

Защита информации осуществляется следующими ***способами***:

– защита информации от утечки (защита информации от разглашения, защита информации от несанкционированного доступа (НСД), защита информации от [иностранной] разведки);

– защита информации от несанкционированного воздействия (НСВ);

– защита информации от непреднамеренного воздействия (НПДВ);

– защита информации от преднамеренного воздействия (ПДВ).

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Заинтересованными субъектами могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных норма-

тивными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от [иностранной] разведки — защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Защита информации от несанкционированного воздействия — защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — защита информации, 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 событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от преднамеренного воздействия — защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Целью защиты информации является заранее намеченный результат защиты информации. Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Общими целями защиты информации с учетом положений законодательства России являются:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

На конкретном объекте информатизации цели могут конкретизироваться.

Задачи защиты информации в зависимости от целей защиты в случаях, установленных законодательством России, обязаны выполнять обладатель информации или оператор информационной системы.

Задачи защиты информации:

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

2) своевременное обнаружение фактов несанкционированного доступа к информации;

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

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

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

6) постоянный контроль за обеспечением уровня защищенности информации.

Как и любая другая практическая деятельность, защита информации основывается на использование определенных методов, к числу которых относят следующие ***методы защиты информации***: препятствие, управление, маскировка, регламентация, принуждение, побуждение[1].

Препятствие как метод защиты информации предполагает создание на пути реализации угрозы объекту безопасности преграды, затрудняющей проникновение злоумышленника или распространение дестабилизирующего фактора.

Управление подразумевает оказание управляющих воздействий на элементы защищаемой системы.

Маскировка — действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника.

Регламентация — разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.

Принуждение заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности.

Побуждение — создание условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

Осуществление рассмотренных методов защиты информации реализуется посредством применения различных средств.

Средства защиты информации — *это совокупность технических, программных и социально-правовых средств, предназначенных для защиты информации.*

В своей совокупности все средства защиты информации могут быть подразделены на следующие основные группы:

---

[1] См.: Кузнецов И.Н. Информация: сбор, защита, анализ: учебник по информационно-аналитической работе. М.: ООО «Изд. Яуза», 2001. С. 47.

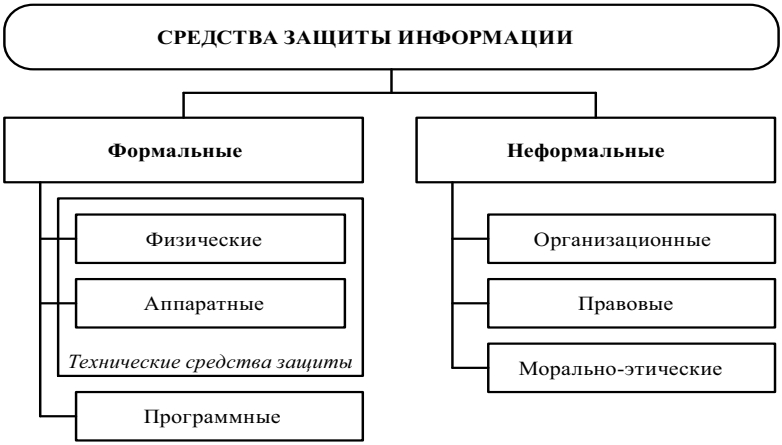


Рис. 2.1. Средства защиты информации

К *формальным средствам защиты информации* относят те средства, которые выполняют свои функции преимущественно без участия человека. Основу *неформальных средств* составляет целенаправленная деятельность людей.

Формальные средства защиты информации делятся на:

– физические;

– аппаратные;

– программные.

Физические средства защиты информации — это различные устройства и системы, предназначенные для создания препятствий на пути движения злоумышленников или распространения дестабилизирующих факторов.

Аппаратные средства защиты информации — это включаемые в состав информационной системы различные устройства, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа, выполняющие свои функции самостоятельно или в едином комплексе с программными средствами.

Физические и аппаратные средства объединяются в класс технических средств защиты информации.

Программные средства защиты информации — система специальных программ, включаемых в состав программного обеспечения информационной системы с целью решения задач по защите информации.

Неформальные средства защиты информации подразделяются на:

– организационные;

– правовые;

– морально-этические.

Организационные средства защиты информации — специально предусматриваемые в технологии функционирования объекта организационно-технические и организационно-правовые мероприятия, осуществляемые для организации и обеспечения защиты информации.

Правовые средства защиты информации — совокупность правовых актов, регулирующих вопросы защиты информации, а также устанавливающих ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

Морально-этические средства — сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а их нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе.

Практическое применение рассмотренных методов и средств защиты информации реализуется путем принятия различных мер, направленных на достижение установленных целей защиты информации: правовых, организационных, инженерно-технических, аппаратно-программных, криптографических, морально-этических, экономических.

Правовые меры защиты информации предполагают разработку и исполнение законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации.

Организационные меры направлены на регламентацию функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Эти мероприятия предусматривают тщательный подбор и расстановку кадров, обучение сотрудников правилам защиты информации, контроль за соблюдением режима секретности, правил обращения с защищаемой информацией.

Среди базовых организационных мер по защите информации можно выделить следующее:

– формирование политики безопасности;

– регламентация доступа в помещения;

– регламентация допуска сотрудников к использованию ресурсов информационной системы и др.;

– определение ответственности в случае несоблюдения требований информационной безопасности.

Организационные меры сами по себе не могут решить задачу обеспечения безопасности. Они должны работать в комплексе с техническими и программными средствами защиты информации в части определения действий людей.

Инженерно-технические меры — это комплекс организационных и технических мероприятий, направленных на организацию активно-пассивного противодействия средствам технической разведки и формирование рубежей охраны территории, зданий, помещений, оборудования с помощью комплексов технических средств.

Аппаратно-программные меры — использование различных защитных электронных и электронно-механические устройства, схемно встраиваемых в аппаратуру системы обработки, передачи и хранения информации, а также защитного программного обеспечения, например, антивирусного.

Криптографические меры — использование криптографических аппаратно-программных комплексов и программных пакетов.

Морально-этические (*морально-нравственные, воспитательные*) меры предполагают, прежде всего, воспитание сотрудника, допущенного к работе с защищаемой информацией. Они подразумевают проведение специальной работы, направленной на формирование у него системы определенных ка-

честв, взглядов и убеждений (прежде всего, понимания важности выполнения требований по защите информации), и обучение сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Экономические меры подразумевают разработку программ по обеспечению защиты информации, определение порядка их финансирования, а также совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических мер защиты информации.

Опыт показывает, что для обеспечения надежной защиты информации необходимо сочетание всех рассмотренных мер. Ни одну из них нельзя упускать, так как каждая мера дополняет другую и недостаток или отсутствие какой-либо из них приведет к нарушению защищенности информации. В этой связи нельзя не согласиться с В.В. Лапиным, заметившим, что «…защита информации — это понятие системное, комплексное, состоящее из множества различных…рубежей обороны (защиты) информационных ресурсов»[1].

Первый рубеж защиты, встающий на пути злоумышленника, является правовым. Он предусматривает установление определенных правил обращения с информацией и ответственности за их нарушение. Он также определяет возможность и/или необходимость применения иных мер защиты информации.

Вторым рубежом являются организационные меры защиты информации, которые направлены на то, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности, в том числе и путем контроля за выполнением установленных правил обращения с информацией.

Третий рубеж защиты определяется применением инженерно-технических мер защиты, предназначенных для противодействия средствам технической разведки, создания препятствий на возможных путях несанкционированного доступа злоумышленника к защищаемой информации.

Четвертый рубеж защиты определяется применением аппаратно-программных средств защиты информации самостоятельно или в комплексе с другими средствами.

Как можно заметить, основой построения системы защиты информации являются правовые, организационные и инженерно-технические меры, которые во многом определяют эффективность всей системы в целом. Рассмотрим подробнее организационно-правовые основы защиты информации, имея в виду, что содержание инженерно-технических и других мер защиты информации будет более детально рассмотрено в дальнейшем.

2.3. Организационно-правовые основы защиты информации в органах внутренних дел

Как уже ранее отмечалось, защита информации в органах внутренних дел осуществляется посредством применения целой совокупности различных средств защиты. Среди них крайне важное значение имеют правовые средства, поскольку в определяющей степени именно они регламентируют возможность применения других средств защиты информации.

---

[1] Лапин В.В. Основы информационной безопасности в ОВД: курс лекций. М.: Московский университет МВД России, 2009. С. 54.

Правовая защита информации *— это защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением*[1].

В качестве правовых мер защиты следует рассматривать:

– установление категорий информации ограниченного доступа на уровне законодательства;

– законодательное ограничение прав на доступ к категориям информации ограниченного доступа;

– лицензирование деятельности, связанной с защитой информации;

– сертификация средств защиты информации;

– установление правовой ответственности за разглашение различных видов тайны и компьютерные преступления, за нарушение правил защиты информации и т.п.

Правовая защита информации реализуется на международном и государственном уровне. На межгосударственном уровне правовая защита закреплена в конвенциях, договорах, декларациях, нормах авторского права, а на государственном уровне она регулируется нормативными правовыми актами, составляющими правовую основу законодательства в сфере защиты информации, и ведомственными правовыми актами по вопросам защиты информации (рис. 2.2).

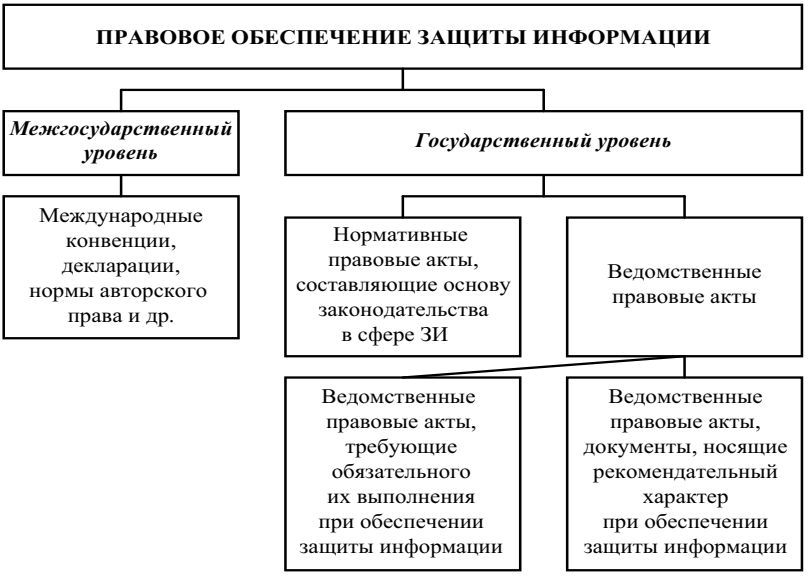


Рис. 2.2. Уровни правового обеспечения защиты информации

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

К первой группе относятся: Конституция, законы, указы Президента и постановления Правительства Российской Федерации, а также уголовный и гражданский кодексы Российской Федерации, Кодекс Российской Федерации об административных правонарушениях и другие нормативные правовые акты, определяющие юридическую ответственность участников процесса защиты информации и регулирующие основные вопросы обеспечения информационной безопасности.

К числу таких «специальных» законодательных актов, составляющих основу законодательства в сфере защиты информации, следует отнести:

– Конституцию Российской Федерации;

– Уголовный кодекс Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Кодекс Российской Федерации об административных правонарушениях;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;

– Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и др.

Ведомственные правовые акты по вопросам защиты информации — это приказы, руководства, положения и инструкции, издаваемые организациями в целях обеспечения защиты принадлежащей им информации. К данной группе относятся, прежде всего, в*едомственные правовые акты, требующие обязательного их выполнения при обеспечении защиты информации* (например, требования к защите информации и нормы защищенности, специальные требования по размещению и монтажу объектов информатизации, порядок и правила обращения с носителями секретных данных). Здесь особо следует выделить «Руководящие документы» по защите от несанкционированного доступа, подготовленные Федеральной службой по техническому и экспортному контролю (правопреемница Гостехкомиссии при Президенте Российской Федерации), а также гармонизированные ею «Критерии оценки безопасности информационных технологий» ITSEC, или «Европейские критерии». Данные документы имеют отношение, в основном, к программной и физической формам защиты информации.

К этой же группе относятся и разрабатываемые различными ведомствами правовые акты, документы по защите информации, носящие *рекомендательный характер*.

К числу ведомственных актов в сфере защиты информации в органах внутренних дел можно отнести:

– приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации»;

– приказ МВД России от 2 августа 2010 г. № 561 «Об утверждении концепции развития системы криптографической защиты информации в органах внутренних дел Российской Федерации до 2013 года»;

– приказ МВД России от 16 января 2012 г. № 25 «Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры»;

– приказ МВД России от 14 марта 2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» и др.

Одним из центральных элементов обеспечения правовой защиты информации и информационных ресурсов органов внутренних дел является ***институт тайны***, предусматривающий установление особого правового режима в отношении информации, требующей защиты.

С правовой точки зрения *тайна* представляет собой *охраняемые государством конфиденциальные сведения, незаконное получение, разглашение, использование которых создает угрозу нанесения вреда правам и законным интересам граждан, общества, государства и влечет за собой ответственность в соответствии с действующим законодательством Российской Федерации*[1].

Правовая защита информации, образующейся в рамках оперативно-служебной деятельности органов внутренних дел, осуществляется в режиме государственной или служебной тайны, режиме тайны следствия, персональных данных. Рассмотрим указанные правовые институты подробнее.

Государственная тайна

В соответствии со ст. 2 **Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»**, ***к государственной тайне относятся защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации***. Перечень таких сведений утвержден **Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»** (в последней редакции).

При этом, в соответствии со ст. 7 вышеупомянутого Закона, не подлежат отнесению к государственной тайне и засекречиванию сведения:

– о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

– о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

– о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

– о фактах нарушения прав и свобод человека и гражданина;

---

[1] См.: Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А.А. Стрельцов и др.; под ред. А.А. Стрельцова. М.: Издательский центр «Академия», 2008.

– о размерах золотого запаса и государственных валютных резервах Российской Федерации;

– о состоянии здоровья высших должностных лиц Российской Федерации;

– о фактах нарушения законности органами государственной власти и их должностными лицами.

Как следует из приведенного определения, к государственной тайне законодатель, помимо прочих, относит сведения в области оперативно-разыскной деятельности. Что это за сведения? Ответ на этот вопрос можно найти в принятом в 1995 году Федеральном законе «Об оперативно-розыскной деятельности»[1]. Согласно ст. 12 данного закона к ним относятся сведения:

– об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности;

– о лицах, внедренных в организованные преступные группы;

– о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе;

– об организации и о тактике проведения оперативно-розыскных мероприятий.

Указанные сведения подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-разыскную деятельность. При этом следует учитывать меру достаточной необходимости, которая позволяла бы сохранять в тайне вышеуказанные сведения и даже в случае рассекречивания ограничивала круг пользователей ими.

Порядок предоставления результатов оперативно-разыскной деятельности органам предварительного расследования регламентируется приказом МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

Помимо рассмотренных, к государственной тайне в системе органов внутренних дел относятся сведения и иного характера. Их перечень определяется приказом Министра внутренних дел, а защита осуществляется в соответствии с законодательством о защите государственной тайне.

Важным признаком государственной тайны является степень секретности сведений, отнесенных к ней.

В нашей стране принята следующая система обозначения сведений, составляющих государственную тайну:

– «особой важности»;

– «совершенно секретно»;

– «секретно».

---

[1] Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Эти грифы проставляются на документах или изделиях (их упаковках или сопроводительных документах). Содержащиеся под этими грифами сведения являются государственной тайной.

В соответствии с Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности (утв. постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870)[1]:

К сведениям *особой важности* следует относить такие сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях.

К *совершенно секретным* сведениям следует относить такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях.

К *секретным* сведениям следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Служебная тайна

В соответствии с **Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности**, утвержденным постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233, *к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью*[2].

При этом, не могут быть отнесены к служебной информации ограниченного распространения:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая

---

[1] Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

– решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

В системе МВД России служебную тайну составляет информация, которая:

– образуется в процессе деятельности органов, подразделений и учреждений системы МВД России или передана им из других федеральных органов исполнительной власти;

– не составляет государственной тайны, однако ее разглашение (распространение) может нанести ущерб интересам МВД России;

– имеет действительную или потенциальную ценность и может являться предметом посягательств в силу неизвестности ее другим лицам и отсутствия к ней свободного доступа на законных основаниях.

Не могут относиться к сведениям, составляющим служебную тайну:

– нормативные акты, устанавливающие правовой статус системы органов внутренних дел, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения, необходимые для обеспечения безопасной жизнедеятельности населенных пунктов, граждан и населения в целом, производственных объектов (сведения о чрезвычайных ситуациях, экологическая и др. информация);

– описание структуры МВД России, его функций, направлений и форм деятельности, а также адрес МВД России;

– порядок рассмотрения и разрешения жалоб, заявлений и устных обращений граждан, а также принятые по ним решения;

– сведения об исполнении бюджета и использовании других государственных ресурсов;

– документы, накапливаемые в открытых фондах библиотек и информационных системах организаций, необходимые для реализации прав и свобод граждан.

На документах (а в необходимых случаях и на их проектах), содержащих служебные сведения, проставляется пометка (гриф) «Для служебного пользования».

Передача документов, содержащих служебные сведения, другим органам и организациям осуществляется по мотивированному запросу с письменного разрешения соответствующего должностного лица – начальника органа, подразделения или учреждения внутренних дел.

Тайна следствия

Использование в практической деятельности следственных подразделений органов внутренних дел института **тайны следствия** имеет своей целью обеспечение эффективности деятельности по раскрытию и расследованию преступлений.

Суть этого правового института заключается в том, что сведения о ходе предварительного расследования могут быть преданы гласности только с разрешения прокурора, следователя или лица, производящего дознание (ст. 161 Уголовно-процессуального кодекса Российской Федерации). Такая информация может касаться как характера производимых следственных действий, так и доказательственной базы, перспектив расследования, круга лиц, участвующих в расследовании. Здесь важно отметить, что на законодательном уровне не закреплен перечень сведений, которые могут составлять тайну следствия. Это означает, что прокурор, следователь или дознаватель могут по своему усмотрению устанавливать, какая информация о предварительном расследовании может быть отнесена к тайне следствия, а какая — нет[1].

Следователь или дознаватель предупреждает участников уголовного судопроизводства о недопустимости разглашения ставших им известными данных предварительного расследования. Об этом у них берется подписка – «Подписка о неразглашении данных предварительного расследования».

Лицо, у которого отбирается подписка, предупреждается об уголовной ответственности, установленной ст. 310 Уголовного кодекса Российской Федерации. Об этом указывается в подписке.

Немаловажную роль в повышении эффективности деятельности органов внутренних дел по противодействию преступности играет надежная защита информации о лицах, содействующих расследованию. Ключевым элементом обеспечения конфиденциальности подобного рода сведений являются положения **Федерального закона от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»**.

В соответствии с этим законом одной из возможных мер безопасности в отношении защищаемого лица является обеспечение конфиденциальности сведений о нем. В том числе может быть наложен запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также могут быть изменены номера его телефонов и государственные регистрационные знаки используемых им или принадлежащих ему транспортных средств. Порядок защиты сведений об осуществлении государственной защиты устанавливается Правительством Российской Федерации.

Персональные данные

В действующем российском законодательстве правовое регулирование вопросов обеспечения защиты персональных данных осуществляется в рамках европейской **Конвенции о защите физических лиц при автоматизирован-**

[1] См.: Ахметшин Р.К. Уголовно-правовые и криминологические меры защиты информации, используемой в правоохранительной деятельности органов внутренних дел: дисс. … канд. юр. наук. М., 2006. С. 48.

ной обработке персональных данных (Страсбург, 28 января 1981 г.), ратифицированной Россией с некоторыми ограничениями, а также **Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**.

В соответствии с Федеральным законом «О персональных данных» под ***персональными данными*** понимается *любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу* (*субъекту персональных данных*).

По своей сути персональные данные представляют собой сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать личность. По своей правовой природе персональные данные — это *особый институт охраны прав на неприкосновенность частной жизни*. К подобного рода данным в общем случае можно отнести сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:

– биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);

– личные характеристики (в том числе о личных привычках и наклонностях);

– сведения о семейном положении (в том числе о семейных отношениях);

– сведения об имущественном, финансовом положении (кроме случаев, прямо установленных законом).

Основная цель принятия Федерального закона «О персональных данных» — обеспечение защиты прав граждан на неприкосновенность частной жизни при сборе и обработке персональных данных; создание правовых гарантий защиты конституционных прав человека и гражданина при обработке его персональных данных. При этом под ***обработкой персональных данных*** понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Необходимым условием обработки персональных данных является требование обеспечение их конфиденциальности.

В соответствии с п. 1 ст. 14 Федерального закона «О персональных данных» субъект персональных данных (то есть лицо, которому они принадлежат) имеет право на получение сведений о наличии у оператора (юридического или физического лица, занимающегося обработкой персональных данных) этих персональных данных, а также на ознакомление с ними. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Поскольку вся деятельность сотрудников органов внутренних дел, особенно в сфере борьбы с преступностью, немыслима без использования подобного рода информации, содержащейся, например, в криминалистических и иных

учетах, то особый интерес представляют положения п. 8 ст. 14 Федерального закона «О персональных данных», устанавливающие исключения из данного правила в случае, если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Правовой основой построения ведомственной системы защиты персональных данных, помимо вышеупомянутого закона, являются приказ МВД России от 6 июля 2012 г. № 678, утвердивший Инструкцию по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, а также приказ ФСТЭК России 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».

В соответствии с данными правовыми актами выбор мер обеспечения безопасности персональных данных осуществляется следующим образом. Из приложения к утвержденному приказом ФСТЭК России от 18 февраля 2013 г. № 21 документу выбирается базовый (обязательный) набор мер, соответствующий уровню защищенности персональных данных. Далее этот базовый набор мер адаптируется под конкретную информационную систему персональных данных и, в случае необходимости, дополняется мерами, необходимыми для нейтрализации угроз, смоделированных оператором, и предусмотренных требованиями прочих нормативных правовых актов в области защиты информации.

Несмотря на всю важность правовых мер защиты информации, они не будут иметь никакого смысла, если не будет обеспечен контроль за их практическим исполнением. Именно контроль за исполнением практических мер по защите информации, а также планирование, контроль и анализ выполнения других мероприятий составляет основное содержание ***организационных мер по защите информации***.

Организационные мероприятия всегда по праву занимают крайне важное место в системе обеспечения безопасности информации, поскольку зачастую возможности несанкционированного доступа к охраняемой информации обуславливаются не различными техническими аспектами, наличием или отсутствием каналов утечки информации, а небрежностью, халатностью пользователей или персонала, игнорирующего элементарные правила защиты информации, недостатками организации системы защиты информации в самой организации, учреждении.

Организационное обеспечение безопасности информации — *это регламентация служебной деятельности и взаимоотношений сотрудников на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к защищаемой информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий*.

По своей сути организационная защита информации является своеобразным «ядром» системы обеспечения информационной безопасности органов внутренних дел. Она призвана посредством выбора конкретных сил и средств реализовать на практике запланированные меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее разглашению, утечке и несанкционированному доступу к ней.

С содержательной точки зрения организационная защита информации может осуществляться по следующим основным направлениям:

– организация работы с сотрудниками;

– организация внутриобъектового и пропускного режимов и охраны;

– организация работы с носителями информации;

– комплексное планирование мероприятий по защите информации;

– организация аналитической работы и контроля.

Ведущую роль в организации защиты информации на объектах информатизации органов внутренних дел играет руководитель соответствующего органа. Он несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к информации с ограниченным доступом, и утраты носителей информации. Он обязан:

– знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки информации с ограниченным доступом;

– определять обязанности и задачи должностным лицам и структурным подразделениям органов внутренних дел в этой области;

– проявлять высокую требовательность к сотрудникам в вопросах сохранности информации с ограниченным доступом;

– оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

В органах внутренних дел для организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

– подразделения по защите информации;

– подразделения охраны и пропускного режима;

– режимно-секретные (выполняющие задачи по обеспечению установленного режима секретности и (или) ведению секретного делопроизводства) подразделения;

– библиотеки секретных изданий и секретных документов, машинописные, множительные и копировальные бюро, иные подразделения, основной функцией которых является обеспечение защиты государственной тайны.

В этих целях в структуре МВД России создана служба технической защиты информации. В составе Центров информационных технологий, связи и защиты информации территориальных органов МВД России на региональном уровне имеются отделы технической защиты информации (ОТЗИ ЦИТСиЗИ). К основным задачам ОТЗИ ЦИТСиЗИ относятся:

– организация в пределах своей компетенции и реализация мероприятий по технической защите государственной тайны и информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну в органах внутренних дел;

– обеспечение реализации единых технических и технологических решений, координация работ и в установленном порядке осуществление контроля деятельности территориальных органов МВД России на районном уровне;

– осуществление мониторинга и анализа состояния защиты информации в территориальном органе МВД России на региональном уровне, оценка угроз информационной безопасности территориальному органу МВД России на региональном уровне;

– организационно-методическое обеспечение деятельности структурных подразделений территориальных органов МВД России на региональном и районном уровнях.

ОТЗИ выполняют следующие основные функции:

– анализ и оценка состояния защиты информации в территориальном органе МВД России;

– разработка и внедрение комплекса организационных и технических мер по повышению уровня защищенности объектов информатизации в соответствии с действующими нормами и требованиями в данной области;

– информирование руководства территориального органа МВД России, а также по его поручениям — руководителей подразделений территориального органа МВД России об угрозах информационной безопасности территориального органа МВД России;

– осуществление контроля за эффективностью принятых мер по защите информации, в том числе за использованием средств защиты информации;

– планирование и организация контроля выполнения подразделениями территориального органа МВД России и территориальными органами требований нормативных правовых актов Российской Федерации, нормативных правовых актов и руководящих документов федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области защиты информации, приказов и распоряжений МВД России по вопросам деятельности ОТЗИ ЦИТСиЗИ, а также оказание им методической и практической помощи;

– осуществление мероприятий по организации и обеспечению противодействия техническим разведкам, технической защиты конфиденциальной ин-

формации, в том числе в информационных системах обработки персональных данных;

– организация разработки моделей угроз и моделей нарушителя на информационные системы, иных документов в области защиты информации;

– выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях, выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах, а также осуществление работ с использованием сведений, составляющих государственную тайну (при наличии лицензий ФСБ России);

– выполнение работ, связанных с созданием средств защиты информации, по технической защите конфиденциальной информации (при наличии лицензий ФСТЭК России);

– обеспечение деятельности органа по аттестации, комиссии территориального органа МВД России в области защиты информации.

Подразделения, обеспечивающие охрану и пропускной режим, создаются в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах органов внутренних дел посторонних лиц и транспорта, нанесения ущерба организации путем краж (хищений) с территории органов внутренних дел материальных средств и иного имущества. В настоящее время эти функции возложены на комендантские подразделения органов внутренних дел.

Режимно-секретные подразделения создаются в органах внутренних дел для решения задач организации, координации и контроля деятельности других структурных подразделений (сотрудников органов внутренних дел) по обеспечению защиты сведений, составляющих государственную или служебную тайну. Одной из основных функций этих подразделений является организация секретного делопроизводства. Реализация этой функции возлагается на подразделение делопроизводства и режима соответствующего органа внутренних дел.

Секретное делопроизводство *— это деятельность, обеспечивающая документирование секретной информации, организацию работы с такими документами и защиту содержащейся в них информации*.

Секретное (конфиденциальное) делопроизводство включает в себя все стадии работы с документами: подготовку и создание секретных документов, их учет и хранение, организацию работы с секретными документами и защиту документированной секретной информации в процессе осуществления управленческой, производственной, научной и иной деятельности.

Таким образом, задачами секретного делопроизводства являются:

– документирование секретной информации;

– организация работы с секретными документами;

– обеспечение защиты информации, содержащейся в секретных документах.

Кроме перечисленных, к работе по организации защиты информации могут привлекаться и иные структурные подразделения органов внутренних дел, для которых выполнение мероприятий по защите информации не является основной функцией. К таким подразделениям относятся кадровый орган, орган юридической службы (юрисконсульт), орган психологической и воспитательной работы и др.

Для проведения работ по организации защиты информации используются также возможности различных нештатных подразделений, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. В их числе постоянно действующая техническая комиссия по защите государственной тайны. К основным функциям этой комиссии относится выработка рекомендаций по защите сведений, составляющих государственную тайну, при решении следующих основных вопросов:

– организация, методическое обеспечение и проведение аналитической работы по предупреждению утечки и комплексной защите сведений, составляющих государственную тайну;

– подготовка решений в отношении информации о мероприятиях, выполняемых органами внутренних дел, подлежащих засекречиванию и защите;

– выработка предложений о дополнении и изменении перечня сведений, отнесенных к государственной тайне, развернутого перечня сведений, подлежащих засекречиванию, обеспечение организации внутриобъектового и пропускного режима;

– разработка научно-технической и методической базы по вопросам выявления и закрытия возможных каналов неправомерного распространения сведений, составляющих государственную тайну, в том числе по противодействию техническим разведкам, защите информационных систем, а также по совершенствованию системы физической защиты объектов;

– разработка системы мер противодействия техническим разведкам, защиты информационных систем, защиты сведений, составляющих государственную тайну;

– организация и координация разработки, внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;

– организация и проведение мероприятий по контролю за эффективностью принимаемых мер по выявлению и закрытию каналов неправомерного распространения сведений, составляющих государственную тайну;

– анализ обстоятельств и причин неправомерного распространения сведений, составляющих государственную тайну;

– подготовка предложений по совершенствованию действующей в органе внутренних дел системы защиты сведений, составляющих государственную тайну.

Приведенный перечень организационных мероприятий не является исчерпывающим и, в зависимости от специфики деятельности органа внутренних дел, степени конфиденциальности используемой информации, объема выполняемых работ, а также опыта работы в области защиты информации может быть дополнен иными мероприятиями.

2.4. Ответственность за правонарушения в сфере защиты информации

Очевидно, что нарушение установленных правил защиты информации, используемой в органах внутренних дел для решения возложенных на них задач, может повлечь различные негативные последствия, в том числе и для третьих

лиц — правообладателей подобного рода информации. В связи с этим действующим законодательством установлена обязанность по обеспечению безопасности защищаемой информации, а также определенные санкции за нарушение установленного порядка обращения с ней.

Общее правило, возлагающее на лицо, получившее доступ к информации с ограниченным доступом, обязанности по сохранению ее конфиденциальности, содержится в положениях Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В соответствии с в п. 2 ст. 9 вышеупомянутого закона, «…обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами». При этом, под конфиденциальностью информации законодатель понимает «…обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя» (ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Нарушение данного требования, а также совершение иных правонарушений в сфере защиты информации, влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации (п. 1 ст. 17 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Следует отметить, что данные положения закона, применительно к сотрудникам органов внутренних дел, напрямую вытекают и из принятого Генеральной ассамблеей ООН 17 декабря 1979 года **Кодекса поведения должностных лиц по поддержанию правопорядка**, в котором указывается, что «…сведения конфиденциального характера, получаемые должностными лицами по поддержанию правопорядка, сохраняются в тайне, если исполнение обязанностей или требования правосудия не требует иного»[1].

Дисциплинарная ответственность в органах внутренних дел применяется за нарушение трудовой, служебной, учебной дисциплины. Основным правовым актом, регламентирующим порядок наложения дисциплинарных взысканий в органах и подразделениях системы МВД России, является *Дисциплинарный устав органов внутренних дел Российской Федерации*, утвержденный Указом Президента Российской Федерации от 14 октября 2012 г. № 1377[2].

В соответствии с данным Уставом, за нарушение служебной дисциплины на сотрудников органов внутренних дел могут быть наложены следующие дисциплинарные взыскания: замечание, выговор, строгий выговор, предупреждение о неполном служебном соответствии, перевод на нижестоящую должность в органах внутренних дел, увольнение со службы в органах внутренних дел. Данный вид ответственности может применяться к сотруднику органов вну-

---

[1] См.: Кодекс поведения должностных лиц по поддержанию правопорядка (Принят резолюцией 34/169 Генеральной Ассамблеи ООН от 17 декабря 1979 года) [Электронный ресурс]. — Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/code_of_conduct.shtml. — Загл. с экрана.

[2] См.: Указ Президента Российской Федерации от 14 октября 2012 г. № 1377 «О Дисциплинарном уставе органов внутренних дел Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

тренних дел в случае нарушения им, например, режима секретности, правил обращения с информацией, относящейся к служебной тайне и т.п., если это правонарушение не влечет за собой административной или уголовной ответственности.

До наложения дисциплинарного взыскания от сотрудника, привлекаемого к ответственности, должно быть затребовано объяснение в письменной форме. При определении вида дисциплинарного взыскания принимаются во внимание: характер проступка, обстоятельства, при которых он был совершен, прежнее поведение сотрудника, совершившего проступок, признание им своей вины, его отношение к службе, знание правил ее несения и другие обстоятельства.

Дисциплинарный устав также определяет порядок обжалования дисциплинарного взыскания, сроки его применения и действия, порядок досрочного снятия.

Гражданско-правовая ответственность применяется при нарушении правовых норм, регулирующих гражданские отношения, и заключается в восстановлении незаконно нарушенных прав, в принудительном исполнении невыполненной обязанности. Основным источником права в этой области является *Гражданский кодекс Российской Федерации*. Как отмечается некоторыми авторами, «…особенность этого вида ответственности состоит в том, что в ряде случаев правонарушитель может без вмешательства государственных органов выполнить свои обязанности, восстановить нарушенные права, прекратить противоправное состояние. На этом основаны дополнительные санкции, применяемые к правонарушителю в процессе реализации данных отношений ответственности (пени, штрафы, другие меры понуждения)»[1].

Так, ст. 1064 ГК РФ устанавливает общие основания ответственности за причинения вреда, согласно которым лицо, причинившее вред личности или имуществу гражданина, а также вред, причиненный имуществу юридического лица, обязано возместить его в полном объеме. При этом обязанность возмещения вреда, причиненного работником организации при исполнении трудовых (служебных, должностных) обязанностей, возлагается на организацию.

В случае, если, например, должностное лицо органа внутренних дел осуществит разглашение полученной органом внутренних дел в установленном законом порядке информации, составляющей коммерческую тайну, то организация — орган внутренних дел обязано будет возместить ущерб, причиненный законному правообладателю этой информации. В свою очередь, это дает организации — органу внутренних дел право обратного требования (регресса) к сотруднику, причинившему вред, в размере выплаченного возмещения (ст. 1081 ГК РФ).

В случае причинения гражданину морального вреда (физических или нравственных страданий) действиями, нарушающими его личные неимущественные права, либо посягающими на принадлежащие гражданину нематериальные блага, этот вред также должен быть возмещен. При этом суд может возложить на лицо, виновное в причинении такого вреда, обязанность его ком-

[1] Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А.А. Стрельцов и др.; под ред. А.А. Стрельцова. М.: Издательский центр «Академия», 2008.

пенсации в денежной форме (ст. 151 ГК РФ). Также гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший эти сведения не докажет, что они соответствуют действительности.

Правовосстановительная ответственность возникает с момента правонарушения и завершается восстановлением (в установленных законом пределах) нарушенного правопорядка.

Административная ответственность осуществляется на основе *Кодекса Российской Федерации об административных правонарушениях*.

В соответствии со ст. 2.1 КоАП «…административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое настоящим Кодексом или законами субъектов Российской Федерации об административных правонарушениях установлена административная ответственность».

Мерой ответственности за совершение административного правонарушения является административное наказание, которое применяется в целях предупреждения совершения новых правонарушений как самим правонарушителем, так и другими лицами. Ст. 3.2 КоАП устанавливает следующие виды административных наказаний: предупреждение; административный штраф; конфискация орудия совершения или предмета административного правонарушения; лишение специального права, предоставленного физическому лицу; административный арест; административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства; дисквалификация; административное приостановление деятельности; обязательные работы; административный запрет на посещение мест проведения официальных спортивных соревнований в дни их проведения.

Современный Кодекс Российской Федерации об административных правонарушениях содержат значительное количество правонарушений в сфере защиты информации, за совершение которых виновное лицо может быть привлечено к административной ответственности, в том числе:

– нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11);

– нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) (ч.1 ст. 13.12);

– использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну) (ч. 2 ст. 13.12);

– нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну (ч. 3 ст. 13.12);

– использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну (ч. 4 ст. 13.12);

– грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) (ч. 5 ст. 13.12);

– нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 ст. 13.12 (ч. 6 ст. 13.12);

– нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 3 и 4 статьи 13.12, если такие действия (бездействие) не содержат уголовно наказуемого деяния (ч. 7 ст. 13.12);

– занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна) (ч. 1 ст. 13.13);

– занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии (ч. 2 ст. 13.13);

– разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 КоАП (ст. 13.14).

Производство по делу начинается с составления протокола об административном правонарушении. Дела об административных нарушениях рассматриваются судьями (мировыми судьями), должностными лицами федеральных органов исполнительной власти, осуществляющих государственный контроль в области обращения и защиты информации и других государственных органов, уполномоченным на то КоАП. Законодательством определены сроки привлечения к административной ответственности и исполнения наложенных взысканий.

За совершение административных правонарушений в сфере защиты информации применяются, как правило, такие виды административных наказаний, как: предупреждение, административный штраф, конфискация орудия совершения или предмета административного правонарушения.

Уголовная ответственность. За совершение наиболее опасных правонарушений (преступлений) в сфере информационной безопасности действующее законодательство предусматривает уголовную ответственность. Порядок осуществления уголовной ответственности регламентируется уголовным, уго-

ловно-процессуальным и уголовно-исполнительным законодательством. Уголовное законодательство составляет Уголовный кодекс Российской Федерации.

В соответствии со ст. 14 УК РФ, преступлением признается виновно совершенное общественно опасное деяние, запрещенное Уголовным кодексом под угрозой наказания. При этом, не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного Уголовным кодексом, но в силу малозначительности не представляющее общественной опасности.

Действующее уголовное законодательство содержит достаточно большое количество уголовно наказуемых правонарушений в сфере защиты информации, в том числе:

– незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе (ч. 2 ст. 183);

– разглашение сведений, составляющих государственную тайну (ст. 283);

– нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий (ст. 284);

– разглашение данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения, если оно совершено без согласия прокурора, следователя или лица, производящего дознание (ст. 310);

– разглашение сведений о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких, если это деяние совершено лицом, которому эти сведения были доверены или стали известны в связи с его служебной деятельностью (ст. 311);

– разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких, если это деяние совершено в целях воспрепятствования его служебной деятельности (ст. 320).

Имея ввиду неуклонно возрастающий уровень информатизации современного общества, широкое использование средств-носителей новых информационных технологий при подготовке и совершении преступлений, особо следует отметить главу 28 УК РФ, предусматривающую уголовную ответственность за:

– неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272);

– создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для не-

санкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273);

– нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (ст. 274).

Порядок привлечения определенного лица к уголовной ответственности регламентируется Уголовно-процессуальным кодексом Российской Федерации и включает в себя несколько стадий: возбуждение уголовного дела, предварительное расследование преступления, производство в судебном органе первой инстанции, кассационное и апелляционное производство, исполнение судебного приговора.

С момента привлечения к уголовной ответственности обвиняемый имеет право на защиту. Уголовно-процессуальным законодательством определены права и обязанности обвиняемого, подозреваемого и других участников уголовного судопроизводства, правомочия должностных лиц и государственных органов, ведающих производством по делу, порядок сбора и исследования доказательств, применения в случае необходимости принудительных мер (мер пресечения, обысков, выемок, приводов и др.).

2.5. Проблемы обеспечения безопасности информации в сфере деятельности органов внутренних дел по противодействию преступности

Занимая одну из ключевых позиций в системе правоохранительных органов государственной власти, органы внутренних дел осуществляют выполнение задач по обеспечению безопасности личности, охране общественного порядка и обеспечению общественной безопасности, защите частной, государственной, муниципальной и иных форм собственности, оказанию помощи физическим и юридическим лицам в защите их прав и законных интересов.

К числу важнейших задач, возложенных на органы внутренних дел действующим законодательством, относится также осуществление деятельности по выявлению, раскрытию и расследованию преступлений. Эта деятельность неразрывно связана с информацией и по сути своей носит ярко выраженный информационный характер. Как заметил по этому поводу Р.С. Белкин, «...в сущности, весь процесс расследования состоит из перемежающихся актов анализа имеющейся информации, выбора соответствующих этой информации приемов и средств работы с доказательствами и их применения…»[1]. В этой связи вполне закономерно, что органы внутренних дел наделены действующим законодательством весьма широкими полномочиями в сфере получения и обработки информации, необходимой для решения возложенных на них задач.

[1] Белкин Р.С. Курс криминалистики: учеб. пособие для вузов. - 3-е изд., доп. М.: ЮНИТИ-ДАНА, Закон и право, 2001. С. 803.

Юридическое закрепление информационных отношений, возникающих в сфере деятельности органов внутренних дел, регулируются, прежде всего, **Федеральным законом от 7 февраля 2011 г. № 3-ФЗ «О полиции» и Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»**.

Российская полиция в соответствии с Федеральным законом «О полиции» осуществляет широкую гамму действий в информационной сфере. Так, она обязана «…принимать и регистрировать (в том числе в электронной форме) заявления и сообщения о преступлениях, об административных правонарушениях, о происшествиях» (пп. 1 п. 1, ст. 12).

В соответствии с пп. 4 п. 1 ст. 13 Федерального закона «О полиции» ей предоставлено право «…в связи с расследуемыми уголовными делами и находящимися в производстве делами об административных правонарушениях, а также в связи с проверкой зарегистрированных в установленном порядке заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, разрешение которых отнесено к компетенции полиции, запрашивать и получать на безвозмездной основе по мотивированному запросу уполномоченных должностных лиц полиции от государственных и муниципальных органов, общественных объединений, организаций, должностных лиц и граждан сведения, справки, документы (их копии), иную необходимую информацию, в том числе персональные данные граждан; при выявлении и пресечении налоговых преступлений запрашивать и получать от кредитных организаций справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица; запрашивать и получать от медицинских организаций сведения о гражданах, поступивших с ранениями и телесными повреждениями насильственного характера либо с ранениями и телесными повреждениями, полученными в результате дорожно-транспортных происшествий, а также о гражданах, имеющих медицинские противопоказания или ограничения к водительской деятельности».

В соответствии с пп. 33 п.1 ст.13 Федерального закона «О полиции» полиция вправе «…вести видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок полиции; формировать, вести и использовать банки данных оперативно-справочной, криминалистической, экспертно-криминалистической, разыскной и иной информации о лицах, предметах и фактах; использовать банки данных других государственных органов и организаций, в том числе персональные данные граждан, если федеральным законом не установлено иное».

Согласно пп. 19 п.1 ст. 13 Федерального закона «О полиции» органы внутренних дел также уполномочены «…производить регистрацию, фотографирование, аудио-, кино- и видеосъемку, дактилоскопирование лиц, задержанных по подозрению в совершении преступления, заключенных под стражу, обвиняемых в совершении преступления, подвергнутых административному наказанию в виде административного ареста, иных задержанных лиц, если в течение установленного срока задержания достоверно установить их личность не представилось возможным, а также других лиц в соответствии с федеральным законом».

Для регулирования информационной работы в органах внутренних дел важное значение имеют правовые нормы **Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»**. Отметим положения Закона, наиболее важные для рассматриваемого вопроса.

В статье 10 Закона говорится: «Органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Федеральным Законом, могут создавать и использовать информационные системы, а также заводит дела оперативного учета». Если обратиться к статье 2 Закона, в которой излагаются задачи оперативно-розыскной деятельности, то становится ясным, что указанные информационные системы должны накапливать сведения, необходимые для выявления, предупреждения, пресечения и раскрытия преступлений, осуществления розыска лиц, скрывающихся от органов дознания, следствия и суда, а также для добывания сведений об угрозах государственной, военной, экономической или экологической безопасности Российской Федерации.

В статье 6 Закона содержится важное положение о том, что информационные системы МВД России и соответствующие внешние системы используются в ходе проведения оперативно-розыскных мероприятий. Таким образом, этим положением четко определяется одно из основных направлений информационной деятельности органов внутренних дел — информационное обеспечение оперативно-розыскной деятельности.

Чрезвычайно важные правовые основания для получения доступа к внешним по отношению к органам внутренних дел информационным массивам и банкам данных имеют статья 15 п. 1 и статья 6 Закона. Из них следует, что органы внутренних дел имеют право гласно и негласно собирать информацию (наводить справки). Основаниями для этого являются не только наличие возбужденного уголовного дела, но и сведения о признаках правонарушения и его субъектах, лицах, скрывающихся от дознания, следствия и суда, событиях или действиях, создающих угрозу экономической безопасности страны.

Отмеченное позволяет еще констатировать не только многообразие полномочий, которыми обладают органы внутренних дел в информационной сфере, но и ту ответственность, которая сопряжена с их практической реализацией. Каждый сотрудник органов внутренних дел обязан четко представлять, что за содержанием информации, обобщающих сведений и данных, с которыми он ежедневно имеет дело, стоят живые люди, и от того, насколько ответственно и профессионально грамотно он работает с информацией, нередко зависят судьбы конкретных людей. В этой связи обеспечение эффективной защиты информации, используемой в деятельности по выявлению, раскрытию и расследованию преступлений, является одной из основных задач органов внутренних дел в информационной сфере.

Вместе с тем, анализ существующего положения дел позволяет выделить целый ряд проблемных вопросов в рассматриваемой сфере.

Так, в Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года констатируется наличие целого ряда проблем в сфере обеспечения информационной безопасности ОВД, требующих своего решения:

– приведение ведомственной нормативной правовой базы в соответствие с законодательством Российской Федерации, регулирующим вопросы обеспечения защиты информации;

– обеспечение ОВД требуемым объемом средств защиты информации, в том числе криптографическими средствами, необходимыми для организации технической защиты информации;

– создание сети органов по аттестации объектов информатизации и оснащению их современными средствами защиты информации, контрольно-измерительной и поисковой техникой;

– организация профессиональной подготовки и переподготовки сотрудников подразделений МВД России в области информационной безопасности.

Несмотря на то, что данные проблемы носят в значительной степени общий характер, они оказывают самое непосредственное негативное воздействие и на эффективность защиты информации в деятельности по раскрытию и расследованию преступлений.

Помимо отмеченного, к числу факторов, влияющих на уровень безопасности информации, используемой в оперативно-следственной деятельности, можно отнести также[1]:

1. Активное противодействие, в том числе и информационно-техническое, деятельности органов внутренних дел со стороны криминального сообщества.

2. Широкое использование криминальными структурами средств и тактики оперативно-розыскной деятельности.

3. Наличие в стране нелегального рынка специальных технических средств негласного получения информации.

4. Недостаточно высокий уровень профессиональной подготовки сотрудников органов внутренних дел в сфере информационной безопасности.

5. Недостаточная разработанность тактики и методики защиты информации при проведении следственных действий и оперативно-разыскных мероприятий.

5. Несовершенство законодательства, главным образом, — в сфере борьбы с организованной и международной преступностью, коррупцией и незаконным оборотом наркотиков.

6. Недостаточное ресурсное обеспечение правоохранительной деятельности.

7. Коррупционные проявления в органах внутренних дел.

8. Девальвация нравственных ценностей общества.

Практические проявления данных факторов обуславливают возникновение различного рода угроз безопасности информационным ресурсам и информационной инфраструктуре органов внутренних дел, используемым в противодействии современной преступности. К подобного рода угрозам относят, в том числе[2]:

---

[1] См. также: Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г. Основы информационной безопасности в ОВД: учебник для вузов. СПб: Университет МВД России, 2010.

[2] См. также: Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г. Основы информационной безопасности в ОВД: учебник для вузов. СПб: Университет МВД России, 2010.

– неконтролируемое распространение (утечку) защищаемой информации в результате разглашения, несанкционированного доступа, ведения агентурной и технической разведок;

– несанкционированные воздействия на информационные ресурсы, средства и системы информатизации;

– нарушение установленного порядка обработки и использования защищаемой информации;

– недостаточное ресурсное обеспечение формирования инфраструктуры и эксплуатации средств информатизации оперативно-следственных подразделений;

– отказы в работе технических средств и систем информатизации;

– широкое применение средств и систем информатизации зарубежного производства;

– шантаж оперативных и следственных работников, целенаправленно осуществляемый организованными преступными группами;

– формирование средствами массовой информации искаженного представления о деятельности органов внутренних дел.

В данных условиях проблема обеспечения надежной защиты информации органов внутренних дел приобретает особую актуальность. Особая значимость вопросов защиты информации в деятельности органов внутренних дел обуславливается все неуклонно возрастающим уровнем информационно-технического противодействия со стороны криминального мира, направленного на организацию утечки защищаемой информации с целью воспрепятствовать осуществлению органами правопорядка своих полномочий в сфере уголовного судопроизводства.

Подводя итог вышесказанному, можно сделать следующие выводы.

Для обеспечения информационной безопасности в органах внутренних дел проводятся различные мероприятия, объединяемые понятием «система обеспечения информационной безопасности органов внутренних дел». Алгоритм построения подобного рода системы необходимо предусматривает: определение целей создания системы обеспечения информационной безопасности; построение обобщенной модели возможного нарушителя; построение модели угроз информационной безопасности; анализ фактического состояния существующей системы обеспечения информационной безопасности; оценку возможных рисков информационной безопасности и, наконец, вывод о необходимости создания системы обеспечения информационной безопасности, предполагаемых методах и средствах защиты информации.

Защита информации является одним из важнейших направлений обеспечения информационной безопасности органов внутренних дел и предполагает осуществление целого комплекса мероприятий, направленных на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Как и любая другая деятельность, защита информации основывается на использование определенных методов, средств и способов защиты информации, практическое применение которых реализуется путем осуществления различ-

ных мер, направленных на достижение установленных целей защиты информации: правовых, организационных, инженерно-технических, аппаратно-программных, криптографических, морально-этических, экономических.

Защита информации — это понятие системное, комплексное, состоящее из множества различных рубежей защиты информационных ресурсов. Основой построения системы защиты информации являются правовые и организационные меры, которые во многом определяют эффективность всей системы в целом.

Правовая защита информации — это защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. Она реализуется на международном и государственном уровне. На межгосударственном уровне правовая защита закреплена в конвенциях, договорах, декларациях, нормах авторского права, а на государственном уровне она регулируется нормативными правовыми актами, составляющими правовую основу законодательства в сфере защиты информации, и ведомственными правовыми актами по вопросам защиты информации.

Одним из центральных элементов обеспечения правовой защиты информации и информационных ресурсов органов внутренних дел является институт тайны, предусматривающий установление особого правового режима в отношении информации, требующей защиты. Правовая защита информации, образующейся в рамках оперативно-служебной деятельности органов внутренних дел, осуществляется в режиме государственной или служебной тайны, режиме тайны следствия, персональных данных.

Несмотря на всю важность правовых мер защиты информации, они не будут иметь никакого смысла, если не будет обеспечен контроль за их практическим исполнением. Именно контроль за исполнением практических мер по защите информации, а также планирование, контроль и анализ выполнения других мероприятий составляет основное содержание организационных мер по защите информации, которые могут осуществляться по следующим основным направлениям: организация работы с сотрудниками; организация внутриобъектового и пропускного режимов и охраны; организация работы с носителями информации; комплексное планирование мероприятий по защите информации; организация аналитической работы и контроля.

Ввиду той важности, которые играют информация и ее защита в современном обществе, действующим законодательством установлена обязанность по обеспечению безопасности защищаемой информации, а также определенные санкции за нарушение установленного порядка обращения с ней. Совершение сотрудником органов внутренних дел правонарушений в сфере защиты информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность.

Данное обстоятельство необходимо иметь ввиду всем сотрудникам органов внутренних дел, поскольку органы внутренних дел наделены весьма широкими полномочиями в сфере получения и обработки информации, необходимой для решения возложенных на них задач. Каждый сотрудник органов внутренних дел обязан четко представлять, что за содержанием информации, обобща-

ющих сведений и данных, с которыми он ежедневно имеет дело, стоят живые люди, и от того, насколько ответственно и профессионально грамотно он работает с информацией, нередко зависят судьбы конкретных людей. В этой связи обеспечение эффективной защиты информации, используемой в деятельности по выявлению, раскрытию и расследованию преступлений, является на современном этапе одной из основных задач органов внутренних дел в информационной сфере.

Контрольные вопросы

1. В чем заключается комплексный и системный подход к организации защиты информации?
2. Перечислите и раскройте основные методы защиты информации.
3. Что понимается под средствами защиты информации.
4. В чем заключается различие формальных и неформальных средств защиты информации?
5. Что понимается под системой обеспечения информационной безопасности?
6. В чем заключается правовое обеспечение защиты информации?
7. Раскройте правовой институт государственной тайны.
8. Что представляет собой служебная тайна как правовой институт защиты информации?
9. Перечислите основные организационные меры защиты информации.
10. Перечислите основные угрозы безопасности информации, используемой в оперативно-следственной деятельности.

3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

3.1. Понятие и виды каналов утечки информации на объектах информатизации

Объект информатизации *— это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров*[1].

В процессе функционирования объекта информатизации защищаемая информация может по различным причинам выйти за пределы установленной сферы обращения. В этом случае утрачивается контроль за ее распространением — происходит утечка информации.

Утечка информации *— это неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками*[2].

Утечку информации в общем плане можно рассматривать как бесконтрольный и неправомерный выход защищаемой информации за пределы организации или круга лиц, которым эта информация была доверена.

Как можно заметить, утечка защищаемой информации происходит, как правило, в результате ее разглашения или несанкционированного доступа к ней.

Разглашение информации *— это несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации*[3].

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См.: Национальный стандарт Российской Федерации ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] См.: Национальный стандарт РФ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Несанкционированный доступ к информации (НСД) *— получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации*[1]. При этом, заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

К числу наиболее распространенных факторов, способствующих утечке информации органов внутренних дел, можно отнести:

– несовершенство правового обеспечения защиты информации в органах внутренних дел;

– нарушение установленных правил защиты информации;

– недостаточность сил и средств для перекрытия каналов утечки информации.

Практические проявления данных факторов могут привести к утечке информации в случае, если этому будут способствовать соответствующие объективные или субъективные условия:

объективные:

– недостаточная правовая регламентация вопросов защиты информации по отдельным вопросам деятельности органов внутренних дел;

– текучесть кадров;

– несоответствие условий деятельности сотрудников органов внутренних дел требованиям по защите информации;

субъективные:

– незнание сотрудниками органов внутренних дел правовых актов, требований по защите информации;

– недостаточное внимание руководства вопросам организации работы по обеспечению защиты информации в органах внутренних дел;

– слабый контроль за выполнением требований по защите информации в практической деятельности сотрудников органов внутренних дел.

Утечка защищаемой информации является следствием практического проявления угроз информационной безопасности, рассмотренных ранее. Именно практическая реализация этих угроз создает предпосылки и возможности для образования канала утечки защищаемой информации.

Канал утечки информации *— это физический путь несанкционированного распространения носителя с защищаемой информацией от ее источника к злоумышленнику*[2]. В зависимости от используемых противником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают ***агентурные, легальные и технические каналы утечки информации***.

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005. С. 171.

1. ***Агентурный канал утечки информации*** *— это использование противником тайных агентов для получения несанкционированного доступа к защищаемой информации*.

Методы агентурной разведки известны с древнейших времен. Например, еще в IV веке до нашей эры известный китайский полководец Сунь-Цзы в главе «Использование секретных агентов» своей книги «Трактат о военном искусстве» раскрыл методы ведения шпионажа, многие из которых используются и в наши дни.

Опасность агентурной разведки заключается в том, что агент имеет непосредственный доступ к секретной информации. Он находится среди тех, кто работает с секретными сведениями и осуществляет их защиту. Однако не менее опасны агенты, имеющие лишь косвенное отношение к конфиденциальным сведениям. В некоторых случаях они имеют возможность добывать очень ценную информацию, не привлекая к себе пристального внимания контрразведки в силу своего невысокого служебного статуса.

Для добывания защищаемой информации через агентуру используются следующие методы: *наблюдение, выведывание, доступ к конфиденциальной информации по службе*.

Используя *доступ по службе* к секретным работам и документам агент в целях сбора интересующей его информации может ее запомнить, делать выписки из документов, осуществлять их копирование или фотографирование и т.д. При выведывании информации расчет делается на «человеческий фактор»: при определенных условиях человек может утратить чувство бдительности и невольно выдать агенту интересующую его информацию. Задача агента заключается в том, чтобы создать такие условия. *Наблюдение* может быть физическим, электронным или комплексным, то есть сочетающим в себе элементы того и другого[1].

2. ***Легальные каналы утечки информации*** *— это использование противником открытых источников информации, выведывание под благовидным предлогом сведений у лиц, которым они доверены по службе*.

Как можно заметить, основным объектом деятельности в рамках легальных каналов утечки ***информации является информация, полученная из открытых источников*** *— не имеющая правовых ограничений публично доступная информация* (*то есть информация, которую любой желающий может законно получить в результате сделанного запроса, проведенного наблюдения или ознакомления с материалами, распространяемыми по каналам массовой коммуникации*), *а также другая, не охраняемая в режиме тайны информация, которая имеет ограниченное публичное распространение или доступ*[2].

К данному виду информации относится подавляющее большинство научной и технической информации, в том числе и те научно-технические издания,

---

[1] См.: Журавленко Н.И., Курбанов Д.А. Основы теории и методологии защиты информации в органах внутренних дел: монография. Уфа: УЮИ МВД РФ, 2001. С. 68.

[2] См.: Григорьев А.Н. Теоретические аспекты информации и ее защиты в предварительном расследовании преступлений: дисс. ... канд. юрид. наук. Калининград: Калининградский юридический институт МВД РФ, 2002. С. 68.

которые выходят только в электронной форме и доступ к которым возможен в том числе и через Интернет, данные состояния рынка, официальные статистические данные и др. За рубежом деятельность по сбору данной категории информации еще называют «разведкой из открытых источников» (Open Source Intelligence – OSCINT) или «легальной разведкой».

Открытая информация является одним из основных объектов интереса также и для правительственных разведслужб. Так, доктор Пауль Леверкюн в своих воспоминаниях о службе разведки и контрразведки Германии, опубликованных еще в 1953 г., писал: «Термин «разведывательная служба» следует понимать в самом широком смысле, т.е. не только как добывание сведений о том, что хранится в тайне от других, но и как изучение того, что открыто выставляется, публикуется и пишется противником»[1].

3. ***Технические каналы утечки информации*** подразумевают использование специальных технических средств для несанкционированного доступа к защищаемой информации. Их спектр весьма широк: от простейших радиомикрофонов стоимостью несколько десятков долларов до сложнейших систем перехвата конфиденциальной информации стоимостью в десятки, сотни тысяч долларов. В настоящее время этот внушительный технический арсенал с успехом применяется криминальными элементами для подготовки и совершения преступлений, организации противодействия правоохранительным органам. Ввиду особой актуальности данного вопроса рассмотрим технические канала утечки информации и основные подходы к организации защиты информации от утечки по ним подробнее.

3.2. Технические каналы утечки информации

В настоящее время деятельность правоохранительных органов осуществляется в условиях усиливающегося информационно-технического противодействия со стороны преступных формирований. Дознание и следствие зачастую сводятся на нет по той причине, что криминальные элементы с помощью новейших технических средств негласного получения информации легко заполучают необходимые сведения о конкретной направленности деятельности органов расследования и без особого труда и опасности парализуют их работу. Отмеченное позволяет отнести утечку информации по техническим каналам к одной из основных угроз безопасности информации ограниченного доступа, используемой в деятельности органов внутренних дел.

Под ***утечкой информации по техническим каналам*** понимается *неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации*[2].

---

[1] Леверкюн П. Служба разведки и контрразведки // Итоги Второй мировой войны. Выводы побежденных. СПб: Полигон; М.: АСТ, 1998. С. 174.

[2] Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005: утв. Приказом Ростехрегулирования от 29 декабря 2005 г. № 479-ст . Введ. 2006-06-01. М.: Стандартинформ, 2006.

Перехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов[1].

Таким образом, по своей сути т***ехнический канал утечки информации*** — *это физический путь несанкционированного распространения информации от носителя защищаемой информации до технического средства, осуществляющего перехват информации*[2].

С содержательной точки зрения технические каналы утечки информации представляют собой «…совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал»[3]. Подобный подход к определению содержания данного понятия отмечается и правовых актах в области защиты информации. Так, в Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года под техническим каналом утечки защищаемой информации понимается совокупность носителя информации (средства обработки), физической среды передачи информации и средств, с помощью которых добывается защищаемая информация[4]. Схожее определение технического канала утечки информации можно встретить и в Специальных требованиях и рекомендациях по технической защите конфиденциальной информации (СТР-К)», утвержденных решением коллегии Гостехкомиссии России № 7.2/02.03.2001 г.

В соответствии с вышесказанным, типовой технический канал утечки информации содержит: источник информации — носитель информации, физическую среду распространения информационного сигнала и техническое средство разведки, с помощью которого осуществляется его (сигнала) регистрация (рис. 3.1).

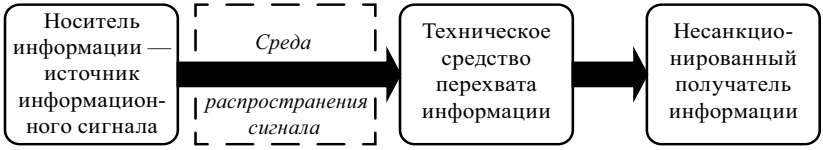


Рис. 3.1. Технический канал утечки информации

---

[1] Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005: утв. приказом Ростехрегулирования от 29 декабря 2005 г. № 479-ст . Введ. 2006-06-01. М.: Стандартинформ, 2006.

[2] См.: Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005. С. 171-172.

[3] Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: ООО «Издательство Машиностроение», 2009. С. 24; Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учебное пособие. М.: Гостехкомиссия России, 1998. С. 11.

[4] См.: Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (утв. приказом МВД России от 14 марта 2012 г. № 169) [Электронный ресурс]. Доступ из СТРАС «Юрист».

В научной литературе[1], действующей нормативно-правовой базе[2] приводятся различные подходы к классификации технических каналов утечки информации. Примем за основу подход, изложенный в работах А.А. Хорева, А.А. Шелупанова и других ученых[3], согласно которому все многообразие технических каналов утечки информации можно разделить на четыре основные группы:

– технические каналы утечки информации, обрабатываемой техническими средствами приема и передачи информации;

– технические каналы утечки информации, передаваемой по каналам связи;

– технические каналы утечки речевой информации;

– технические каналы утечки видовой информации.

Технические каналы утечки информации, обрабатываемой техническими средствами приема и передачи информации. В настоящее время практически любой вид человеческой деятельности сопряжен с использованием *технических средств приема и передачи информации*, к которым относятся средства вычислительной техники, офисные АТС, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.п.

В зависимости от физической природы возникновения информационного сигнала, а также среды его распространения и способов перехвата технические каналы утечки информации, обрабатываемой техническими средствами ее приема и передачи, подразделяют на:

Электромагнитные:

---

[1] См.: Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учебное пособие/под редакцией Ю.Ф. Каторина. СПб: НИУ ИТМО, 2012; Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005; Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008 и др.

[2] См., например: приказ ФСБ России от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»; постановление Правительства России от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: ООО «Издательство Машиностроение», 2009; Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учебное пособие. М.: Гостехкомиссия России, 1998.

– перехват побочных электромагнитных излучений элементов технических средств приема и передачи информации, электромагнитных излучений на частотах работы их высокочастотных генераторов и частотах самовозбуждения усилителей низкой частоты;

электрические:

– съем наводок электромагнитных излучений технических средств приема и передачи информации на соединительные линии и проводники;

– съем информационных сигналов с линий электропитания и цепей заземления технических средств приема и передачи информации;

– съем информации путем установки в технические средства приема и передачи информации аппаратных закладок;

параметрические:

– перехват информации путем «высокочастотного облучения» технических средств ее приема и передачи.

Технические каналы утечки информации, передаваемой по каналам связи. Практическая деятельность органов внутренних дел немыслима без использования каналов радио- и радиорелейной связи. Подобного рода каналы связи характеризуются тем, что в них в качестве среды передачи информационного сигнала используются электромагнитные волны, поэтому технический канал перехвата информации, передаваемой по этим каналам связи, носит название *электромагнитного*. Он заключается в перехвате специальными техническими средствами ведения радиоразведки высокочастотных электромагнитных излучений передатчиков средств связи, модулированных информационным сигналом, и их последующим декодированием.

Рассматриваемый канал перехвата информации наиболее широко используется для прослушивания разговоров, ведущихся по радиотелефонам, радиостанциям, сотовым телефонам, радиорелейным и спутниковым линиям связи.

Самый простой случай реализации электромагнитного канала утечки информации, передаваемой по каналам радио- и радиорелейной связи, — это перехват переговоров, ведущихся с использованием радиотелефонов и радиостанций, практически повсеместно используемых в деятельности органов внутренних дел. Что такое радиостанция, вполне понятно. Радиотелефон же по своей сути представляет собой комплекс, состоящий из двух радиостанций, — мобильной и стационарной, которая обладает большей мощностью и подключается к телефонной сети. Так как для обмена информацией между станциями используется радиоканал, то для прослушивания радиотелефонных разговоров вполне достаточно наличие комплекса, состоящего из приемника с соответствующим диапазоном, антенны и устройства звукозаписи для фиксации перехваченной информации.

Наряду с мобильными системами связи в практике деятельности органов внутренних дел широкое применение нашли и системы связи, использующие для распространения сигнала твердые среды, то есть те, в которых передача сигнала осуществляется по специально проложенным проводным линиям.

Прежде всего, речь идет, конечно же, о телефонных линиях связи. В общем виде структура телефонной системы связи выглядит следующим образом (рис. 3.2)[1].

[1] Лысов А.В., Остапенко А.Н. Телефон и безопасность (Проблемы защиты информации в телефонных сетях). СПб, 1995. С. 7.

Рис. 3.2. Структурная схема телефонной системы связи

Сигнал с аппарата по телефонному проводу попадает в распределительную коробку, а оттуда в кабельную линию. После коммутации на автоматической телефонной станции (АТС) сигнал распространяется по многоканальным кабелям либо по радиоканалу.

Наибольшую опасность в плане перехвата информации представляет участок от телефонного аппарата абонента до АТС. В общем случае можно выделить два способа перехвата информации на этом участке.

Первый способ заключается в несанкционированном контактном подключении к проводным линиям связи и перехвате передаваемых по ним информационных электрических сигналов (поэтому он носит название электрического).

Следует заметить, что это самый простой способ перехвата телефонных разговоров, доступный даже непрофессионалам. Наиболее вероятное место перехвата информации данным способом — участок между телефонным аппаратом абонента и распределительной коробкой, то есть то место, к которому имеется относительно свободный доступ. Безусловно, данный способ может быть использован и на других участках телефонной сети, однако в плане практической реализации он гораздо сложнее, поскольку для этого необходимо не только получить доступ к магистральным кабельным линиям, пролегающим под землей, но и правильно определить нужную телефонную пару в магистральном многожильном кабеле.

Самый простой способ перехвата телефонных разговоров по данному каналу — это параллельное подключение к телефонной линии (постоянное или временное), схема реализации которого показана на рис. 3.3.

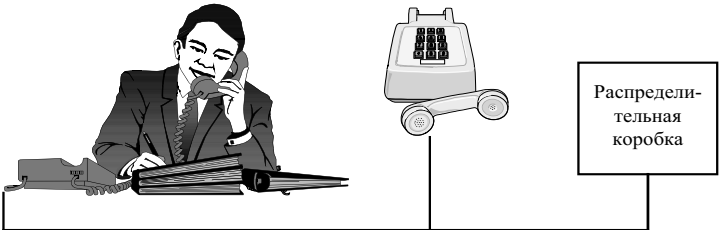


Рис. 3.3. Схема непосредственного подключения к телефонной линии

Для постоянного прослушивания телефонных разговоров по конкретному номеру в любом удобном месте (например, в соседнем помещении) может быть установлен параллельный телефон, с которого систематически может вестись контроль ведущихся по данному номеру разговоров. Однако, в случае

необходимости осуществить прослушивание конкретного телефонного разговора может быть использован и стандартный тестовый телефон («монтерская трубка»), с помощью которого может быть осуществлено временное подключение к нужной телефонной линии в любом доступном месте.

Следует заметить, что на практике данные способы перехвата информации, передаваемой по телефонной линии, профессионалами, как правило, не применяются, поскольку параллельное подключение к телефонной линии, во-первых, достаточно легко обнаружить, а во-вторых, крайне велик риск быть обнаруженным. В большей степени это удел «любителей».

В случае контактного подключения к телефонным линиям в подавляющем большинстве случаев для этих целей используются телефонные радиозакладки — устройства, обеспечивающие перехват информации, передаваемой по телефонной линии, и ее передачу оператору по радиоканалу. Подключение таких устройств к телефонной линии может осуществляться практически в любом доступном месте, а так как в основном они питаются от телефонной линии, то срок их службы не ограничен.

Однако, помимо непосредственного (контактного) подключения к проводным линиям, съем передаваемой по ним информации возможен также и путем использования технических средств разведки, обеспечивающих детектирование и преобразование электромагнитного поля, возникающего вокруг проводных линий при прохождении по ним электрического информационного сигнала (данный технический канал утечки информации называется индукционным). Достоинством данного способа съема информации с телефонной линии является то, что не требуется непосредственное подключение к линии, вследствие чего значительно снижается вероятность обнаружения проводимого мероприятия по перехвату информации. Однако качество перехватываемой информации, как правило, значительно хуже, чем при использовании устройств с непосредственным (гальваническим) подключением. Кроме того, питание устройств бесконтактного съема информации с телефонной линии осуществляется от встроенных источников питания, что также накладывает определенные ограничения на возможности их использования.

Для перехвата информации по данному каналу, как правило, применяются бесконтактные датчики, использующие в качестве канала передачи перехваченной информации проводные линии (вывод информации осуществляется на головные телефоны либо звукозаписывающее устройство) или радиоканал (схема их использования показана на рис. 3.4).

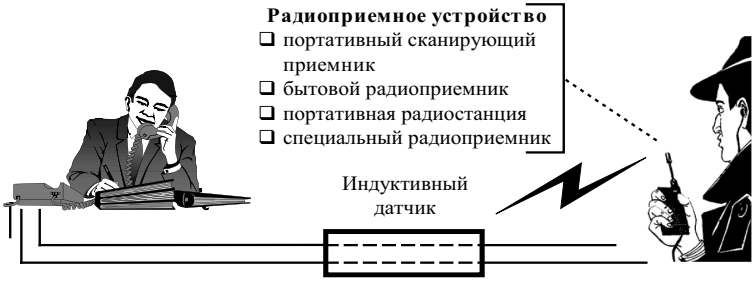


Рис. 3.4. Схема бесконтактного перехвата информации, передающейся по телефонной линии

В общем виде некоторые возможные схемы утечки информации, обрабатываемой техническими средствами приема и передачи информации, а также передаваемой по каналам связи, могут быть представлены так, как это показано на рис. 3.5.

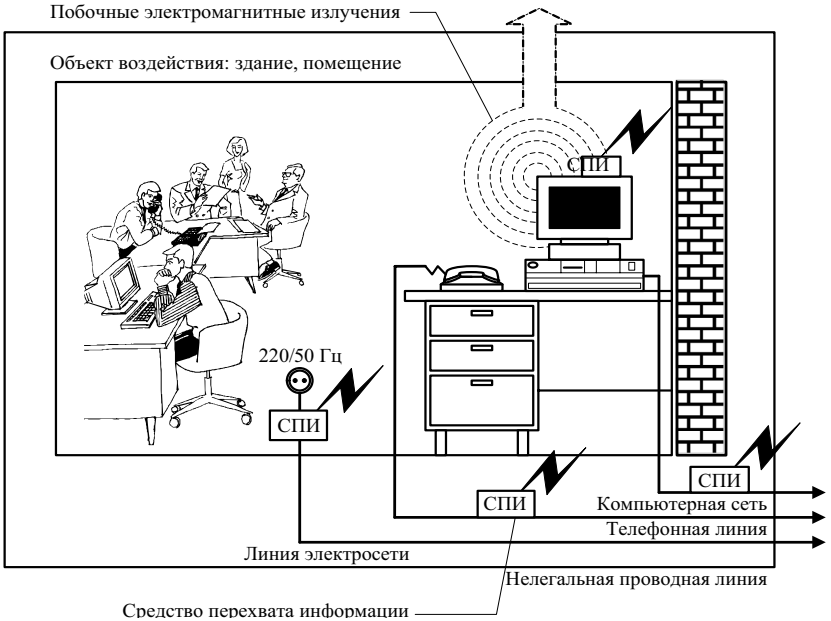


Рис. 3.5. Возможные схемы утечки информации, обрабатываемой техническими средствами приема и передачи информации, а также передаваемой по каналам связи

Как можно заметить из приведенного рисунка, побочные электромагнитные излучения и наводки (ПЭМИН) технических средств приема и передачи информации могут распространяться за пределы контролируемой зоны, что делает возможным их перехват злоумышленником с помощью средств радио-, радиотехнической разведки. Согласно оценочным данным, по каналу ПЭМИН может быть перехвачено не более 1-2 процентов данных, обрабатываемых на персональных компьютерах и других технических средствах приема и передачи информации[1]. Однако, следует помнить, что в настоящее время значительная часть важной информации, содержащей государственную или служебную тайну, обрабатывается на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата — это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе.

[1] Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: ООО «Издательство Машиностроение», 2009. С. 41.

Для съема информации, обрабатываемой в средствах компьютерной техники, в эти средства могут быть установлены специальные электронные устройства перехвата информации — аппаратные закладки, которые представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала накапливается на специальном запоминающем устройстве, а уже затем по сигналу извне передается на запросивший ее объект

Также перехват информации, обрабатываемой техническими средствами приема и передачи информации, возможен путем подключения к соединительным линиям вспомогательных технических средств и систем и посторонним проводникам, проходящим через помещения, где установлены технические средства приема и передачи информации, к их системам электропитания и заземления. Для этого используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Перехват информации, передаваемой по линям связи, может быть осуществлен путем подключения аппаратуры разведки, например, к телефонной линии или кабельной системе компьютерной сети.

Технические каналы утечки речевой информации. Общение между людьми — это процесс коммуникативного взаимодействия его участников, в ходе которого между ними происходит обмен акустической (речевой) информацией.

С точки зрения физики носителями речевой информации являются акустические сигналы, которые представляют собой возмущение упругой среды (воздуха), проявляющееся в возникновении и распространении акустических колебаний различной формы и длительности.

Источником акустического сигнала являются механические колебательные системы, в том числе и органы речи человека. В том случае, если источником акустического сигнала является человеческая речь, то такой сигнал называют речевым. Кроме того, в качестве источника акустического (речевого) сигнала могут выступать и различного типа преобразователи, в том числе и электроакустические. К последним относятся микрофоны, телефоны, громкоговорители и другие устройства, предназначенные для преобразования акустических сигналов в электрические и обратно.

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200-300 Гц до 4-6 КГц.

Восприятие речевых сигналов человеком осуществляется с помощью органов слуха. Однако эти сигналы способны вызвать звуковые ощущения, если частоты соответствующих им колебаний лежат в пределах от 16 Гц до 20 кГц.

Средой распространения речевых сигналов могут являться газовые (воздушные) и твердые среды.

В зависимости от физической природы возникновения речевых сигналов, среды их распространения и способов перехвата технические каналы утечки речевой информации можно разделить на *акустические, виброакустические, акустоэлектрические, параметрические, и оптико-электронный*[1].

[1] См.: Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: ООО «Издательство Машиностроение», 2009; Хорев А. А.

Акустические каналы утечки речевой информации. При ведении разговора органы речи человека порождают акустические колебания, которые, как уже отмечалось, могут распространяться в различных средах. Средой распространения речевого сигнала в акустических каналах утечки речевой информации является воздух. Речевой сигнал, достигая органов слуха человека, возбуждает колебания давления, которые воздействуют на его слуховой аппарат. Роль слухового аппарата человека в акустических каналах утечки речевой информации выполняют микрофоны, которые воспринимают распространяющийся в воздухе речевой сигнал и преобразуют его в электрический.

Для перехвата информации по данному каналу используются *направленные микрофоны и миниатюрные высокочувствительные микрофоны*. Последние используются в качестве чувствительного элемента *в портативных диктофонах и акустических закладочных устройствах*[1] (*акустических закладках*) — устройствах, в которых микрофон конструктивно объединен с миниатюрным передатчиком[2].

Диктофоны представляет собой устройства для записи, или для записи и воспроизведения устной речи с целью ее последующего прослушивания. Они являются одними из самых популярных средств перехвата акустической (речевой) информации, поскольку использование портативных диктофонов не связано с необходимостью проникновения на контролируемый объект. Кроме того, популярность диктофонов для несанкционированной регистрации акустической (речевой) информации обусловлена и тем, что они могут быть приобретены на абсолютно законном основании — для этого не надо являться субъектом оперативно-розыскной деятельности.

Для негласного ведения звукозаписи используются, как правило, портативные диктофоны, отвечающие следующим требованиям:

– минимальные размеры и бесшумность работы;

– продолжительность непрерывной записи — не менее нескольких часов;

– наличие функции управления голосом;

– возможность записи от встроенного или внешнего микрофона;

– качество записи, которое должно обеспечивать узнаваемость голосов и разборчивость речи, записанной как с близкого, так и с дальнего (до 10-15 м) расстояния.

Технические средства и способы промышленного шпионажа. — М.: ЗАО «Дальснаб», 1997. С. 18; Хорев А.А. Технические каналы утечки акустической (речевой) информации [Электронный ресурс]. — Режим доступа: http://www.bnti.ru/showart.asp?aid=957&lvl=04.02. — Загл. с экрана.

[1] Закладочное устройство — техническое средство, скрытно устанавливаемое на объекте информатизации или в контролируемой зоне с целью перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы (Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации»).

[2] Бузов Г. Современные типы закладочных устройств и методы борьбы с ними// Information Security/ Информационная безопасность. 2014. № 3 [Электронный ресурс]. — Режим доступа: http://www.itsec.ru/articles2/Oborandteh/sovremennye-tipy-zakladochnyh-ustroystv-i-metody-borby-s-nimi. — Загл. с экрана.

Тактические особенности использования портативных диктофонов для скрытного ведения звукозаписи в основном зависят от:

– типа используемого микрофона (встроенный или внешний);

– наличия камуфляжа.

Направленные микрофоны применяются в том случае, когда отсутствует возможность проникновения на контролируемый объект или если конфиденциальный разговор происходит вне помещения (например, на улице или на открытой местности). Такие микрофоны воспринимают и усиливают акустический сигнал, идущий только из одного направления (от источника акустического сигнала), и ослабляют посторонние звуки. Конструктивно направленные микрофоны состоят из двух основных элементов: чувствительного элемента — собственно микрофона, и механической системы (акустической антенны), обеспечивающей направленные свойства комплекса.

Акустические закладки представляют собой миниатюрные устройства, конструктивно объединяющие чувствительный элемент и передатчик. При перехвате акустической информации, распространяющейся в воздушных и водных средах, используются акустические закладки микрофонного типа. Чувствительным элементом в этих устройствах являются миниатюрные микрофоны, которые преобразуют перехватываемый акустический сигнал в электрический[1].

Перехваченный таким образом акустический сигнал может передаваться по одному из возможных каналов передачи информации: радиоканалу, оптическому каналу в инфракрасном диапазоне волн, токоведущим линиям, трубам, элементам конструкций и т.д. Наиболее часто для этих целей используется радиоканал. Акустическое закладочное устройство микрофонного типа с передачей перехваченной информации по радиоканалу называется *радиозакладкой*.

Конструктивно простейшее радиозакладочное устройство состоит из трех основных узлов, определяющих технические возможности и методы его использования: микрофона, радиопередатчика и источника питания. Устройство управления не является обязательным элементом радиозакладного устройства. Оно предназначено для расширения его возможностей: включения-выключения передатчика, микрофона, переключения режимов и др.[2]

Радиозакладочные устройства могут исполняться как в некамуфлированном, так и камуфлированном исполнении. Для установки некамуфлированных радиозакладных устройств необходимо несанкционированное проникновение в контролируемое помещение, что не всегда возможно. К тому же вероятность обнаружения таких устройств при тщательном визуальном осмотре помещения достаточно высока, поэтому на практике чаще используются камуфлированные радиозакладочные устройства. Причем камуфляж может быть самый разнообразный: зажигалка, часы, калькулятор, сотовый телефон, авторучка и т.п.

---

[1] Хорев А.А. Аналоговые акустические радиозакладки//Спецтехника и связь. 2010. № 1. С. 20-27.

[2] См.: Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 1: Технические методы и средства: монография. - Изд. 2-е доп. и перераб. / под ред. д-ра юрид. наук, проф. В.М. Мешкова. Калининград: Калининградский ЮИ МВД России, 2003.

а

б

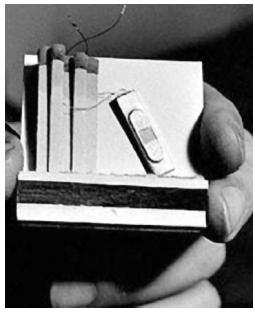


Рис. 3.6. Устройства перехвата информации по акустическому каналу: а) направленный микрофон; б) радиозакладка, закамуфлированная под коробок спичек

Сигналы, поступающие с технических средств перехвата акустической информации, или непосредственно записываются на специальные портативные устройства звукозаписи, или передаются с использованием специальных передатчиков в пункт приема, где осуществляется их запись.

Виброакустические каналы утечки речевой информации. Речевой сигнал, распространяясь в воздухе, может встречать на своем пути различные твердые тела — конструкции зданий и сооружений (стены, потолок, батареи отопления, оконные стекла и т.д.). Сталкиваясь с преградой, речевой сигнал частично отражается и поглощается. Вместе с тем при воздействии сигнала на поверхность твердых тел в последних возникают механические колебания — вибрации, регистрируя которые можно осуществлять перехват акустической (речевой) информации. Для этого используются специальные устройства — электронные стетоскопы, которые преобразуют акустические колебания в твердых телах в электрические сигналы.

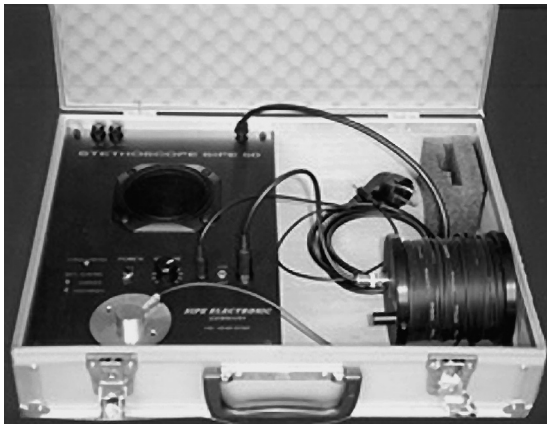


Рис. 3.7. Электронный стетоскоп

Чувствительным элементом электронных стетоскопов является контактный микрофон, соединенный с усилителем. Стетоскоп представляет собой вибродатчик, усилитель и головные телефоны. С помощью подобных устройств можно осуществлять прослушивание разговоров через стены толщиной до 1 м. Стетоскоп может оснащаться проводным, радио или другим каналом передачи информации. Достоинством стетоскопа является трудность его обнаружения при установке в соседних помещениях.

Электронные стетоскопы применяются в том случае, если имеется возможность беспрепятственного проникновения в смежное с контролируемым помещение. В том случае, если возможность беспрепятственного проникновения в смежное помещение отсутствует, вибродатчик оснащается средствами передачи перехваченного акустического сигнала по проводным, радио- и другим возможным каналам передачи информации. На практике для этих целей обычно используется радиоканал, а вибродатчик, оснащенный средствами передачи акустического сигнала по радиоканалу, называется *радиостетоскопом*.

В общем виде схема утечки речевой информации по акустическому и виброакустическому каналам может быть представлена так, как это показано на рис. 3.8.

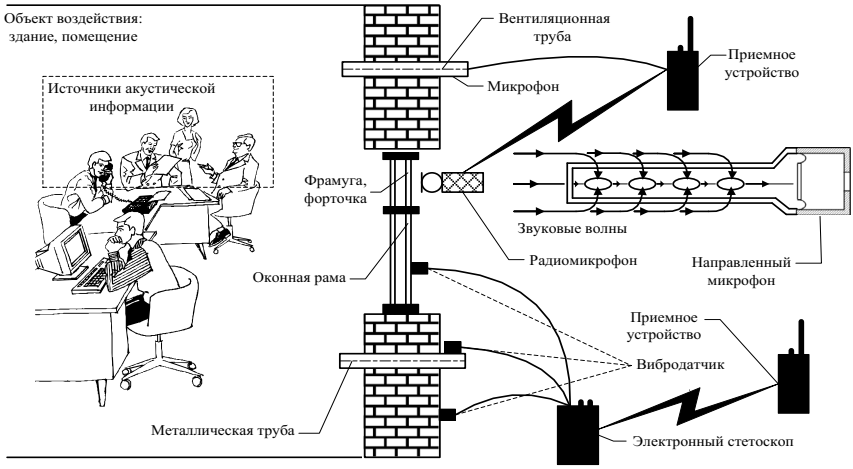


Рис. 3.8. Схема утечки речевой информации по акустическому и виброакустическому каналам

Как следует из представленного рисунка, перехват речевой информации (ведущихся в помещении разговоров) может быть осуществлен, например, с помощью микрофона, установленного в вентиляционной трубе, выходящей за пределы помещения. Передача перехваченного сигнала на приемное устройство может вестись по проводным линиям связи. В случае, если у расположенного в помещении окна открыта фрамуга, форточка, или приоткрыто само окно, перехват речевой информации может быть осуществлен с помощью радиомикрофона, установленного в непосредственной близости от окна. В этом

случае также возможно использование и направленного микрофона. Использование же электронного стетоскопа (радиостетоскопа) позволит злоумышленнику осуществить перехват ведущихся в помещении разговоров без проникновения в само помещение. Вибродатчики могут быть установлены на внешней стороне стены помещения, на поверхности какой-либо металлической конструкции, выходящей за пределы помещения (например, трубы отопления), а также прикреплены к поверхности стекла в окне с внешней стороны.

Акустоэлектрические каналы утечки речевой информации. Перехват информации в данных каналах утечки информации осуществляется путем использования устройств, реализующих принцип *высокочастотного навязывания*.

Под высокочастотным навязыванием (ВЧ-навязыванием) понимают способ несанкционированного получения речевой информации, основанный на зондировании мощным ВЧ-сигналом заданной области пространства. Он заключается в модуляции электромагнитного зондирующего сигнала речевым в результате их одновременного воздействия на элементы обстановки или специально внедренные устройства[1]. В случае использования ВЧ-навязывания в качестве подслушивающего устройства может выступать, например, телефонный аппарат.

Прослушивание помещения через телефон можно осуществить, используя «микрофонный эффект», основанный на том, что детали и узлы телефона (в частности, его вызывная цепь) могут работать как микрофон и наводить в линию достаточно сильный сигнал, который после его усиления пригоден для записи и прослушивания.

Следует отметить, что «микрофонным эффектом» обладают довольно старые модели телефонных аппаратов, которых еще немало в органах внутренних дел. Однако необходимо иметь в виду, что в настоящее время встречаются дешевые электронные аппараты (китайского, тайваньского и другого происхождения), которые могут включаться на передачу (то есть для прослушивания помещения) при определенной нагрузке линии.

Перехват акустической информации по акустоэлектрическому каналу также может осуществляться путем использования пассивных закладочных устройств. Они интересны тем, что в них нет ни источника питания, ни передатчика, ни собственно микрофона, и эти устройства не могут быть обнаружены, при отсутствии внешнего облучения, известными средствами поиска радиозакладочных устройств.

Параметрические каналы утечки речевой информации. Использование в практике деятельности органов внутренних дел современных технических средств обработки информации, наряду с той несомненной пользой, которую они приносят для решения стоящих перед органами внутренних дел задач, обуславливает и возможность несанкционированной утечки информации, основанной именно на применении таких технических средств в практической деятельности сотрудников ОВД.

---

[1] См.: Энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко / под общ. ред. Е.В. Куренкова. СПб: ООО «Издательство Полигон», 1999. С. 20; Хорев А.А. Технические средства и способы промышленного шпионажа. М.: ЗАО «Дальснаб», 1997. С. 88.

Идея в данном случае довольно проста. Суть ее заключается в том, что электронные устройства, установленные в помещениях, в процессе работы создают в окружающем пространстве высокочастотные излучения, параметры которых могут меняться в случае воздействия на них какого-либо акустического сигнала, например, ведущимся в помещении разговором (поэтому этот канал утечки информации и называется параметрическим), то есть их модуляции информационным сигналом. Промодулированные таким образом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и декодированы с помощью специального оборудования.

Следует отметить, что дальность перехвата подобных сигналов, как правило, невелика, но иногда может превышать 100 метров.

Еще одним способом перехвата акустической информации по параметрическому каналу является использование полуактивных закладных устройств (или аудиотранспондеров). Работать аудиотранспондер начинает только при облучении его мощным высокочастотным зондирующим сигналом, который активизирует устройство. Этот сигнал выделяется приемником аудиотранспондера и модулируется сигналом, поступающим либо непосредственно с микрофона, либо с микрофонного усилителя полуактивного закладного устройства. После чего промодулированный высокочастотный сигнал переизлучается, при этом его частота смещается относительно несущей частоты зондирующего сигнала.

Здесь нельзя не привести одну историю, относящуюся к «классике» разведывательной деятельности. *В 1945 году американскому послу в Москве Аверелу Гарриману пионерами «Артека» был подарен деревянный герб Соединенных Штатов из ценных пород дерева. Растроганный посол повесил подарок детишек у себя в кабинете. И лишь через восемь лет американцы узнали, что в гербе было установлено подслушивающее устройство. В гербе находился полый металлический цилиндр без источников питания, торец которого был закрыт тонкой металлической мембраной. Под клювом орла было просверлено отверстие, позволявшее звуковым волнам достигать мембраны. Из соседнего здания в сторону этого подслушивающего устройства, установленного в гербе, направлялось излучение высокой частоты. Звуковые волны, сопровождавшие разговоры в кабинете американского посла, вызывали колебания мембраны, закрывающей металлический цилиндр. В результате изменялась электрическая емкость между этой мембраной и специальным настроечным винтом. Эти изменения приводили к модуляции отраженного излучения указанным звуковым сигналом. В приемном пункте этот сигнал принимался и обрабатывался. Устройство оказалось настолько чувствительным, что была прекрасно слышна не только речь, но и звуки поворота ключа в дверном замке*[1].

Оптико-электронный канал утечки речевой информации. Для перехвата акустической (речевой) информации по данному каналу используются лазер-

[1] Догополов Н. Восемь лет подарок из «Артека» снимал информацию из кабинета посла США//Российская газета — Неделя №6239 (263) [Электронный ресурс]. — Режим доступа: https://rg.ru/2013/11/21/posolstvo.html. — Загл. с экрана.

ные системы акустической разведки (ЛСАР), которые иногда еще называются «лазерными микрофонами».

Принцип действия таких систем заключается в следующем: при ведении разговора распространяющийся в воздухе акустический (речевой) сигнал воздействует на различные тонкие отражающие поверхности (оконные стекла, зеркала и тому подобное), заставляя их вибрировать с частотой, равной частоте акустического сигнала, создавая, таким образом, как бы фонограмму ведущегося разговора. Лазерным передатчиком, входящим в состав ЛСАР, генерируется излучение — лазерный луч, который, достигая оконного стекла, отражается от его поверхности и моделируется воздействующим на стекло акустическим сигналом. Отраженный луч затем воспринимается специальным фотоприемником, который демодулирует его и восстанавливает исходный акустический сигнал.

В общем виде схема утечки информации по оптико-электронному каналу может быть представлена так, как это показано на рис. 3.9.

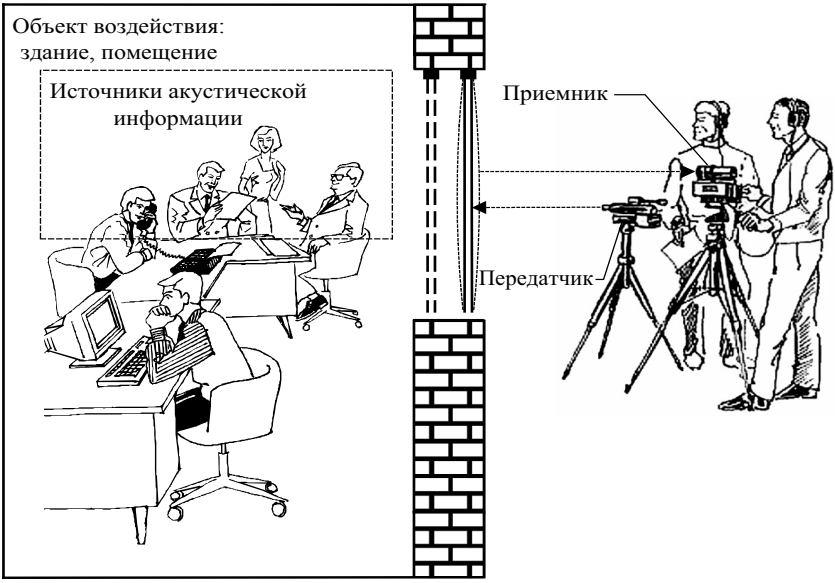


Рис. 3.9. Схема утечки информации по оптико-электронному каналу

Несмотря на несомненные достоинства данного класса оборудования для перехвата акустической (речевой) информации, широкое их использование на практике ограничивается рядом факторов. Прежде всего, это высокая стоимость подобных систем — несколько десятков тысяч долларов. Очевидно, что такие затраты по плечу лишь очень немногим субъектам, занимающимся незаконным сбором конфиденциальной информации. Кроме того, для практического применения ЛСАР необходимы специалисты

высокого уровня, обладающие не только практическими навыками обращения с подобными системами, но и владеющие тактикой их применения в различных условиях.

Технические каналы утечки видовой информации. Наряду с конфиденциальной информацией, обрабатываемой техническими средствами приема и передачи информации, и акустической (речевой) информацией, важную роль в деятельности органов внутренних дел играет и видовая информация, получаемая техническими средствами разведки в виде изображений объектов или документов.

В зависимости от характера видовой информации можно выделить два способа ее получения:

– визуальное наблюдение;

– фото- и видеосъемка.

Визуальное наблюдение. В целях получения интересующей информации злоумышленниками может быть организовано наблюдение как собственно за интересующим его объектом — сотрудником органов внутренних дел, так и за квартирой, в которой проживает он или члены его семей, за зданием территориального органа внутренних дел и т.п. Для этого криминальными элементами, в зависимости от условий наблюдения, могут использоваться самые разнообразные технические средства.

Для наблюдения в светлое время суток — различные оптические приборы (монокуляры, бинокли, телескопы и т.п.), телевизионные камеры (системы). *Для наблюдения в ночное время* — приборы ночного видения, телевизионные камеры (системы), тепловизоры.

При этом для наблюдения с большого расстояния, как правило, используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния — камуфлированные, скрытно установленные телевизионные камеры. Причем видеоизображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

Проведение фото- и видеосъемки. Фото- и видеосъемка объектов наблюдения проводится как для документирования результатов наблюдения, так и для дальнейшего, более подробного изучения объекта наблюдения. В этих целях используются различные видеокамеры и фотографические средства.

Для съемки в светлое время суток с большого расстояния используются фотоаппараты и видеокамеры с длиннофокусными объективами, а для съемки с близкого расстояния — портативные камуфлированные фотоаппараты и видеокамеры, сопряженные с устройствами видеозаписи или передачи видеоинформации по радиоканалу.

Съемка объектов ночью проводится, как правило, с близкого расстояния. Для этих целей используются портативные фотоаппараты и видеокамеры, сопряженные с приборами ночного видения, или тепловизоры, а также портативные закамуфлированные видеокамеры высокой чувствительности, сопряженные с устройствами передачи информации по радиоканалу.

Рис. 3.10. Миниатюрные видеокамеры

Наличие рассмотренных каналов утечки информации, в том числе и технических, представляет несомненную опасность для конфиденциальной информации органов внутренних дел и предопределяет необходимость построения эффективной системы инженерно-технической защиты информации, используемой в органах внутренних дел.

3.3. Организационная и инженерно-техническая защита информации органов внутренних дел от утечки

Обеспечение защиты информации от утечки обеспечивается реализацией целого комплекса мер, ключевую роль в котором играют мероприятия организационного и инженерно-технического характера.

Организационные мероприятия — это мероприятия по защите информации, проведение которых не требует применения специально разработанных технических средств защиты. К основным организационным мероприятиям по защите информации от утечки по техническим каналам, проводимым на объектах информатизации, подлежащих защите, можно отнести следующие:

1. Выбор помещения для установки основных и вспомогательных технических средств и систем[1].

2. Использование только сертифицированных технических средств и систем защиты информации.

---

[1] *Основные технические средства и системы (ОТСС)* — технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (АС различного уровня и назначения), средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) — технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

В общем случае под ***сертификацией*** понимается *подтверждение соответствия продукции или услуг установленным требованиям или стандартам*.

В свою очередь, под ***сертификацией средств защиты информации по требованиям безопасности информации*** понимается *деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации*.

Сертификат на средство защиты информации — документ, подтверждающий соответствие средства защиты информ*ации требованиям по безопасности информации.*

Сертификация средств защиты информации, прежде всего, подразумевает проверку их качественных характеристик для реализации основной функции — защиты информации на основании государственных стандартов и требований по безопасности информации. Применительно к сведениям, составляющим государственную тайну, общие принципы организации сертификации средств защиты информации определены нормами статьи 28 Закона «О государственной тайне»: *средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.*

Одним из основных руководящих документов по сертификации средств защиты информации является Положение о сертификации средств защиты информации, утвержденное постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Согласно данному Положению технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации и подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам.

Системы сертификации создаются Федеральной службой по техническому и экспортному контролю (ФСТЭК России), ФСБ России, Министерством обороны Российской Федерации. Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. В каждой системе сертификации разрабатывается и согласовывается с Межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Применительно к органам внутренних дел можно выделить следующие основные системы обязательной сертификации средств защиты информации по требованиям безопасности информации:

РОСС RU.0001.01БИОО: Система сертификации средств защиты информации по требованиям безопасности информации (ФСТЭК России);

РОСС RU.0001.030001: Система сертификации средств криптографической защиты информации (ФСБ России);

РОСС RU.0003.01БИ00: Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (ФСБ России).

Система сертификации средств защиты информации по требованиям безопасности информации (РОСС RU.0001.01БИОО). 27 октября 1995 года приказом Председателя Гостехкомиссии России было введено в действие *Положение о сертификации средств защиты информации по требованиям безопасности информации.* В соответствии с данным положением обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом, подлежащей защите в соответствии с действующим законодательством, систем управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства, средства общего применения, предназначенные для противодействия техническим разведкам, а именно:

– технические средства защиты информации от утечки по техническим каналам, включая средства контроля эффективности принятых мер защиты информации, основные и вспомогательные технические средства и системы в защищенном исполнении;

– средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности;

– средства контроля эффективности применения средств защиты информации;

– защищенные программные средства обработки информации;

– программные средства общего назначения.

В остальных случаях сертификация носит добровольный характер (добровольная сертификация) и осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.

Сертификационные испытания средств защиты в рамках данной системы сертификации предусматривают комплекс мероприятий по проверке соответствия этих средств формальным базовым требованиям по обеспечению безопасности информации, изложенным в нормативных документах Гостехкомиссии России (ныне — ФСТЭК России).

Использование формальных критериев оценки при сертификации позволяет сделать обоснованный вывод о возможности средств защиты выполнять свои функции не только на качественном, но и на количественном уровне. В зависимости от степени соответствия средств защиты совокупности предъявляемых к ним формальных требований может быть сделан вывод о возможности, либо невозможности использования данных средств для защиты информации в зависимости от степени ее конфиденциальности, схемы циркуляции защищаемой информации и других параметров.

В настоящее время ФСТЭК России ведет государственный реестр сертифицированных средств защиты информации. Ознакомится с ним можно на сайте ФСТЭК России по адресу: http://fstec.ru/normotvorcheskaya/sertifikatsiya/153-

sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00.

Система сертификации средств криптографической защиты информации (РОСС RU.0001.030001). Данная система сертификации была зарегистрирована в Госстандарте России 15 ноября 1993 года. Она устанавливает правила сертификации по требованиям безопасности информации:

– шифровальных средств;

– систем и комплексов телекоммуникаций высших органов государственной власти Российской Федерации;

– закрытых систем и комплексов телекоммуникаций[1] органов государственной власти субъектов Российской Федерации, центральных органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности и форм собственности;

– информационно-телекоммуникационных систем и баз данных государственных органов, Центрального банка Российской Федерации, Внешэкономбанка и их учреждений, иных государственных учреждений Российской Федерации.

Первоначально данная система сертификации действовала под управлением Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), однако в дальнейшем, в связи с упразднением ФАПСИ руководство этой системой перешло к ФСБ России.

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (РОСС RU.0003.01БИ00). Приказом ФСБ России от 13 ноября 1999 г. № 564 утверждены Положения о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия. В соответствии с утвержденным данным приказом Положением о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, обязательному сертифицированию подлежат:

– технические средства защиты информации, включая средства контроля эффективности принятых мер защиты информации;

– технические средства и системы в защищенном исполнении;

– технические средства защиты специальных оперативно-технических мероприятий (специальных технических средств, предназначенных для негласного получения информации);

– технические средства защиты информации от несанкционированного доступа (НСД);

– программные средства защиты информации от НСД и программных закладок;

– защищенные программные средства обработки информации;

– программно-технические средства защиты информации;

---

[1] К закрытым системам и комплексам телекоммуникаций относятся системы и комплексы телекоммуникаций, в которых обеспечивается защита информации с использованием шифровальных средств, защищенного оборудования и организационных мер.

– специальные средства защиты от идентификации личности;

– программно-аппаратные средства защиты от несанкционированного доступа к системам оперативно-розыскных мероприятий (СОРМ) на линиях связи.

С перечнем средств защиты информации, сертифицированных ФСБ России, можно ознакомится на сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (ЦЛСЗ ФСБ России) по адресу: http://clsz.fsb.ru.

1. Установление контролируемой зоны вокруг объекта;

2. Режимное ограничение доступа на объекты размещения основных технических средств и систем и в выделенные помещения;

3. Категорирование и аттестация объектов информатизации и выделенных помещений по требованиям безопасности информации в соответствие с нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и других уполномоченных органов.

***Выделенное помещение** — это специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера*[1].

В качестве выделенных помещений целесообразно выбирать помещения, не имеющие общих ограждающих конструкций с помещениями, в которые имеется доступ посторонних лиц. По возможности окна выделенных помещений не должны выходить на места стоянки машин, а также на ближайшие здания, из которых возможно ведение разведки с использованием технических средств. Выделенные помещения должны располагаться в пределах контролируемой зоны.

Контролируемая зона — *это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств*.

Границей контролируемой зоны могут являться периметр охраняемой территории, а также ограждающие конструкции охраняемого здания или охраняемой части здания. В некоторых случаях границей контролируемой зоны могут быть ограждающие конструкции (стены, пол, потолок) выделенных помещений.

В отдельных случаях на период обработки техническими средствами конфиденциальной информации контролируемая зона временно может устанавливаться большей, чем охраняемая территория организации. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

Выделенные помещения во внеслужебное время должны закрываться, опечатываться и сдаваться под охрану. В служебное время доступ сотрудников в эти помещения должен быть ограничен (по спискам) и контролироваться (учет посещаемости). При необходимости данные помещения могут быть оборудованы системами контроля управления доступом.

---

[1] Руководящий Документ ФСТЭК России «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (Утвержден зам. директора ФСТЭК России 18 мая 2007 г.).

Введение категорирования объектов информатизации необходимо для определения объема требований по технической защите информации, необходимых для разработки и внедрения комплекса организационных и технических мер в соответствии с присвоенной категорией.

При присвоении категории объекту информатизации необходимо руководствоваться, прежде всего, ценностью информации, обрабатываемой на данном объекте. Ценность информации определяется через меру ущерба, который может быть нанесен деятельности органов внутренних дел или государству в целом.

Процесс присвоения объекту информатизации категории включает в себя:

– определение высшей степени (грифа) секретности информации, предназначенной для обработки на объекте информатизации;

– определение условий расположения объекта информатизации (только для основных технических средств и систем 1, 2 и 3 категорий) относительно постоянных представительств иностранных государств, обладающих правом экстерриториальности;

– оформление акта категорирования на объект информатизации.

Объектам информатизации могут быть присвоены следующие категории:

– *первая категория* присваивается объектам информатизации, основные технические средства и системы, выделенные помещения которых предназначены для обработки информации, высшая степень секретности которой относится к грифу «особой важности»;

– *вторая категория* присваивается объектам информатизации, основные технические средства и системы, выделенные помещения которых предназначены для обработки информации, высшая степень секретности которой относится к грифу «совершенно секретно»;

– *третья категория* присваивается объектам информатизации, основные технические средства и системы, выделенные помещения которых предназначены для обработки информации, высшая степень секретности которой относится к грифу «секретно»;

– *четвертая категория* присваивается объектам информатизации, которые предназначены для обработки информации, содержащей сведения, составляющие служебную тайну (или конфиденциальную информацию, в первую очередь, персональные данные). Данная категория может быть присвоена объектам информатизации, которые предназначены для обработки информации, содержащей сведения, составляющие иные, отличные от государственной или служебной видов тайн. Доступ к ним и их распространение ограничены в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, ведомственными нормативными актами.

Четвертая категория также может быть присвоена объектам информатизации, которые предназначены для обработки информации, не подлежащей в соответствии с законом ограничению в доступе к ней и (или) ограничению в ее распространении, когда данная информация должна быть защищена от несанкционированного изменения (искажения), уничтожения и блокирования

Ответственность за своевременное и правильное категорирование объекта информатизации несет непосредственно руководитель подразделения, в распоряжении которого находится данный объект.

При вводе основных технических средств и систем, выделенных помещений в эксплуатацию должна периодически проводиться их ***аттестация по требованиям безопасности информации***.

Аттестация объекта информатизации органов внутренних дел по требованиям безопасности информации носит обязательный характер для объектов информатизации, предназначенных для обработки сведений, составляющих государственную тайну, а также для государственных информационных систем.

В настоящее время в ведении МВД России находятся следующие государственные информационные системы[1]:

1. *«Федеральная автоматизированная дактилоскопическая информационная система» (федеральная АДИС-МВД)*. Данная система предназначена для решения следующих задач: формирование и ведение на базе органов внутренних дел информационных дактилоскопических массивов, полученных в процессе проведения государственной дактилоскопической регистрации, и информации о следах рук неустановленных лиц, изъятых с мест преступлений; информационное обеспечение правоохранительных органов при осуществлении функций по предупреждению, пресечению, выявлению, раскрытию и расследованию преступлений, предупреждению и выявлению административных правонарушений, розыску пропавших без вести, установлению по неопознанным трупам личности человека, установлению личности граждан Российской Федерации, иностранных граждан и лиц без гражданства, граждан не способных по состоянию здоровья или возрасту сообщить данные о своей личности; накопление и актуализация дактилоскопических массивов общефедерального уровня; поиск информации по объектам учета системы; выдача информации по объектам учета системы; обеспечение безопасности информационных ресурсов.

2. *Федеральная государственная информационная система: «Система обеспечения предоставления информации МВД России в рамках межведомственного электронного взаимодействия МВД России* (*ВИС-СМЭВ*)*»*. ВИС- СМЭВ — служебная информационная система, предназначенная для организации доступа электронных сервисов МВД России в систему межведомственного электронного взаимодействия.

3. *Федеральная государственная информационная система «Интегрированный банк данных федерального уровня»* (*ИБД-Ф*), предназначенная для: информационного обеспечения деятельности органов внутренних дел Российской Федерации и других федеральных органов государственной власти по выявлению, раскрытию и расследованию преступлений, по установлению местонахождения лиц, объявленных в федеральный и межгосударственный розыск, а также для подтверждения наличия (отсутствия) сведений о суди-

[1] Государственные информационные системы, находящиеся в ведении МВД России [Электронный ресурс]. — Режим доступа: https://мвд.рф/Deljatelnost/gosprogram/gis. — Загл. с экрана.

мости, реабилитации, времени и месте отбывания наказания. Данная система обеспечивает формирование, ведение централизованных оперативно-справочных, криминалистических, розыскных и иных учетов органов внутренних дел с использованием интегрированных банков данных на федеральном уровне.

Ответственность за организацию обеспечения защиты информации ограниченного доступа на объектах информатизации, в том числе и за проведение их аттестации, возлагается на руководителей подразделений системы МВД и их структурных подразделений, эксплуатирующих объекты, что отражается в их должностных регламентах.

Важно подчеркнуть, что отсутствие аттестованного по требованиям безопасности информации объекта информатизации или срок действия аттестата которого истек, приводит к отказу в выдаче лицензии ФСБ России на право обработки информации, составляющей государственную тайну, что делает невозможным осуществление оперативно-служебной деятельности всего подразделения. Кроме того, в случае невыполнения данных требований руководитель территориального органа МВД России (в соответствии с положением о территориальном органе МВД России), а также лица, непосредственно занимающиеся обработкой информации, могут быть привлечены к гражданской, административной или уголовной ответственности.

Нормативно-правовой основой проведения аттестации является **Положение по аттестации объектов информатизации по требованиям безопасности информации** (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.)[1].

В соответствии с данным Положением под ***аттестацией объектов информатизации*** понимается *комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации*. Только лишь наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленный в «Аттестате соответствия».

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации. Основная цель ее проведения — подтверждение соответствия комплекса используемых на конкретном объекте информатизации мер и средств защиты информации от несанкционированного доступа требуемому уровню безопасности информации, в том числе по ее защите:

– от компьютерных вирусов;

– от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект;

---

[1] Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g. — Загл. с экрана.

– от утечки информации или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация проводится в соответствии со схемой, выбираемой на этапе подготовки к аттестации из следующего основного перечня работ:

– анализ исходных данных по аттестуемому объекту информатизации;

– предварительное ознакомление с аттестуемым объектом информатизации;

– проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

– проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

– проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

– проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Аттестация объектов информатизации, предназначенных для обработки сведений, составляющую государственную тайну, проводится организациями, имеющими аттестат аккредитации органа по аттестации и соответствующие лицензии ФСТЭК России на осуществление мероприятий и оказание услуг в области защиты государственной тайны (в части технической защиты информации).

Аттестация объектов информатизации, предназначенных для обработки сведений конфиденциального характера, проводится организациями, имеющими лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

В системе МВД России аттестация объектов информатизации проводится, как правило, ведомственными органами по аттестации.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

1. *Подача и рассмотрение заявки на аттестацию*. Заявитель заблаговременно направляет в орган по аттестации заявку на ее проведение, в которой указывает исходные данные по аттестуемому объекту информатизации. Форма заявки установлена упомянутым ранее «Положением по аттестации объектов информатизации по требованиям безопасности информации».

Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

2. *Предварительное ознакомление с аттестуемым объектом*. Если в поданной заявке указано недостаточно исходных данных по аттестуемому объ-

екту информатизации, в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до начала аттестационных испытаний.

3. *Испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте информатизации*. Если на аттестуемом объекте используются несертифицированные средства и системы защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

4. *Разработка программы и методики аттестационных испытаний*. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом, органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяется состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или привлечения испытательных центров (лабораторий). Программа аттестационных испытаний согласовывается с заявителем.

5. *Заключение договоров на аттестацию.* На данном этапе заключается договор между заявителем и органом по аттестации на проведение аттестации. Также осуществляется заключение договоров органа по аттестации с привлекаемыми экспертами, оформляется предписание о допуске аттестационной комиссии к проведению аттестации.

6. *Проведение аттестационных испытаний объекта информатизации*. В ходе аттестационных испытаний выполняется следующее:

– осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

– определяется правильность категорирования объектов электронно-вычислительной техники и классификации автоматизированных систем (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

– проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

– проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

– проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

– оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных наруше-

ний, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

7. *Оформление, регистрация и выдача «Аттестата соответствия»*. «Аттестат соответствия» выдается на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить выявленные недостатки орган по аттестации принимает решение об отказе в выдаче «Аттестата соответствия». При этом может быть предложен срок повторной аттестации при условии устранения недостатков.

8. *Рассмотрение апелляций.* В случае, если заявитель не согласен с отказом в выдаче «Аттестата соответствия», он может подать апелляцию в вышестоящий орган по аттестации или в ФСТЭК. Апелляция рассматривается в срок, не превышающий один месяц с привлечением заинтересованных сторон.

9. *Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации.* Проводится ФСТЭК России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации — периодически в соответствии с планами работы по контролю и надзору.

Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и надзор, может быть приостановлено или аннулировано действие «Аттестата соответствия».

Решение об аннулировании действия «Аттестата соответствия» принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

Инженерно-технические мероприятия по защите информации — *это комплекс организационных и технических мероприятий, направленных на организацию активно-пассивного противодействия средствам технической разведки и формирование рубежей охраны территории, зданий, помещений, оборудования с помощью комплексов технических средств*[1]. Включает в себя:

– сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здания и помещения;

– средства защиты информации от утечки по техническим каналам;

– средства обеспечения охраны территорий, зданий, помещений;

– средства противопожарной охраны;

– технические средства и мероприятия, предотвращающие вынос персоналом из помещений документов, дисков и других носителей информации.

С помощью реализации инженерно-технических мер защиты информации решаются следующие *задачи*:

1) создание физических (механических) препятствий на пути проникновения к носителям информации;

2) выявление попыток проникновения на объект охраны, к местам сосредоточения носителей защищаемой информации;

3) предупреждение о возникновении чрезвычайных ситуаций и их ликвидация;

4) поддержание связи с различными организациями, подразделениями, помещениями и другими объектами охраны;

5) нейтрализация, поглощение или отражение излучения используемых радиотехнических устройств;

6) введение технических разведок в заблуждение (дезинформация) относительно истинного содержания защищаемой информации.

7) комплексная проверка режимных помещений, использующихся каналов связи и средств обработки информации на соответствие требованиям безопасности информации;

8) защита информации в автоматизированных системах обработки данных в целях предотвращения ее несанкционированного копирования, искажения или изменения.

Говоря о содержании системы инженерно-технической защиты информации органов внутренних дел от утечки и умышленного перехвата, следует, прежде всего, отметить, что эта система должна состоять из двух блоков (подсистем) — *подсистемы физической защиты информации и подсистемы защиты информации от утечки*[2] (рис. 3.11).

---

[1] См.: Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005. С. 128.

[2] См.: Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005. С. 529.

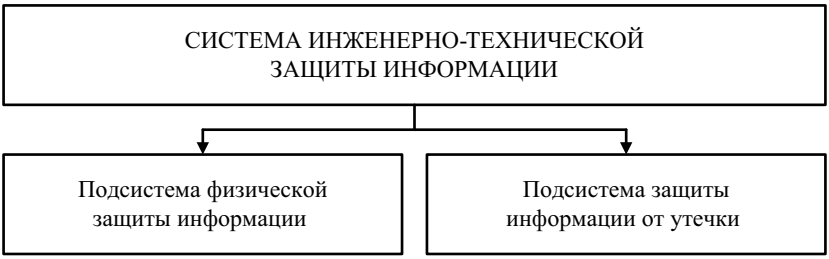


Рис. 3.11. Структура системы инженерно-технической защиты информации

Подсистема физической защиты информации создается для противодействия преднамеренным угрозам воздействия злоумышленника и стихийным силам, прежде всего, — пожару. Средства этой подсистемы реализуют методы физической защиты с помощью инженерных конструкций и технических средств охраны.

В общем случае подсистема физической защиты информации включает в себя комплекс инженерной защиты информации и комплекс технической охраны объекта защиты.

Инженерная защита информации в органах внутренних дел обеспечивается созданием различного рода преград на возможных путях движения злоумышленников и распространения стихийных явлений к источникам защищаемой информации. К числу таких преград относятся: заборы, стены, окна и двери зданий, помещений и т.д.

Объекты и помещения, в которых осуществляется хранение защищаемой информации, должны иметь капитальные (по охране) наружные и внутренние стены.

Капитальными (по охране) наружными стенами следует считать такие, которые выполнены из следующих материалов[1]:

Материал	**Толщина, мм**
Кирпичная кладка	500
Бетонные блоки	200
Железобетонные панели	180

Капитальными (по охране) внутренними стенами следует считать такие, которые выполнены аналогично капитальным наружным стенам, либо[2]:

[1] См.: Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 2: Организационно-правовые методы и средства: монография / под ред. проф. В.М. Мешкова. Калининград: Калининградский ЮИ МВД России, 2003. С. 145.

[2] Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 2: Организационно-правовые методы и средства: монография / под ред. проф. В.М. Мешкова. Калининград: Калининградский ЮИ МВД России, 2003. С. 152.

Материал	Толщина, мм
Спаренные гипсобетонные панели с проложенной между ними металлической решеткой из арматуры	80 (каждая)
Кирпичная кладка, армированная металлической решеткой	120

Наружные стены, не отвечающие указанным требованиям, с внутренней стороны по всей площади должны быть укреплены металлическими решетками из арматуры, которые затем оштукатуриваются. Решетки привариваются к прочно заделанным в стену стальным анкерам.

Очень часто злоумышленники проникают на объект через дверь. В этой связи двери должны быть такими прочными, чтобы оказывать достаточное сопротивление при физическом воздействии человека, а также при попытке открыть их при помощи простых инструментов, например, лома, топора, молотка, долота или отвертки.

Входные двери должны отвечать следующим требованиям:

– быть исправными;

– быть полнотелыми;

– полотно двери должно плотно прилегать к дверной коробке;

– толщина дверного полотна — не менее 40 мм;

– иметь не менее двух врезных несамозащелкивающихся замков.

Серьезным препятствием при попытках проникновения в помещение является *стальная дверь*. При использовании декоративных покрытий такие двери по внешнему виду могут не отличаться от пластмассовых или деревянных. При выборе двери необходимо проверить жесткую фиксацию элементов затвора при закрытом замке.

Окна, витрины, фрамуги и форточки во всех помещениях охраняемого объекта должны быть остеклены и иметь надежные, исправные запоры. Наиболее пристальное внимание необходимо уделять защите легко достигаемых окон, расположенных:

– на небольшой высоте с плохо просматриваемой стороны здания;

– в непосредственной близости от пожарных лестниц;

– в неосвещенных местах.

Для защиты окон используют каркасные и бескаркасные решетки. Есть и другой, не менее эффективный способ защиты остекленных проемов — *применение светопрозрачных защитных пленок*. Это многофункциональные полимерные пленки, которые наносятся на обыкновенное стекло. Пленочное покрытие превращает стекло в материал с принципиально иными качественными характеристиками, повышающими возможности защиты от утечки информации и несанкционированного доступа к ней.

Последние рубежи защиты создают металлические шкафы и сейфы, в связи с чем к их механической прочности предъявляются повышенные требования.

Металлические шкафы предназначены для хранения документов с невысоким грифом конфиденциальности. Их надежность определяется только прочностью металла и секретностью замков.

Для хранения особо ценных документов применяются сейфы, которые делятся на три группы: взломостойкие, огнестойкие и огневзломостойкие.

В настоящее время в России действует Национальный стандарт Российской Федерации ГОСТ Р50862-2012 «Сейфы, сейфовые комнаты и хранилища ценностей» (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2012 г. № 1031-ст), регламентирующий качественные показатели сейфов, их классификацию и методы испытаний. Данный ГОСТ предусматривает десять классов устойчивости сейфов к взлому и шесть классов огнеустойчивости.

К средствам инженерной защиты информации в органах внутренних дел относятся и различного рода преграждающие устройства систем контроля и управления доступом: вращающиеся двери, раздвижные и вращающиеся трех- или четырехштанговые турникеты и т.п.

Для обнаружения попыток преодоления злоумышленником различного рода преград (барьеров), созданных в целях защиты информации, применяются *технические средства охраны объектов*.

К числу таких средств, широко используемых в практической деятельности органов внутренних дел, следует отнести, прежде всего, с*истемы охранной и пожарной сигнализации*, представляющие собой совокупность совместно действующих технических средств для обнаружения признаков появления несанкционированного проникновения человека (нарушителя) на защищаемый объект и (или) пожара на них, передачи, сбора, обработки и предоставления информации в заданном виде пользователю.

Для конкретной системы состав технических средств определяется способом организации охраны, а также потребностями пользователя. В зависимости от вида охраны она может быть организована как автономная или централизованная.

Для *автономной охраны* характерно наличие единого объекта защиты, состоящего из одного или комплекса помещений, расположенных в пределах нескольких зданий, объединенных общей территорией.

Основными устройствами современных систем автономной сигнализации, независимо от выполняемых дополнительных функций или объекта размещения, являются:

– *детекторы*, реагирующие на различные внешние факторы (открытие окна или двери, задымление и т.п.);

– *блок управления* — в нем записаны критические величины внешних раздражителей (уровень, задымления, загазованности) и команды, которые должны выполнить исполнительные устройства в случае превышения этих уровней (дозвон владельцу, в полицию, в МЧС).

– *исполнительные устройства* — обычно тревожные световые и звуковые приспособления (сирены, проблесковые маяки);

– *GSM модуль* — имеется практически во всех современных наборах автономной сигнализации. Устаревшие системы, рассчитанные только на локальную тревогу без последующего информирования владельца о нарушении, малоэффективны и сейчас практически не используются.

Блок управления может быть связан с детекторами по кабелям или по радиоканалу.

Централизованная охрана организуется для большого количества объектов, пространственно разнесенных на значительной территории. Тогда дополнительно необходимо наличие подсистемы передачи извещений. На практике все сигналы тревоги передаются на центральный пульт охраны для незамедлительного реагирования. Передача информации может происходить по радиоканалу, каналу GSM, телефонной линии. Все линии передачи информации могут совмещаться при построении одного защитного комплекса.

Подсистема защиты информации от утечки предназначена для снижения риска несанкционированного распространения информации от ее источника, расположенного внутри контролируемой зоны, к злоумышленнику. Достижение этой цели осуществляется путем применения различных сил и средств обнаружения и нейтрализации угроз подслушивания, наблюдения, перехвата и утечки информации по различным каналам, прежде всего, техническим.

Рассмотрим возможное содержание подсистемы защиты информации от утечки на примере такого типового объекта, как служебный кабинет сотрудника органов внутренних дел.

Исключительные особенности правоохранительной деятельности со всей очевидностью ставят вопрос об организации рабочего места сотрудника органов внутренних дел и, прежде всего, следователя (дознавателя), поскольку именно от качества предварительного расследования в значительной степени зависит эффективность предпринимаемых государством усилий по противодействию современной преступности.

Как представляется, в обобщенном виде схему возможной утечки информации из рабочего кабинета сотрудника органов внутренних дел можно представить так, как это показано на рис. 3.12. Каждый из возможных способов перехвата информации предопределяет необходимость применения своих методов и средств защиты информации, обобщенный анализ которых позволяет выдвинуть следующие основные рекомендации по организации и оборудованию рабочего места сотрудника органов внутренних дел по требованиям защиты информации[1].

1. Необходимым условием практической реализации некоторых из рассмотренных ранее технических каналов утечки информации является наличие прямой видимости источника информации. Это относится, прежде всего, к использованию направленных микрофонов и лазерных систем разведки для перехвата речевой информации. Блокирование данных каналов утечки ин-

[1] См. также: Ишин А.М., Григорьев А.Н. Информация и расследование преступлений (технические меры обеспечения информационной защищенности деятельности по раскрытию и расследованию преступлений): научно-практическое пособие. Калининград: КЮИ МВД России, 2002; Григорьев А.Н. Организация технической защиты криминалистически значимой информации при производстве предварительного расследования // Вестник криминалистики / отв. ред. А.Г. Филиппов. Вып. 3(11). М.: Спарк, 2004. С. 49–55; Паршина Е.Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании преступлений: дисс. … канд. юрид. наук. Ижевск, 2004. С. 179–187.

1. Перехват акустической (речевой) информации с помощью закладных устройств, скрытно установленных в предметах мебели, бытовой техники и т.п.
2. Перехват акустической (речевой) информации с помощью прятативных диктофонов а) закамуфлированных под какие-либо предметы, например, ежедневник и т.п.; б) скрытно установленных, например, в предметы мебели и т.п.; в) находящихся у посетителей
3. Перехват акустической информации через открытые окна с помощью направленных микрофонов
4. Перехват акустической информации с помощью контактных микрофонов (стетоскопов)
5. Перехват а) акустической информации через телефонный аппарат за счет наводок и навязывания, или использования устройств типа «телефонное ухо»; б) информации, передаваемой по проводным линиям связи путем контактного подключения к ним
6. Перехват информации, передаваемой по каналам радио-, радиорелейной связи (пейджинговая, сотовая связь)

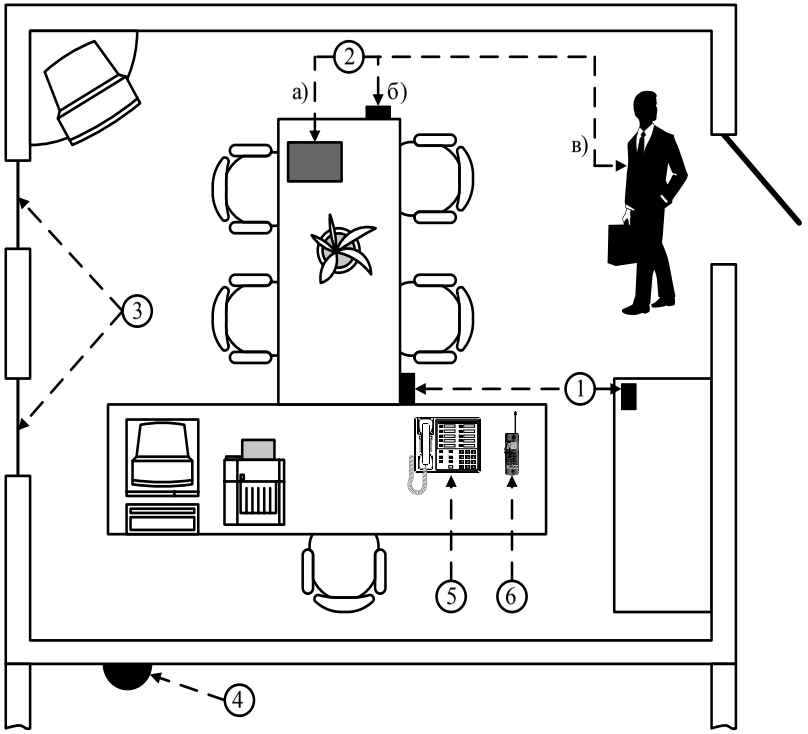


Рис. 3.12. Схема возможной утечки информации из рабочего кабинета сотрудника органов внутренних дел

формации возможно и без привлечения специальных технических средств, достаточно выбрать правильное месторасположение служебного кабинета: необходимо, чтобы его окна выходили во внутренний двор.

2. Для того, чтобы существенно снизить риск утечки информации по виброакустическому каналу, следует исключить расположение служебного кабинета в угловых помещениях. Также недопустимо располагать служебный кабинет в помещениях, являющихся смежными с помещениями других организаций.

3. В кабинете целесообразно установить пластиковые окна с трех или пятикамерными стеклопакетами с рельефным стеклом. Окна также должны быть оборудованы жалюзи. При проведении в кабинете мероприятий, требующих повышенного уровня секретности, окна кабинета должны быть закрыты, а жалюзи — опущены. Это позволит исключить возможность перехвата информации по оптико-электронному каналу, а также предотвратит утечку видовой информации.

4. В целях защиты от подслушивания в кабинете должна быть обеспечена хорошая звукоизоляция в местах возможного перехвата информации. Для этого представляется целесообразным оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов.

5. Для защиты акустической информации от ее перехвата по акустическому и виброакустическому каналам с помощью закладочных устройств следует оборудовать кабинет *системами виброакустического зашумления*.

Принцип работы подобного рода систем достаточно прост. Они излучают шумоподобные сигналы речевого диапазона частот, снижая тем самым уровень разборчивости речи до необходимых значений. Даже если речевая информация и будет перехвачена злоумышленником, то отделить информацию от помех будет практически невозможно.

Система виброакустического зашумления состоит из *генератора шума*, который отправляет сгенерированный сигнал на *виброизлучатели* (как правило, крепятся в элементах строительных конструкций помещения) и *акустоизлучатели* (могут размещаться над навесными потолками, в дверных тамбурах, в самом помещении и т.д.).

Наиболее широкое распространение получили генераторы «*белого*» шума, обеспечивающие генерацию сигнала с равномерно распределенным спектром, подобно шуму бегущей воды. Однако наиболее эффективным считается использование генераторов *адаптивного шума*. Суть работы подобного рода устройств заключается в анализе акустической обстановки в помещении и автоматическом определении необходимого уровня шума в той или иной полосе речевого диапазона. Это позволяет генератору увеличить интенсивность шума с частотой голосов собеседников и уменьшить интенсивность остальных помех. Такая технология позволяет поддерживать оптимальное соотношение шум/полезный сигнал и уменьшить, таким образом, отрицательные моменты работы людей в защищаемом помещении.

В качестве примера подобного рода устройств можно привести систему виброакустической и акустической защиты «Соната-АВ» (ЗАО «Анна»)

модель 3М, предназначенную для активной защиты речевой информации в выделенных (защищаемых) помещениях от утечки по акустическим и виброакустическим каналам[1].

Рис. 3.13. Генераторный блок системы «Сонат

Данное устройство позволяет эффективно блокировать следующие каналы утечки акустической речевой информации: непреднамеренное подслушивание из-за недостаточной звукоизоляции помещения, за счет применения радио- и проводных микрофонов, за счет применения направленных микрофонных систем, за счет применения контактных микрофонов (стетоскопов, радиостетоскопов).

Важно отметить, что «Соната-АВ» модель 3М имеет сертификат ФСТЭК, удостоверяющий, что данная система является техническим средством защиты акустической речевой информации, обрабатываемой в выделенных помещениях до 1 категории включительно, от утечки по акустическому и виброакустическому каналам путем постановки помех в диапазоне частот 90 . . . 11200 Гц, не создает технических каналов утечки информации и может устанавливаться в выделенных помещениях до 1 категории включительно без применения дополнительных мер защиты.

6. Для предотвращения утечки информации, обусловленной побочными электромагнитными излучениями и наводками компьютера и других средств обработки информации, могут быть использованы шумогенераторы, которые осуществляют формирование и излучение в непосредственной близости от защищаемого средства электронной техники широкополосного шумового сигнала с уровнем, превышающим уровень информационных излучений во всем частотном диапазоне, где имеют место эти излучения, а также осуществляют наводки (по эфиру) и маскирующие шумовые колебания в отводящие цепи.

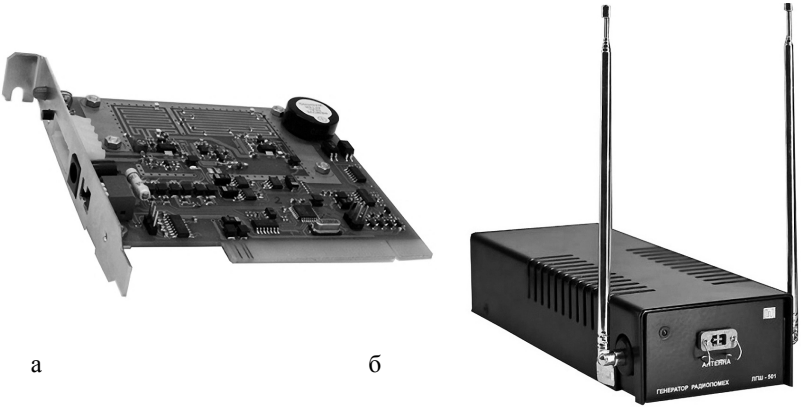
Примером подобного рода устройств является генератор шума ГШ-К-1800 (научно-производственный центр Фирма «НЕЛК»), предназначенный для защиты информации от утечки за счет побочных электромагнитных излучений

[1] См.: Аппаратура защиты от акустической разведки «Соната АВ» модель 3М [Электронный ресурс]. — Режим доступа: http://www.npoanna.ru/Content.aspx?name=models.sonata-avm#/cat/3. — Загл. с экрана.

и наводок, создаваемых средствами вычислительной техники[1]. Эти побочные излучения могут быть приняты чувствительной приемной аппаратурой на расстоянии более 100 м, а информация может быть восстановлена потенциальным противником.

Генератор шума ГШ-К-1800 встраивается в системный блок компьютера и обеспечивает маскировку (защиту) ПЭМИН средств вычислительной техники, размещенных в помещении площадью приблизительно 40-50 кв. м. Защита обеспечивается путем формирования и излучения в окружающее пространство электромагнитного поля шума и наведения маскирующего сигнала в отходящие цепи и инженерные коммуникации.

К данному классу устройств относится и генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-501» (Лаборатория ППШ), предназначенный для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех[2].



а б

3.14. Генераторы шума а) генератор шума ГШ-К-1800;
б) генератор шума ЛГШ-501

7. При проведении в служебном кабинете следственных действий представляется целесообразным использование портативных систем обнаружения технических средств негласного получения информации. К подобного рода устройствам можно отнести, например, селективный обнаружитель цифровых радиопередающих устройств ST165 (производитель — Сигнал-Т). Данное устройство предназначено для обнаружения и идентификации переносных

[1] См.: Генератор шума ГШ-К-1800 [Электронный ресурс]. — Режим доступа: http://infobez.org/activities/catalog/szi_tk/zawita_informacii_v_pobochnyh_kanalah/generator_shuma_gsh-k-1800/. — Загл. с экрана.

[2] Пространственное зашумление. ЛГШ-501 [Электронный ресурс]. — Режим доступа: http://www.pps.ru/?part=catalog&product=59. — Загл. с экрана.

радиопередающих устройств стандартов сотовой связи (сотовые телефоны и модемы GSM 900, 1800, UMTS), беспроводной передачи данных (Wi-Fi и BLUETOOTH) и беспроводных телефонов (DECT)[1]. Поскольку обнаружение передающих устройств осуществляется бесконтактным методом, то факт использования ST165 никоим образом не нарушает права проверяемых лиц.

8. Для исключения возможности утечки речевой информации посредством несанкционированного использования аппаратов систем сотовой связи в служебном кабинете может быть установлена система подавления сотовых телефонов. В качестве примера можно отметить блокиратор сотовой и беспроводной связи ST 202 «UDAV-M» (Центр безопасности информации «Маском»), предназначенный для блокирования сотовых телефонов и беспроводных средств связи, которые могут использоваться в качестве канала передачи подслушивающими устройствами[2].

Рис. 3.15. Блокиратор сотовой и беспроводной связи ST 202 «UDAV-M»

9. Избежать утечки акустической информации из служебного кабинета через сотовый телефон, принадлежащий сотруднику, в случае его негласной дистанционной активизации поможет использование портативных акустических устройств для защиты сотовых телефонов от негласной активации, таких, например, как «Капсула-2» (Центр безопасности информации «Маском»). Данное устройства обеспечивает защиту речевой информации путем постановки акустической помехи во внутреннем объеме изделия и обладает возможностью индикации о поступлении входящих вызовов/сообщений на размещаемые внутри абонентские устройства сотовой связи[3].

---

[1] См.: ST 165 Селективный обнаружитель цифровых радиопередающих устройств [Электронный ресурс]. — Режим доступа: http://signal-t.ru/catalog/signal_t/mobilnye-poiskovye-ustroystva/st-165-selektivnyy-obnaruzhitel-tsifrovykh-radioperedayushchikh-ustroystv/. — Загл. с экрана.

[2] См.: Блокиратор сотовой и беспроводной связи ST 202 «UDAV-M» [Электронный ресурс]. — Режим доступа: http://www.mascom.ru/equipment/sredstva-zashchity-informatsii/blokiratory-sotovoy-i-besprovodnoy-svyazi/blokirator-sistem-besprovodnoy-svyazi-st-202-udav-m.php. — Загл. с экрана.

[3] См.: Капсула. Акустический сейф [Электронный ресурс]. — Режим доступа: http://www.mascom.ru/equipment/tekhnicheskie-sradstva-v-zashchishchennom-ispolnenii/akusticheskie-seyfy/kapsula.php. — Загл. с экрана.

10. При установке в рабочем кабинете сотрудника телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера их следует отключать от сети на время проведения этих мероприятий или использовать соответствующие средства защиты.

Вообще спектр технических средств защиты телефонных линий весьма широк, они существенно различаются как по стоимости, так и по сложности в эксплуатации. С данных позиций и с учетом уровня финансирования правоохранительной деятельности полагаем возможным и необходимым оборудование рабочего места сотрудника устройством защиты телефонных переговоров ЦИКАДА-М (Центр безопасности информации «Маском»)[1].

Данное устройство предназначено для защиты телефонных переговоров на участке линии от абонента до ГАТС и обеспечивает эффективное противодействие следующим средствам несанкционированного съема информации:

– телефонным радиопередатчикам с питанием от линии и с внешним питанием, включенным в линию последовательно, параллельно или через индуктивные датчики;

– аппаратуре магнитной записи, подключаемой к линии через контактные адаптеры или индуктивные датчики;

– микрофонам и радиомикрофонам с питанием от линии и аналогичной аппаратуре (в том числе, параллельным ТА), использующей линию в качестве канала передачи информации или в качестве источника электропитания;

– аппаратуре «ВЧ-навязывания».

Приведенный перечень рекомендаций и технических средств защиты информации, безусловно, не является исчерпывающим. Ключевым вопросом определения необходимого состава системы инженерно-технической защиты информации применительно к реальным условиям расследования конкретного уголовного дела, является анализ вероятности реализации угроз перехвата информации, используемой в ходе расследования. Как представляется, при проведении подобного анализа необходимо принимать в расчет следующее[2].

1. *Потенциальную ценность информации — объекта возможных посягательств, для преступных сообществ, фигурантов по уголовному делу*. В следственной деятельности ценность информации, используемой в расследовании уголовного дела, определяется главным образом тем, насколько эта информация способствует установлению лица, виновного в совершении преступления, доказыванию его вины и других обстоятельств, определенных уголовно-процессуальным законом. Обладание следователем подобного рода информацией может служить сигналом о возможной активизации криминальных элементов, направленной на организацию утечки информации, которой располагает следствие, для организации противодействия ведущемуся расследованию, в том

---

[1] См.: ЦИКАДА-М. Устройство защиты телефонных переговоров [Электронный ресурс]. — Режим доступа: http://mascom-dv.ru/index.php/katalogi/eqipments/zashchita-rechevoj-informatsii/133-sredstva-zaschiti-telefonnih-peregovorov-ot-nesankcionirovannogo-proslushivaniya/493-cikada-m. — Загл. с экрана.

[2] См.: Григорьев А.Н. Теоретические аспекты информации и ее защиты в предварительном расследовании преступлений: дисс. ... канд. юрид. наук. Калининград: Калининградский юридический институт МВД РФ, 2002. С. 172-176.

числе — с целью определить степень осведомленности следователя о тех или иных обстоятельствах совершенного преступления, разрабатываемых следствием версиях, планируемых следственных действиях, заполучить фамилии и адреса свидетелей по уголовному делу для оказания на них давления и т.п.

2. *Круг фигурантов по уголовному делу, их связи в преступной среде, в среде бизнеса и правоохранительных органов, органах власти, их финансовые возможности.*

3. *Стоимость технических средств, необходимых для перехвата информации по тому или иному каналу.* Стоимостной фактор играет немаловажную роль в определении возможности использования того или иного канала перехвата информации в силу различной стоимости необходимых для этого технических средств. Если, например, стоимость несложных в изготовлении акустических закладных устройств, используемых для перехвата акустической информации по воздушным каналам, колеблется в пределах 50-200 долларов США, то стоимость, систем перехвата сотовых телефонов, лазерных систем акустической разведки может составлять десятки, а то и сотни тысяч долларов. Вполне очевидно, что возможность использования последних в целях осуществления перехвата информации не под силу отдельному, пусть даже и очень опасному преступнику. Это по плечу только хорошо организованным преступным группам, обладающим значительными финансовыми возможностями.

4. *Сложность организационных мероприятий по внедрению технических средств негласного получения информации на объект*. Практическое использование специальных технических средств негласного получения информации определяет необходимость проведения определенных организационных мероприятий по их внедрению, созданию условий для их применения, которые весьма разнятся в зависимости от используемого канала перехвата информации.

Практика показывает, что в общем случае в качестве наиболее вероятных путей внедрения специальных технических средств перехвата информации (СПИ) можно выделить следующие:

– установка подобного рода средств в конструкции зданий и помещений во время строительно-ремонтных работ. Следует сказать, что проведение указанных работ предоставляет самые широкие возможности по внедрению наиболее сложных (как в чисто техническом плане, так и в плане обнаружения) СПИ на объект. Однако, проведение подобного рода мероприятий требует наличие нескольких высококвалифицированных специалистов (3-5 человек) и организации конспиративного проникновения на объект в течении нескольких часов;

– установка СПИ в предметы мебели, другие предметы интерьера и обихода, различные технические средства, как общего назначения, так и предназначенные для обработки информации. Наибольшую опасность в этом случае представляют предметы и оборудование, изготовленные на заказ;

– установка СПИ в различные предметы, вручаемые в качестве подарка. Указанные предметы впоследствии могут использоваться для оформления интерьера служебного помещения, что, учитывая технические характеристики современных СПИ (прежде всего их габариты), обуславливает их потенциальную опасность и требует проверки подобного рода предметов на наличие в них встроенных устройств перехвата информации;

– установка СПИ в ходе ремонтно-профилактических работ на инженерных системах и сетях объекта.

5. *Сложность практического использования технических средств перехвата информации*. Возможность практического использования тех или иных средств технической разведки нередко определяется конкретными погодными, временными, пространственными и т.п. условиями. Так, например, использование лазерных микрофонов крайне затруднительно в условиях тумана, дождливой погоды.

6. *Наличие в регионе высококвалифицированных специалистов в области ведения технической разведки*. Ведение технической разведки требует наличия не только необходимых технических средств, но и, как правило, высококвалифицированных специалистов, обладающих опытом работы с ними. В этих целях преступные группировки, обладающие значительными финансовыми возможностями, могут привлекать для выполнения подобного рода «заказов» работников организаций, вполне легально работающих на региональном рынке и имеющих все необходимые лицензии на осуществление деятельности в области защиты информации.

Оснащение объектов органов внутренних дел различными техническими средствами защиты является крайне важной, но не единственной составляющей системы защиты информации от утечки. Немаловажную роль здесь играет проведение специальных поисковых мероприятий по выявлению средств негласного получения информации.

3.4. Организация и проведение специальных проверок объектов информатизации органов внутренних дел

Специальная проверка *— проверка объекта информатизации в целях выявления и изъятия возможно внедренных средств негласного получения информации*[1].

Подобного рода проверки включают в себя:

– специальные проверки технических средств;

– специальные обследования помещений.

Порядок проведения специальной проверки определяется Правительством Российской Федерации и проводится соответствующими органами ФСБ России или организациями, имеющими необходимые лицензии.

Лицензирование — это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ. Получить право или разрешение на определенную деятельность может не каждый субъект, а только отвечающий определенным критериям в соответствии с правилами лицензирования.

---

[1] Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Лицензия — специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Согласно положениям ст. 27 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

В соответствии с пп. 3, 5 п.1 ст. 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», необходимо получение лицензии для осуществления следующих видов деятельности в сфере защиты информации:

– деятельности по выявлению электронных устройств, предназначенных для негласного получения информации. Однако, и это крайне важно с практической точки зрения, наличие лицензии не требуется в случае, если подобного рода работы проводятся для обеспечения собственных нужд;

– деятельности по технической защите конфиденциальной информации.

Специальная проверка технических средств *— это комплекс мероприятий по поиску электронных устройств съема информации («закладочных устройств»), возможно внедренных в технические средства*[1].

Специальным проверкам подвергаются технические средства иностранного производства, а также технические средства отечественного производства, содержащие комплектующие иностранного производства, в случае если они предназначены для:

– обработки сведений, составляющих государственную тайну;

– размещения в защищаемых помещениях;

– обработки информации с ограниченным доступом.

Специальным проверкам в обязательном порядке подвергаются как технические средства, хранящие или обрабатывающие информацию, содержащую сведения, отнесенные к государственной тайне, так и вспомогательные устройства и приборы, установленные в выделенных помещениях в соответствии со *Специальными требованиями и рекомендациями по защите информации, составляющей государственную тайну, от утечки по техническим каналам* (утв. Решением Государственной технической комиссии при Президенте Российской Федерации от 23.05.1997 № 55).

Технические средства, хранящие или обрабатывающие в организации информацию с ограниченным доступом, не составляющую государственную тайну, а также вспомогательные устройства и приборы, установленные в за-

[1] Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки по ТКУИ [Электронный ресурс]. — Режим доступа: http://www.intuit.ru/studies/courses/2291/591/lecture/12707. — Загл. с экрана.

щищаемых помещениях, подвергаются специальной проверке по решению руководителя организации или по требованию государственного заказчика.

В проведении подобного рода проверок можно выделить несколько этапов:

– прием-передача технического средства, формирование исходных данных для составления программы проведения специальной проверки;

– разработка программы проведения специальной проверки технического средства;

– проведение технических проверок;

– анализ результатов.

Для проведения проверки технические средства предоставляются в полной комплектации и исправном состоянии. Также организации, осуществляющей специальную проверку, предоставляются сведения, необходимые для разработки программы специальной проверки. Условно эти сведения можно разделить на три группы:

– *данные о техническом средстве* (назначение технического средства, комплектация, документация, сведения о поставщике и способе приобретения);

– *данные о планируемом применении технического средства* (сведения о том, будет ли техническое средство обрабатывать защищаемую информацию, или располагаться в помещении, где такая информация обрабатывается; сведения о наличии у обрабатываемой информации грифа секретности; сведения о способе применения (в составе системы или самостоятельно), о подключении к коммуникациям);

– *данные о месте размещения* (описание объекта, на котором планируется размещение технического средства, перечень защищаемых на нем сведений, минимальное расстояние до границы контролируемой зоны, возможность и периодичность пребывания иностранных граждан на объекте и т.п.).

По полученным данным проводится проверка, в ходе которой изучаются схема и конструкция построения технического средства, а также принципы обработки в нем информации (как и по каким элементам она циркулирует). На основе данного анализа делаются выводы о естественных каналах утечки информации в силу конструктивных и функциональных особенностей технического средства и возможно внедренных в него специальных электронных устройствах.

Следующий этап — составление программы проведения специальной проверки. Типовая техническая проверка включает в себя:

– дозиметрический контроль изделия для обнаружения радиоактивных меток и радиоизотопных источников питания;

– вихретоковый контроль объектов (узлов) технических средств обработки и передачи информации, не содержащих металлических элементов;

– контроль тары, не имеющей полупроводниковых элементов, прибором нелинейной локации (при необходимости рентгеноскопический контроль) с целью выявления специальных электронных устройств, выполняющих роль «маяка»;

– проведение радиоконтроля с целью выявления демаскирующих признаков активных закладочных устройств;

– проверка возможности осуществления ВЧ-навязывания элементам технического средства;

– разборка технического средства, осмотр его элементов и узлов с целью выявления демаскирующих признаков специальных электронных устройств;

– контроль элементов и узлов технических средств, не содержащих полупроводниковых элементов, прибором нелинейной локации (при необходимости рентгеноскопический или рентгенографический контроль);

– электротехнические измерения параметров элементов и узлов с целью выявления отклонений в схемотехнических и конструктивных решениях;

– рентгенография или рентгеноскопия элементов и узлов технического средства с целью выявления схемных изменений в элементах и неразборных узлах технического средства;

– дешифрация рентгеновских снимков и проведение визуально-оптического контроля внешнего вида и внутренней структуры узлов и элементов технического средства;

– сборка технического средства и контроль работоспособности.

После анализа результатов технической проверки выносится заключение о наличии или отсутствии в техническом средстве специальных электронных устройств. Оформляется акт проведения специальной проверки, в котором приводится перечень проверенных элементов и вид технических проверок, ФИО лиц, проводивших эти проверки и общее заключение по результатам проверки.

Специальное обследование помещений — *это комплекс инженерно-технических мероприятий, проводимых с использованием специализированных технических средств, с целью выявления возможно внедренных электронных средств съема информации в ограждающих конструкциях, мебели и предметах интерьера защищаемого помещения.*

Специальные обследования помещений в обязательном порядке проводятся в отношении выделенных помещений первой категории. В остальных случаях — по решению руководителя организации или по требованию государственного заказчика.

Специальные обследования помещений занимают заметное место в общей системе мероприятий по защите информации. Они проводятся:

– при аттестации помещений;

– периодически (в соответствии с заранее разработанным планом-графиком);

– после проведения в помещениях каких-либо работ (ремонта, монтажа оборудования, изменения интерьера и т.д.);

– после неконтролируемого посещения посторонними лицами;

– во всех случаях, когда возникает подозрение в утечке информации через возможно внедренные средства несанкционированного съема информации.

Говоря о методике проведения поисковых мероприятий, отметим, что по *глубине проводимых проверок* поисковые мероприятия подразделяются на четыре уровня.

Первый уровень: в результате проверки могут быть обнаружены активные радиоизлучающие изделия, установленные непосредственно в проверяемом или смежных с ним помещениях (радиомикрофоны с автономным источником питания, телефонные радиопередатчики).

Второй уровень: могут быть обнаружены все устройства первого уровня плюс сетевые передатчики, использующие в качестве канала передачи сеть питания 220В, 50Гц.

Третий уровень: могут быть выявлены все изделия второго уровня плюс все типы кабельных микрофонных систем, а также оргтехника, работающая в режиме передачи за границы зоны охраны сигнала, содержащего полезную информацию.

Четвертый уровень: могут быть выявлены все типы заносных и закладных электронных устройств перехвата информации и естественные каналы утечки информации.

Мероприятия по поиску средств съема информации могут проводиться как в служебных, так и в не служебных помещениях сотрудников органов внутренних дел и могут быть подразделены на *плановые, внеплановые* и *повседневные*.

Мероприятия, относящиеся к первой группе, должны проводиться специалистами, как правило, по определенному графику с использованием специальных технических систем обнаружения средств несанкционированного съема информации. Они в обязательном порядке должны включать в себя регулярный мониторинг радиоэфира объекта защиты (составление карты радиоэфира здания ОВД, отслеживание и анализ ее изменений) и проведение поисковых мероприятий как минимум второго уровня.

В общем случае в организации проведения поисковых мероприятий можно выделить следующие этапы.

1. *Подготовка к проведению поисковых мероприятий.* На данном этапе производится оценка возможных технических каналов утечки информации, на основе которой составляется план проведения поисковых мероприятий с указанием их сроков и последовательности выполнения работ. Определяются основные направления поиска, выделяются объекты обследования, определяется перечень необходимой поисковой техники.

2. *Проведение поисковых мероприятий.*

а) *Визуальный осмотр*. В ходе проведения визуального осмотра реально существующая обстановка сравнивается с чертежами, планами помещения, содержащимися в техническом паспорте здания, проводится сверка имеющихся в помещении предметов интерьера и мебели с описью закрепленного за помещением имущества.

Особое внимание при проведении осмотра необходимо обращать на предметы (сувениры, подарки и т.п.) и электронные устройства, происхождение которых достоверно не установлено.

Также осматриваются и вводы инженерных коммуникаций в здание и прилегающее к ним пространство. Вскрываются и просматриваются короба, стояки и ниши, где проходят проводные коммуникации, электроустановочная арматура.

б) *Контроль и анализ радиоэфира*. Задачей данного этапа является обнаружение подозрительных радиоизлучений в помещениях объекта проверки. Для этого составляется карта занятости эфира в месте расположения проверяемого объекта. По результатам ее изучения выявляются сигналы «легальных» радиостанций, которые исключаются из дальнейшего анализа, и подозрительные

радиоизлучения, подлежащие тщательному исследованию. Для локализации последних могут быть использованы индикаторы электромагнитного поля.

в) *Проверка электронных приборов*. Самый эффективный и надежный способ проведения подобной проверки — сравнение с эталоном. Для этого электронные устройства вскрывают и тщательно осматривают на предмет выявления изменений, внесенных в схему прибора.

Данный способ позволяет выявить несанкционированные конструктивные изменения электронных устройств, но только те, которые возможно обнаружить при их визуальном осмотре. Для выявления подозрительных излучений этих устройств необходимо исследование излучаемого им радиосигнала с помощью индикатора поля, портативного частотомера и комплекса радиоконтроля.

г) *Проверка предметов интерьера и мебели.* Проверка мебели и других предметов интерьера (карнизы, лампы, торшеры, вазы, часы, письменные приборы и т.п.) должна начинаться с их тщательного визуального осмотра, проводимого в том числе и с использованием досмотровых приборов (досмотровые зеркала, фонари, эндоскопы и т.п.).

При проведении визуального осмотра особое внимание следует уделить всякого рода дополнительным брускам, установленным якобы для усиления конструкции, а также способам их крепления.

Аппаратурная проверка мебели и предметов интерьера обычно проводится с помощью металлоискателя, нелинейного локатора и рентгеновского аппарата. Тип поискового прибора выбирается в зависимости от материала обследуемого предмета. Однако окончательный ответ на вопрос, что является причиной срабатывания поисковой аппаратуры, может дать только физическое вскрытие, например, частичная разборка проверяемого предмета и, наконец, рентгенографирование.

д) *Проверка проводных линий, электроустановочных и коммуникационных изделий.* Работы по проверке проводных коммуникаций начинаются с изучения их принципиальных схем, схем их прохождения на поэтажных планах здания, визуального прослеживания этих линий и проверки соответствия фактического прохождения коммуникаций указанным схемам и планам. Следует установить, не подключены ли к линиям, входящим в проверяемое помещение, другие потребители.

Работу по физической и аппаратурной проверке проводных коммуникаций можно разбить на два этапа. Первый выполняется на линиях, не отсоединенных от распределительных щитов и других коммутационных устройств (работа «под напряжением» для электросети). В ходе данного этапа определяется наличие в линии речевых сигналов от микрофонов подслушивания, передаваемых как в слышимом диапазоне (20 Гц — 20 кГц), так и в диапазоне выше 20 кГц. Указанная проверка осуществляется с помощью усилителей и специальных сканирующих устройств, подключаемых к проверяемой линии.

Второй этап начинается с отключения проверяемых линий и демонтажа всех осветительных приборов, установочных и других изделий, которые затем тщательно проверяются и просвечиваются рентгеном.

Особое внимание следует уделить проверке телефонных линий. Телефонная линия обследуется индикатором поля или другим устройством контроля

эфира под нагрузкой. В ходе проверки имитируется разговор по указанной линии, а оператор перемещается вдоль нее с индикатором поля или другим подобным прибором. При обнаружении подозрительных излучений производится многократное разъединение. Если уровень подозрительного сигнала меняется в такт с этим, можно сделать вывод, что обнаруженный сигнал с большой долей вероятности можно отнести к средству съема информации и его следует поставить на контроль для последующей дешифровки. Перемещая аппаратуру контроля вдоль телефонной линии, можно определить места расположения источника подозрительного излучения.

е) *Обследование ограждающих конструкций.* Обследование ограждающих конструкций помещения представляет собой заключительный и весьма ответственный этап аппаратурного обследования. Основным поисковым прибором при этом, как правило, является нелинейный локатор[1].

Перед началом обследования ограждающих конструкций нелинейным локатором следует внимательно осмотреть соседние помещения и вынести из них все устройства, содержащие электронные элементы и узлы. В крайнем случае следует как можно дальше отнести их от стен, смежных с проверяемым помещением.

При появлении отклика его положение фиксируется на стене с помощью маркера, кусочка клейкой ленты или иным доступным способом. Затем проводится дешифровка откликов и оценка возможных причин их возникновения. Если имеется такая возможность, следует попробовать обследовать подозрительное место с противоположной стороны. Подозрительные отклики, причину которых установить не удается, следует идентифицировать путем физического вскрытия или рентгено-графирования.

ж) *Заключительный этап поискового мероприятия.* На данном этапе составляются отчетные документы о результатах проведения на объекте поисковых работ, которые должны включать в себя и рекомендации по организации защиты информации на объекте, перекрытию выявленных каналов утечки, проведению дополнительных работ по проверке эксплуатируемых на объекте технических средств.

При появлении признаков утечки защищаемой информации должны проводится *внеплановые поисковые мероприятия.* Если вести речь об осуществляемой органами внутренних дел деятельности по выявлению, раскрытию и расследованию преступлений, то к числу таких признаков можно отнести: упреждающие действия криминальных элементов — фигурантов по уголовному делу, связанные с оказанием давления на свидетелей, потерпевших и других участников уголовного судопроизводства, уничтожением вещественных доказательств и т.п.

По используемым методикам и техническим средствам данные мероприятия соответствуют плановым проверочным мероприятиям за одним исключением. Полагаем, что при проведении подобного рода проверочных меропри-

---

[1] *Нелинейный локатор* — прибор, предназначенный для обнаружения в строительных конструкциях помещений и предметах их интерьера скрытно установленных радиопередающих устройств и других технических средств съема информации, содержащих в себе полупроводниковые компоненты и находящихся как во включенном, так и в выключенном состоянии.

ятий особое внимание должно уделяться маскировке их проведения, чтобы сохранить в тайне сам факт и результаты их проведения от криминальных элементов, осуществляющих несанкционированный перехват информации. Соблюдение указанного позволит следователю, в случае необходимости, использовать это для введения преступных элементов в заблуждение относительно тех или иных обстоятельств расследуемого уголовного дела, планируемых действий и т.п., обеспечивая тем самым решение определенных тактических задач расследования.

И, наконец, следователем или дознавателем без привлечения специалистов и специальных технических средств могут проводиться *повседневные поисковые мероприятия*. Основная цель подобного рода мероприятий — непродолжительное (лучше всего утром, за некоторое время до начала рабочего дня) визуальное обследование своего служебного кабинета на предмет выявления в нем технических средств перехвата информации.

При проведении визуального осмотра помещения в первую очередь осмотру подлежат:

1) сувениры, подарки, предметы мебели и интерьера. К последним относятся все предметы обихода и оборудование, постоянно находящееся или временно принесенное в помещение (лампы, торшеры, вазы, часы и т.п.).

Осмотр указанных предметов имеет своей целью:

– выявление в обследуемом помещении новых предметов, которые ранее в нем отсутствовали и в которых могут быть установлены технические средства перехвата информации;

– выявление факта несанкционированного нарушения конструктивной целостности предметов (например, следов их разборки), что может свидетельствовать об их использовании для камуфляжа подобного рода устройств;

– обнаружение в указанных предметах установленных технических средства перехвата информации.

В целях облегчения решения указанных задач при первичном проведении визуального осмотра целесообразно нанести на указанные предметы скрытые метки, которые позволили бы в дальнейшем определить — не был ли данный предмет кем-либо подменен. Также, целесообразным представляется проведение фотосъемки обследуемого помещения с целью фиксации пространственного расположения предметов мебели и интерьера. Проведение фотосъемки может оказать неоценимую помощь в обнаружении признаков возможной установки технических средств перехвата информации в обследуемом помещении, появления в нем новых предметов, в которых могут встроены подобного рода устройства (например, оставленный кем-то ежедневник, сотовый телефон, включенный в розетку электротройник иного цвета и т.п.), обнаружении признаков вскрытия предметов мебели и интерьера (рабочего стола, навесных полов, настенных панелей и т.п.).

2) наиболее доступные места возможной установки специальных технических средств негласного получения информации.

Проведение подобного рода поисковых мероприятий, безусловно, не является решением проблемы и в случае выявления подозрительных устройств необходимо привлечение специалистов для их дальнейшего исследования. Однако, это может снизить риск утечки информации, ограничивая возможности

злоумышленника в использовании технических средств разведки. Кроме того, обнаружение при проведении поисковых мероприятий средств ведения технической разведки не только свидетельствует о наличии угрозы безопасности защищаемой информации, но и является тревожным сигналом об активизации криминальных элементов, о возможном использовании ими в дальнейшем и других мер противодействия органам внутренних дел, в том числе и связанных с угрозой жизни и здоровью как самого сотрудника органов внутренних дел, так и членов его семьи.

Подводя итоги рассмотрения вопросов, затронутых в настоящем разделе учебного пособия, отметим следующее.

В процессе функционирования объекта информатизации защищаемая информация может по различным причинам выйти за пределы установленной сферы обращения. В этом случае утрачивается контроль за ее распространением — происходит утечка информации.

Утечка защищаемой информации является следствием практического проявления угроз информационной безопасности и может происходить по разным каналам: легальным, агентурным и техническим.

Усиливающийся в последнее время уровень информационно-технического противодействия органам внутренних дел со стороны криминального мира, характеризующегося широким использованием новейших технических средств негласного получения информации, актуализирует проблему защиты информации и информационных ресурсов органов внутренних дел от утечки по техническим каналам.

Обеспечение защиты информации от утечки по техническим каналам обеспечивается реализацией целого комплекса мер, ключевую роль в котором играют мероприятия организационного и инженерно-технического характера.

К основным организационным мероприятиям по защите информации от утечки по техническим каналам, проводимым на объектах информатизации, подлежащих защите, можно отнести следующие: выбор помещения для установки основных и вспомогательных технических средств и систем; использование только сертифицированных технических средств и систем защиты информации; установление контролируемой зоны вокруг объекта; режимное ограничение доступа на объекты размещения основных технических средств и систем и в выделенные помещения; категорирование и аттестация объектов информатизации и выделенных помещений по требованиям безопасности информации.

Инженерно-технические мероприятия по защите информации включают в себя: сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здания и помещения; средства защиты технических каналов утечки информации; средства обеспечения охраны территорий, зданий, помещений; средства противопожарной охраны; технические средства и мероприятия, предотвращающие вынос персоналом из помещений документов, дисков и других носителей информации.

Крайне важную роль в обеспечении защиты информации от утечки по техническим каналам играют специальные проверки объектов информатизации. Подобного рода проверки включают в себя специальные проверки технических средств и специальные обследования помещений.

Специальная проверка технических средств подразумевает проведение целого комплекса мероприятий по поиску электронных устройств съема информации («закладочных устройств»), возможно внедренных в технические средства.

Специальное обследование помещений предполагает осуществление комплекса инженерно-технических мероприятий, проводимых с использованием специализированных технических средств, с целью выявления возможно внедренных электронных средств съема информации в ограждающих конструкциях, мебели и предметах интерьера защищаемого помещения.

Контрольные вопросы

1. Что понимается под утечкой информации?
2. Перечислите виды каналов утечки защищаемой информации.
3. Приведите понятие и виды технических каналов утечки информации.
4. Приведите основные характеристики технических каналов утечки информации, передаваемой по каналам связи.
5. Приведите основные характеристики технических каналов утечки речевой информации.
6. Что понимается под инженерно-технической защитой информации?
7. Раскройте структуру системы инженерно-технической защиты информации.
8. Для чего проводится специальная проверка технических средств?
9. Что понимается под специальным обследованием помещений, каковы цели его проведения?
10. Какова основная цель аттестации объектов информатизации по требованиям безопасности информации?

4. ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

4.1. Основные угрозы безопасности информации в компьютерных системах

В современных условиях эффективность правоохранительной деятельности во многом определяется количественными и качественными характеристиками информации, которой располагают правоохранительные органы. В этом смысле информация является не только основой деятельности органов внутренних дел, но и связующим звеном со всей деятельностью государства по борьбе с преступностью. Отмеченное предопределяет широкое использование в практике правоохранительной деятельности информационных систем, построенных на базе новых информационных технологий.

Интенсивная информатизация правоохранительной сферы общества, помимо очевидных преимуществ, порождает и новые вызовы безопасности информации, используемой в деятельности органов внутренних дел. Тревожной тенденцией в сфере кибербезопасности является рост количества атак на российские информационные ресурсы, активизация деятельности иностранных разведок по внедрению в информационные системы органов государственной власти Российской Федерации своих программных средств. Как отметил в своем выступлении на прошедшем 8 июля 2015 г. в г. Вологде совещании, посвященном вопросам противодействия угрозам в информационной сфере, Секретарь Совета Безопасности Российской Федерации Н.П. Патрушев: «…специалисты отмечают заметное увеличение числа компьютерных атак на информационно-телекоммуникационные сети и информационные системы органов государственной власти. Отмечается наличие в информационных системах программных средств иностранных технических разведок. Это требует совершенствования системы защиты информации»[1].

Данные обстоятельства со всей очевидностью предопределяют необходимость принятия адекватных мер противодействия угрозам безопасности информации в компьютерных системах органов внутренних дел.

В научной литературе под компьютерной системой понимается «…комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации»[2].

Отталкиваясь от рассмотренного ранее понятия угрозы безопасности информации, *под* ***угрозой безопасности информации в компьютерных системах*** *будем понимать совокупность условий и факторов, создающих потен-*

[1] Патрушев рассказал о внедрении разведками вирусов в информационные системы госвласти [Электронный ресурс]. — Режим доступа: http://vz.ru/news/2015/7/8/755034.print.html. — Загл. с экрана.

[2] Лапин В.В. Основы информационной безопасности в ОВД: курс лекций. М.: Московский университет МВД России, 2009. С. 65.

циальную или реальную опасность нарушения целостности, доступности, конфиденциальности обрабатываемой в них информации и/или нарушения надежности реализации функций компьютерной системы.

В настоящее время известен достаточно обширный перечень угроз безопасности информации в компьютерных системах. Однако, как отмечалось ранее, безопасность информационных ресурсов и информационной инфраструктуры органов внутренних дел проявляется через обеспечение безопасности их наиболее важных свойств, к числу которых относят целостность, доступность и конфиденциальность. Соответственно, для компьютерных систем угрозы могут быть классифицированы, прежде всего, по аспекту информационной безопасности, против которого они направлены в первую очередь[1]:

– *угрозы нарушения целостности информации*, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение либо искажение, приводящие к нарушению ее качества или полному уничтожению;

– *угрозы нарушения доступности* (отказ в обслуживании), направленные на создание таких ситуаций, когда определенные действия либо блокируют доступ к некоторым ресурсам информационной системы, либо снижают ее работоспособность. Блокирование доступа к ресурсу может быть постоянным или временным;

– *угрозы нарушения конфиденциальности*, направленные на разглашение информации с ограниченным доступом. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. Применительно к компьютерной системе данная угроза реализуется всякий раз, когда злоумышленник получает несанкционированный доступ к хранящейся в ней информации.

Помимо отмеченного, угрозы безопасности информации и информационным процессам в компьютерных системах по своей природе могут быть подразделены на *случайные* и *преднамеренные*[2].

Под случайной угрозой понимают непреднамеренное изменение информации в процессе ввода, хранения, обработки или передачи. Случайные воздействия могут быть аппаратными и программными. В результате случайных воздействий на аппаратном уровне происходит физическое изменение сигналов, в том числе непосредственно хранимых данных, либо носителей информации. На программном уровне случайные воздействия могут привести к изменению алгоритма функционирования процесса обработки данных.

Источниками случайных угроз могут быть:

– отказы и сбои аппаратного обеспечения компьютерных систем (в том числе из-за стихийных бедствий);

– ошибки в программном обеспечении;

– ошибки в работе пользователей компьютерных систем и персонала, занятого в их обслуживании;

---

[1] См.: Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМ К Пресс, 2012. С. 31-32.

[2] См.: Лапин В.В. Основы информационной безопасности в ОВД: курс лекций. М.: Московский университет МВД России, 2009; Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМ К Пресс, 2012. С. 34

– помехи в линиях связи из-за воздействий внешней среды;

– аварийные ситуации из-за стихийных бедствий и различного рода техногенных аварий.

Ошибки в программном обеспечении являются одним из самых распространенных видов угроз безопасности в компьютерных системах. Наличие таких ошибок является объективных фактом, обусловленным тем, что программное обеспечение создается не компьютером, а человек. Несмотря на то, что при создании программного продукта порядка 50% общего времени и стоимости расходуется на отладку и тестирование программы[1], гарантировать отсутствие в программном продукте ошибок невозможно. Большинство из этих ошибок не представляют никакой опасности, некоторые же могут привести к серьезным последствиям. Так, например, известен случай, когда из-за программной ошибки в декабре 2010 г. три спутника, необходимые для завершения формирования орбитальной группировки системы ГЛОНАСС, упали в Тихий океан вскоре после запуска ракетой «Протон-М». Как показало проведенное расследование, причиной аварии явилась ошибка в программировании, которая привела к тому, что в ракету залили неправильное количество топлива.

Ошибки в программном обеспечении также могут быть использованы злоумышленниками для перехвата контроля над компьютерной системой, несанкционированного использования ее ресурсов. Обычно подобные ошибки устраняются с помощью пакетов обновлений, которые регулярно выпускаются производителем программного обеспечения. Своевременная установка таких пакетов является необходимым условием обеспечения безопасности информации в компьютерной системе.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя, направленными на изменение количественных и качественных характеристик информации и/или ее носителей.

Под *нарушителем безопасности информации понимается физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах*[2].

В общем случае можно выделить следующие виды нарушителей[3]:

– специальные службы иностранных государств (блоков государств);

– террористические, экстремистские группировки; преступные группы (криминальные структуры);

---

[1] См.: Степанченко И.В. Методы тестирования программного обеспечения: учеб. пособие. Волгоград: ВолгГТУ, 2006.

[2] См.: Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 531-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] См.: ФСТЭК России. Методика определения угроз безопасности в информационных системах (проект) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/ attachments/download/812. — Загл. с экрана.

– внешние субъекты (физические лица);

– разработчики, производители, поставщики программных, технических и программно-технических средств;

– лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

– лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, уборщики и т.д.);

– пользователи информационной системы;

– администраторы информационной системы и администраторы безопасности;

– бывшие работники (пользователи).

Применительно к конкретной компьютерной системе виды нарушителей определяются на основе предположений о возможных мотивах их действий. Таковыми могут быть:

– нанесение ущерба государству, отдельным сферам его деятельности;

– реализация угроз безопасности информации по идеологическим или политическим мотивам;

– организация террористического акта;

– причинение имущественного ущерба путем мошенничества или иным преступным путем;

– дискредитация или дестабилизация деятельности органов государственной власти, организаций;

– внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;

– любопытство или желание самореализации;

– выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;

– реализация угроз безопасности информации из мести;

– реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя, представляющую собой «…его комплексную характеристику, отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения»[1].

Модель вероятного нарушителя безопасности информации в компьютерных системах необходима для систематизации информации о типах и возможностях субъектов, целях несанкционированных воздействий и выработки адекватных мер противодействия. При разработке модели нарушителя учитываются: типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации; цели, которые могут преследо-

[1] Дровникова И.Г., Буцынская Т.А. Модель нарушителя в системе безопасности [Электронный ресурс]. — Режим доступа: http://www.aktivsb.ru/ info600.html.

вать нарушители каждого вида при реализации угроз безопасности информации; возможные способы реализации угроз безопасности информации[1].

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики — важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы обеспечения информационной безопасности.

В самом общем виде модель вероятного нарушителя безопасности информации в компьютерных системах основывается на следующих предположениях[2]:

– квалификация нарушителя может быть на уровне разработчика компьютерной системы;

– нарушителем может быть как постороннее лицо, так и законный пользователь компьютерной системы;

– нарушителю известна информация о принципах работы компьютерной системы;

– нарушитель выберет наиболее слабое звено в защите компьютерной системы.

Важно отметить, что применительно к конкретной компьютерной системе угрозы безопасности информации определяются по результатам оценки возможностей внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

Для определения угроз безопасности информации в компьютерных системах органов внутренних дел применяются нормативные и методические документы ФСБ России и ФСТЭК России.

Наиболее распространенным видом нарушения безопасности информации в компьютерных системах является несанкционированный доступ (НСД).

Несанкционированный доступ (НСД) к компьютерной информации — *доступ к информации или действия с информацией, нарушающие правила раз-*

---

[1] См.: Миронова В.Г., Шелупанов А.А. Модель нарушителя безопасности конфиденциальной информации // Информационная безопасность систем. 2012. № 1(31). С. 28-34.

[2] См.: Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. М.: ИД «ФОРУМ»; «ИНФРА-М», 2011. С. 20.

граничения доступа с использованием штатных средств, предоставляемых средством вычислительной техники или автоматизированной системой[1].

Таким образом, суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение установленных в организации правил работы с информацией. При этом, несанкционированный доступ к компьютерной системе может быть осуществлен как штатными средствами компьютерной системы, так и специально созданными аппаратными и программными средствами.

В специальной литературе выделяют различные способы осуществления несанкционированного доступа к компьютерной системе. В качестве наиболее распространенных можно выделить следующие:

– перехват пароля;
– подбор пароля;
– компрометация пароля;
– маскарад;
– незаконное использование привилегий;
– использование вредоносных программ.

Для ***перехвата паролей*** используется специальное программное обеспечение, с помощью которого пароль может быть похищен, например, во время его ввода с клавиатуры, в процессе обработки в оперативной памяти компьютера или при его передаче на сервер.

Перехват паролей, которые пользователь вводит с клавиатуры, осуществляется при помощи так называемых «клавиатурных шпионов» — программ, которые перехватывают всю вводимую пользователем с клавиатуры информацию и тем или иным способом передают ее злоумышленнику.

Перехват пароля при его обработке в оперативной памяти компьютера может быть осуществлен при помощи специализированных программ, например, NtPassDump[2].

В случае передачи пароля по сети он может быть перехвачен при помощи «снифферов», которые представляют собой программы, предназначенные для перехвата и последующего анализа передаваемой по сети информации.

Подбор пароля осуществляется с помощью специальных программных средств, которые используют два основных метода вскрытия парольной защиты компьютерных систем: полный перебор (или метод «грубой силы», англ. *brute force*) и перебор по словарю.

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 531-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См.: Середа С. Информационная безопасность корпоративных информационных систем [Электронный ресурс]. — Режим доступа: http://sapland.ru/articles/ stats/ inphormatsionnaya-bezopasnosti-korporativnih-inphormatsionnih-sistem-tipovie-ugr.html. — Загл. с экрана.

В первом случае подбор пароля осуществляется прямым перебором всех возможных его комбинаций, во втором — возможные значения паролей выбираются из специальных словарей, которые содержат десятки и сотни тысяч слов, имен, названий, наиболее часто употребляемых в качестве паролей, и могут подключаться к программам взлома паролей.

В качестве примера программных средств, предназначенных для подбора пароля, можно привести пакет программ *ElcomSoft Password Recovery Bundle*. Справедливости ради следует отметить, что данное программное обеспечение разрабатывалось не для взлома парольной защиты компьютерных систем, а для решения задач судебной компьютерно-технической экспертизы.

Причиной ***компрометации пароля*** является, как правило, неосторожность его обладателя. Пароль будет скомпрометирован, в частности, если пользователь запишет его и оставит в месте, доступном для третьих лиц (например, на своем рабочем столе, мониторе и т.д.).

Возможно и намеренное разглашение пароля, вызванное определенными обстоятельствами. Например, сотрудник находится в отпуске, а руководителю организации необходимо срочно получить важный документ, который хранится в компьютере сотрудника.

Пароль может быть скомпрометирован и в том случае, если при его составлении использовались данные, так или иначе связанные с личность сотрудника (фамилия, имя, номер телефона и т.д.).

Маскарад — это такой способ осуществления несанкционированного доступа к компьютерной системе, при котором один пользователь выполняет какие-либо действия от имени другого, обладающего соответствующими полномочиями. Целью маскарада является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя, например, передача сообщения в сети от имени другого пользователя.

Незаконное использование привилегий. Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный. Несанкционированный захват привилегий, например, посредством маскарада, приводит к возможности выполнения нарушителем определенных действий в обход системы защиты.

Вредоносные программы. Под вредоносной программой *понимается программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы*[1].

Основными видами вредоносных программ являются:

– программные закладки;

– классические программные (компьютерные) вирусы;

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

– вредоносные программы, распространяющиеся по сети (сетевые черви);

– другие вредоносные программы, предназначенные для осуществления НСД.

Вредоносные программы могут переходить из одного вида в другой, например, программная закладка может сгенерировать программный вирус, который, в свою очередь, попав в условия сети, может сформировать сетевого червя или другую вредоносную программу.

Таким образом, приходится констатировать наличие достаточно большого числа различных каналов утечки компьютерной информации, хранимой и обрабатываемой в информационных системах органов внутренних дел. Нередко реализация этих угроз образует состав преступлений, предусмотренных действующим уголовным кодексом Российской Федерации.

4.2. Понятие, виды и общая характеристика преступлений в сфере компьютерной информации

Каждый новый виток развития цивилизации ознаменуется фантастическими изобретениями и открытиями. Одним из таких событий в XX веке стало создание устройств, способных обрабатывать огромные потоки информации — электронных вычислительных машин. Pro mundi beneficio, однако, преступный мир всегда невидимой тенью впитывал в себя передовые достижения человечества, породив новые виды преступлений — в сфере компьютерной информации.

По данным международной исследовательской компании Allianz Global Corporate & Specialty, в 2016 году общий ущерб от интернет-преступности для мировой экономики (включая прямые потери, недополученную прибыль и расходы на восстановление систем) превысил 575 млрд долларов. Это около 1% мирового ВВП. В 2017 году ущерб мировой экономики от участившихся кибератак, по прогнозам Сбербанка, может перевалить за 1 трлн долларов, а через три года — вырасти до 2 трлн долларов (для сравнения: мировой оборот наркоторговли сейчас оценивается примерно в 500 млрд долларов в год)[1].

В этой связи вполне закономерно то, что многие страны мира, и Россия не является исключением, пошли по пути криминализации неправомерных действий, совершаемых в отношении компьютерных систем и компьютерной информации.

В 1996 г. в самой первой редакции Уголовного кодекса Российской Федерации (далее — УК РФ) впервые в отечественном уголовном праве законодателем был создан субинститут преступлений в сфере компьютерной информации (глава 28).

Под ***преступлениями в сфере компьютерной информации*** понимаются *виновно совершенные общественно опасные деяния, посягающие на нормаль-*

[1] См.: Грамматчиков А., Вандышева О. Идет кибервойна народная [Электронный ресурс]. — Режим доступа: http://expert.ru/expert/2017/05/idet-kibervojna-narodnaya. — Загл. с экрана.

ный порядок обращения охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания[1].

При этом в действующем уголовном законодательстве ***компьютерная информация*** рассматривается как *сведения* (*сообщения, данные*), *представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.*

Анализ содержащихся в главе 28 УК РФ статей (их всего три) позволяет выделить соответственно три вида компьютерных преступлений.

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации» предусматривает уголовную ответственность *за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.*

Понятие неправомерного доступа к охраняемой законом информации уже рассматривалось ранее. Однако, говоря о неправомерном доступе к компьютерной информации, важно иметь в виду, что уголовная ответственность наступает за неправомерный доступ не к любой, а только к *охраняемой законом компьютерной информации*, то есть любой информации, охраняемой законом в связи с охраной вещных и обязательственных прав на ЭВМ и информационное обеспечение информационных технологий, а также в связи с тайной связи. Она может быть документированная или недокументированная, может относиться к «информационным ресурсам ограниченного доступа» и не относиться к ним, может охраняться как объект авторских прав и может не охраняться им. Не ограничивается круг охраняемой законом информации и сведениями, составляющими государственную, коммерческую, профессиональную, личную, семейную и другие тайны.

Состав неправомерного доступа к компьютерной информации предполагает обязательное наступление одного из указанных в уголовном законе последствий: *уничтожение, блокирование, модификация* либо *копирование информации*.

Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» предусматривает уголовную ответственность за *создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.*

Как уже ранее отмечалось, под вредоносной программой понимается программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы[2].

---

[1] См.: Богдановская В.А., Згадзай О.Э. Расследование преступлений в сфере компьютерной информации. Казань: Казанский юридический институт МВД России, 2012.

[2] См.: Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Для того чтобы программа считалась вредоносной, она должна соответствовать следующим трем критериям[1]:

1. Уничтожение информации или нарушение работы всей системы. Однако осуществление лицом только взлома защиты от копирования еще нельзя оценивать как создание вредоносной программы.

2. Несанкционированная работа. Программа, например, форматирования диска, входящая в комплект любой операционной системы, сама по себе еще не является вредоносной, так как ее запуск санкционируется пользователем.

3. Заведомая вредоносность программы — явной целью ее создания является несанкционированное уничтожение информации. Программы, содержащие в себе различные ошибки, могут быть оценены как нарушение прав потребителей или как преступная халатность, но не как создание вредоносной программы.

Под с*оздани*ем *вредоносной программы* следует понимать творческую деятельность, направленную на создание качественно новой программы, заведомо наделяемой функциями, выполнение которых может оказать неправомерное воздействие на компьютерную информацию и средства компьютерной техники.

Под использованием вредоносной программы понимается ее непосредственное использование для несанкционированного уничтожения, блокирования, модификации, копирования информации, нарушения работы ЭВМ, их системы или сети.

Распространение вредоносной программы означает как распространение ее с помощью средств связи, так и простую передачу ее другому лицу в любой форме (в том числе и в виде записи на бумаге). Распространение машинных носителей вредоносной программы означает передачу носителя другому лицу, включая копирование или дозволение копирования программы на носитель другого лица[2].

И, наконец, ***статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»*** предусматривает уголовную ответственность *за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации.*

Под правилами эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей следует понимать как правила, которые могут быть установлены компетентным государственным органом, так и технические правила, установленные изготовителями компьютерного оборудования, разработчиками программ,

---

[1] См.: Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015. С. 163.

[2] См.: Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений. М.: Собрание, 2004.

сетевыми администраторами, владельцем компьютерной системы или по его полномочию. Эти правила определяются соответствующими техническими нормативными актами. Они также излагаются в паспортах качества, технических описаниях и инструкциях по эксплуатации, передаваемых пользователю при приобретении вещественных средств компьютерной техники (ЭВМ и периферийных устройств), в инструкциях по использованию программ для ЭВМ. Соответствующие инструкции могут излагаться на бумажных и машинных носителях; в последнем случае они включаются в программу, которая обеспечивает к ним доступ при желании пользователя.

В правилах эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей быть установлены как требования технического характера, так и положения, регулирующие работу с программными продуктами (последовательность подачи команд или выполнения процедур, запрет на выполнение каких-либо операций с программным обеспечением, контроль за совместимостью различных программных продуктов, обязательное выполнение определенных процедур при наступлении определенных обстоятельств и т.д.).

Таким образом, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей могут быть подразделены на *физические* (неправильная установка приборов, нарушение температурного режима в помещении, неправильное подключение к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных приборов и узлов) и *интеллектуальные* (неверное ведение диалога с компьютерной программой, ввод данных, обработка которых непосильна данным средствам вычислительной техники).

Сопоставляя компьютерные преступления с другими составами правонарушений, предусмотренных уголовным кодексом, можно выделить их следующие *отличительные особенности:*

– *высокая скрытность (латентность), сложность сбора улик по установленным фактам;*

– *сложность доказательства в суде подобных дел;*

– *«интернациональность» компьютерных преступлений.* В настоящее время с развитием телекоммуникационных систем реальностью стала возможность совершения компьютерного преступления злоумышленником, находящимся за тысячи километров от места преступления. Достаточно вспомнить хотя бы нашумевшую в свое время историю с Владимиром Левиным, который в 1994 г. сумел проникнуть в компьютерную систему Ситибанка. «Дело Левина» было отнесено по классификации международной уголовной полиции к категории «транснациональных сетевых компьютерных преступлений»;

– *высокий ущерб даже от единичного преступления*. Так, например, в январе 2016 года в результате несанкционированного доступа хакерами было похищено 508,67 млн руб. с корреспондентского счета Русского международного банка в Центробанке России[1].

[1] См.: Хакеры похитили более 500 млн рублей со счета Русского международного бака в ЦБ [Электронный ресурс]. — Режим доступа: http://www.kommersant.ru/doc/2979241. — Загл. с экрана.

– *вполне определенный контингент лиц, совершающих правонарушения в сфере компьютерной информации*: это, как правило, высококвалифицированные программисты, специалисты в области телекоммуникационных систем, системные и банковские программисты.

Для обозначения лиц, совершающих преступления в сфере компьютерной информации, как правило, используется термин «хакер» (англ. *hacker* от *hack* — рубить, кромсать).

Исследователи, как российские, так и зарубежные, обычно выделяют следующие особенности личности хакеров:

– стремление четко сформулировать любую возникающую проблему, выделить основные и второстепенные элементы;

– сильно развитое формальное (с точки зрения математики и логики) мышление, которое зачастую подводит в реальной жизни;

– стремление к точности, четкости и однозначности в языке, применение при этом компьютерного жаргона мало понятного неспециалисту, но представляющего собой весьма четкий «специальный» понятийный аппарат[1].

Как свидетельствуют результаты научных исследований, компьютерные преступники делятся на три основные возрастные группы: 11-15 лет, 17-25 лет и 30-45 лет[2].

Представители первой, и отчасти — второй, возрастных групп — это школьники или студенты высших или средних специальных учебных заведений, которые активно ищут пути самовыражения и находят их, погружаясь в виртуальный мир компьютерных сетей.

Компьютерные преступники, входящие в третью возрастную группу, представляют более серьезную опасность. Это уже вполне сформировавшиеся личности, обладающие высокими профессиональными навыками и определенным жизненным опытом. Совершаемые ими действия носят осознанный корыстный характер.

Практически все известные отечественные преступники в сфере компьютерной информации — мужчины, женщины — скорее исключение[3].

Основными целями и мотивами совершения преступлений в сфере компьютерной информации выступают: корысть — 57,3%, хулиганские побуждения —18,3%, месть — 9,2%, коммерческий шпионаж, саботаж или диверсия — 10,6%[4].

В своем комплексном исследовании, посвященном проблемам противодействия компьютерной преступности, В.М. Быков и В.Н. Черкасов выделяют

---

[1] См.: Мещеряков В.А. Словарь компьютерного жаргона. Воронеж: Изд. ВГУ, 1999.

[2] См.: Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. М.: Изд. «Щит-М», 1999.

[3] Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. М.: Изд. «Щит-М», 1999.

[4] Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015.

следующие виды лиц, совершающих преступления в сфере компьютерной информации[1]:

– *исследователи* — немногочисленная категория, представители которой заняты исследованием возможностей и уязвимостей программного обеспечения;

– *взломщики* — лица, осуществляющие взломы компьютерных систем исходя из потребности в самовыражении и желания способствовать совершенствованию информационных технологий;

– *вандалы* — вторгаются в компьютерные системы с целью причинения ущерба, но при этом движимы не корыстными соображениями, а идейными, в частности, например, такими как выражение общественного протеста;

– *кракеры* (*крэкеры*) — специализируются на коммерческих взломах, то есть совершают вторжение с корыстными целями;

– *пираты* — осуществляют взлом защитных систем лицензионных продуктов, борясь за свободный доступ к информации, против ограничений копирайта и секретности данных, или преследуя корыстные мотивы;

– *кибертеррористы* — преступники, проникающие в компьютерные системы с целью нанести максимальный урон противнику;

– *санитары* — немногочисленная группа, убежденная, что порядок в Сети могут обеспечить сами пользователи; их деятельность направлена на искоренение сетевого вандализма и детской порнографии, которые они воспринимают как основную угрозу Интернета.

– *вирмейкеры* (*вексеры, технокрысы*) — программисты, специализирующиеся на создании компьютерных вирусов;

– *трейдеры* — сами не пишут вирусы, но коллекционируют их, обмениваясь экземплярами с другими трейдерами;

– *деструкторы* — создают программы-вандалы и вирусы, нацеленные на массовое уничтожение компьютеров;

– *кодеры* — новички, пробующие свои силы в написании вирусов;

кардеры — специализируются на махинациях с кредитными картами и банкоматами;

– *фрикеры* — действуют в области спутниковой и сотовой связи.

И, наконец, к числу *основных обстоятельств, способствующих совершению компьютерных преступлений*, можно отнести следующие:

1. Рост числа средств компьютерной техники, используемых в России и, как следствие этого, рост числа их пользователей, увеличение объемов информации, хранимой и обрабатываемой с помощью компьютеров.

2. Недостаточность мер по защите средств и систем компьютерной техники, недопонимание многими руководителями предприятий, организаций важности проблем обеспечения информационной безопасности, защиты информации.

3. Несовершенство используемого программного обеспечения с точки зрения обеспечения защиты информации, обрабатываемой с его помощью.

---

[1] Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015.

4. Несовершенство самих технических средств защиты информации.

5. Широкий выход российских пользователей в мировые информационные сети для обмена информацией.

6. Использование в преступной деятельности современных технических средств, в том числе и компьютерных.

7. Ошибки и небрежность в работе пользователей компьютеров.

Отмеченное предопределяет необходимость организации эффективной системы защиты информации, хранимой и обрабатываемой в информационных системах ОВД, адекватной существующим угрозам и способной обеспечить успешное решение стоящих перед правоохранительными органами задач.

4.3. Средства и способы защиты компьютерной информации от несанкционированного доступа

Для обеспечения защиты информации, обрабатываемой в современных компьютерных системах, используется целый комплекс организационных, программных, технических, технологических, правовых и, при необходимости, криптографических средств и мер.

Организационные средства защиты сводятся к регламентации доступа к информационным и вычислительным ресурсам, функциональным процессам систем обработки данных, к регламентации деятельности персонала и др. Их цель — в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Наиболее типичные организационные мероприятия включают в себя следующие меры:

– ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации;

– мероприятия по подбору персонала, связанного с обработкой данных в компьютерных системах;

– допуск к обработке и передаче конфиденциальной информации только тех сотрудников, которые имеют на то надлежащие полномочия;

– учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;

– организация защиты от установки прослушивающей аппаратуры в помещениях, связанных с обработкой информации;

– организация учета использования и уничтожения документов (носителей) с информацией ограниченного доступа;

– разработка должностных инструкций и правил по работе с компьютерными средствами и информационными массивами;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– использование сертифицированных средств защиты информации;

– использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;

– необходимое резервирование технических средств компьютерной системы;

– использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

– размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;

мразмещение объектов защиты на максимально возможном расстоянии относительно границы контролируемой зоны и др.

Программные средства защиты активнее и шире других применяются в современных компьютерных системах, реализуя такие функции защиты, как разграничение и контроль доступа к ресурсам; регистрация и анализ протекающих процессов, событий, пользователей; предотвращение возможных разрушительных воздействий на ресурсы; идентификация и аутентификация пользователей и процессов и др.

В настоящее время наибольший удельных вес в этой группе средств защиты информации составляют специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения.

Технические средства призваны создать некоторую физически замкнутую среду вокруг объекта и элементов защиты. В этом случае используется такие мероприятия, как:

– организация физической защиты помещений и собственно технических средств с помощью технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки;

– ограничение электромагнитного излучения путем экранирования помещений, где происходит обработка информации, листами из металла или специальной пластмассы;

– осуществление электропитания оборудования, обрабатывающего ценную информацию, от автономного источника питания или от общей электросети через специальные сетевые фильтры;

– применение, во избежание несанкционированного дистанционного съема информации, жидкокристаллических или плазменных дисплеев, струйных или лазерных принтеров соответственно с низким электромагнитным и акустическим излучением;

– использование автономных средств защиты аппаратуры в виде кожухов, крышек, дверец, шторок с установкой средств контроля вскрытия аппаратуры и др.

Технологические средства защиты информации — это целый комплекс мероприятий, которые включаются в качестве неотъемлемой составляющей в технологические процессы обработки данных в компьютерных системах. Среди них основными являются:

– сохранение обрабатываемых файлов во внешней памяти компьютера, осуществляемое в ручном или автоматическом режимах;

– регистрация пользователей средств компьютерной техники в журналах;

– автоматическая регистрация доступа пользователей к тем или иным ресурсам;

– создание архивных копий массивов и носителей информации;

– разработка специальных инструкций по выполнению всех технологических процедур и др.

Криптографические средства защиты предназначены для осуществления криптографического преобразования информации, обеспечивающего возможность ее прочтения (восстановления) только при знании определенной ключевой информации (ключа).

Безусловно, никакая криптография не способна защитить информацию от ошибочных действий персонала, пользователей компьютерных систем, от ее утечки по техническим каналам. Однако в случае, если речь идет о защите критически важной информации, а угрозой является реальный человек — злоумышленник и существует вероятность физического доступа злоумышленника к носителям этой информации, криптография является необходимым условием защиты компьютерной информации, поскольку шифрование данных делает бесполезными их хищение или несанкционированное копирование.

К правовым средствам защиты относятся правовые акты, в том числе и локальные, регламентирующие правила обращения с защищаемой информацией.

Здесь особо следует выделить руководящие документы Федеральной службы по техническому и экспортному контролю — ФСТЭК России (правопреемница Гостехкомиссии при Президенте РФ) и, в частности, такой руководящий документ, как «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»[1]. Данный документ определяет девять классов защищенности автоматизированных систем от несанкционированного доступа к информации. Выбор класса производится заказчиком и разработчиком с привлечением специалистов по защите информации. К числу определяющих признаков относятся:

– наличие в системе информации различного уровня конфиденциальности;

– уровень полномочий субъектов на доступ к конфиденциальной информации;

– режим обработки данных в системе — коллективный или индивидуальный.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в системе. В пределах каждой группы соблюдается иерархия требований к защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности автоматизированных систем.

Опыт показывает, что для обеспечения надежной защиты информации необходимо сочетание всех вышеперечисленных мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером по-

[1] См.: Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/296. — Загл. с экрана.

тенциальных и реальных угроз информации, наличием современных средств защиты. В общем случае технические меры защиты информации составляют незначительную часть от общих мер обеспечения информационной безопасности. Однако ни одну из них нельзя упускать, так как каждая мера дополняет другую и недостаток или отсутствие какой-либо из них приведет к нарушению защищенности информации.

Анализ ряда правовых актов ФСТЭК России[1] позволяет сформулировать минимально необходимый набор требований к защите информации в компьютерных системах:

1. Включить компьютер и загрузить операционную систему могут только зарегистрированные пользователи и только в разрешенное для каждого из них время.

2. Доступ к конфиденциальной информации и той информации, которая хранится на защищаемых носителях, должен предусматривать процедуру обязательной регистрации.

3. Пользователь, обрабатывающий конфиденциальные данные, должен иметь возможность удостовериться в неизменности системного и прикладного программного обеспечения, пользовательских данных, в отсутствии вредоносных программ.

4. Права по доступу к информации и возможностям ее обработки должны определяться функциональными обязанностями пользователя.

5. Пользователям при обработке защищаемой информации разрешается применение только тех программных средств, которые необходимы им для выполнения своих функциональных обязанностей.

6. Для хранения информации с ограниченным доступом должны использоваться только учтенные носители информации.

7. Конфиденциальная информация, обрабатываемая полномочным пользователем, без соответствующего разрешения не должна прямо или косвенно быть доступна иному субъекту.

8. Технология функционирования компьютерной системы должна предусматривать автоматическую регистрацию наиболее важных событий, связанных с доступом пользователей к защищаемой информации и компьютерной системе в целом.

9. При печати документов на бумажные носители автоматически должен фиксироваться факт распечатки в специальном журнале и автоматически выводиться соответствующий штамп на сам документ.

---

[1] См.: Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/296; Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/ download/297.

10. В компьютерной системе должен быть администратор безопасности, отвечающий за практическую реализацию принятой в организации политики безопасности.

При этом, все перечисленные требования должны обеспечиваться средствами самой компьютерной системы автоматически.

Приведенный набор требования далеко не полон. В общем случае основными способами защиты информации в компьютерных системах от несанкционированного доступа являются[1]:

– идентификация и аутентификация пользователей;
– ограничение доступа на вход в систему;
– разграничение доступа;
– регистрация событий (аудит);
– криптографическая защита;
– управление политикой безопасности;
– уничтожение остаточной информации;
– антивирусная защита.

Идентификация и аутентификация пользователей. Для того чтобы только зарегистрированный пользователь смог включить компьютер и получить доступ к хранящимся в компьютерной системе данным, процедура доступа осуществляется в три этапа: идентификация — аутентификация — авторизация.

Идентификация *— это присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов*[2]. Осуществление процедуры идентификации позволяет компьютерной системе определить пользователя, который в данный момент времени работает за компьютером или пытается его включить (осуществить вход в систему).

Аутентификация *— это проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности*[3]. Данная процедура позволяет компьютерной системе убедиться в том, что пользователь, представившийся каким-либо легальным сотрудником, таковым и является.

Авторизация *— предоставление пользователю полномочий в соответствии с политикой безопасности, установленной в компьютерной системе.*

---

[1] См.: Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие / науч. ред. д-р техн. наук, проф. Н.А. Гайдамакин. Екатеринбург: УГТУ-УПИ, 2008.

[2] См.: Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/298. — Загл. с экрана.

[3] См.: Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/298. — Загл. с экрана.

Конечной целью осуществления процедур идентификации и аутентификации является допуск субъекта (объекта) к обрабатываемой в компьютерной системе информации с ограниченным доступом, либо отказ в допуске в случае отрицательного исхода проверки. Объектами идентификации и аутентификации могут быть как люди (пользователи, обслуживающий персонал и др.), так и технические средства (рабочие станции, мониторы и т.д.), документы (ручные, распечатки и др.) и др. При этом установление подлинности субъекта (объекта) может производиться аппаратным устройством, программой или человеком.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

– индивидуального объекта заданного типа;

– знаний некоторой известной только ему и проверяющей стороне информации;

– индивидуальных биометрических характеристик.

К *первой группе* относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от несанкционированного доступа к средствам компьютерной техники.

Во *вторую группу* входят методы аутентификации, использующие пароли. Это наиболее широко распространенный метод аутентификации в современных компьютерных системах.

Пароль — это идентификатор субъекта доступа, который является его (субъекта) секретом[1]. С практической точки зрения пароль представляет собой некоторую секретную (известную только конкретному пользователю) последовательность символов, которую пользователь должен ввести с помощью устройства ввода информации для того, чтобы получить доступ к компьютерной системе.

По оценкам экспертов порядка 80% компьютерных взломов становятся возможными вследствие несовершенства парольной защиты компьютерных систем. В этой связи для обеспечения надежности механизма парольной защиты крайне важно придерживаться определенных правил:

1) пароль при вводе не должен отображаться на экране монитора, его нельзя записывать и хранить в местах, доступных посторонним лицам (на рабочем столе, под клавиатурой и т.д.);

2) длина пароля должна быть не менее 8 символов, чтобы избежать его взлома методом прямого перебора (наиболее надежные пароли состоят из 14 и более знаков);

3) при составлении пароля нельзя использовать распространенные слова и имена, а также информацию, связанную с личностью пользователя (его имя, фамилию, дату рождения, номер телефона и т.п.);

4) пароль должен содержать не только буквы, как прописные, так и строчные, но и цифры, а также различные специальные символы, причем, желательно, с изменениями раскладки клавиатуры;

---

[1] См.: Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/ download/298. — Загл. с экрана

5) каждый новый пароль должен значительно отличаться от паролей, использовавшихся ранее;

6) пароль должен периодически меняться, но изменения должны осуществляться не по графику, а случайным образом;

7) файл, в которым хранятся пароли пользователей компьютерной системы, должен иметь надежную защиту от несанкционированного доступа и, желательно, криптографическую защиту;

8) каждый пароль должен использоваться уникально — только одним пользователем и для получения доступа только к одной из систем или программ;

9) не следует использовать подсказки к паролям, предлагающие при задании пароля указать дополнительные сведения;

10) пароль не должен пересылаться по электронной почте, передаваться по телефону или по другим недостаточно надежно защищенным каналам связи.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с достаточно высокой точностью аутентифицировать обладателя конкретного биометрического признака, однако, как свидетельствует практика их применения, и обмануть их зачастую оказывается достаточно просто[1].

Ограничение доступа на вход в систему. Ограничение доступа к ресурсам компьютерной системы обеспечивается, прежде всего, принятием организационно-технических мер ограничения физического доступа несанкционированных пользователей к помещениям, в которых установлены и функционируют элементы компьютерной системы. Эта задача решается путем усиления инженерной защищенности помещений, установки систем охранной сигнализации, видеонаблюдения, устройств защиты рабочего места и т.д. Эти меры касаются ограничения доступа к элементам компьютерной системы как физическим объектам.

Применительно же непосредственно к функционированию компьютерной системы под ограничением доступа на вход в систему понимают, как правило, комплекс мер, выполняемых в процессе загрузки операционной системы[2]. Для обозначения процесса правильного и легального включения компьютера обычно используют термин «доверенная загрузка», под которой понимается загрузка строго определенной, не измененной операционной системы и только в том случае, если подтверждено, что в компьютере не произошло никаких несанкционированных изменений и что включает его именно тот пользователь, который имеет право на нем работать именно в это время[3].

---

[1] См.: Как обезопасить биометрические системы идентификации? [Электронный ресурс]. — Режим доступа: http://ru.euronews.com/2014/03/17/behind-the-mask-of-biometric-security. — Загл. с экрана.

[2] См.: Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие / науч. ред. д-р техн. наук, проф. Н.А. Гайдамакин. Екатеринбург: УГТУ-УПИ, 2008.

[3] См.: Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». М.: Радио и связь, 1999.

Одним из возможных способов обеспечения безопасного входа в компьютерную систему является операция ввода пароля BIOS при включении компьютера.

Базовая система ввода-вывода BIOS представляет собой набор базовых программ для проверки оборудования во время запуска, для загрузки операционной системы, а также для поддержки обмена данными между устройствами. BIOS хранится в энергонезависимом постоянном запоминающем устройстве (ПЗУ), благодаря чему ее программы могут быть выполнены при включении компьютера.

В установках BIOS можно установить два пароля — user password и supervisor password. Первый из них (user password) обеспечивает парольную защиту как начала загрузки BIOS, так и режима установки параметров (SETUP) BIOS, а второй (supervisor password) закрывает только режим установки параметров BIOS.

Основной недостаток данного способа — ненадежность защиты. Кратковременное отключение расположенного на материнской плате элемента питания CMOS-памяти BIOS, в которой хранится пароль BIOS, приведет к сбросу пароля. Кроме того, парольная система BIOS не обеспечивает идентификации конкретного пользователя. Также, существуют программы, предназначенные для извлечения паролей из CMOS-памяти.

Возможным решением данной проблемы является использование средств защиты информации, использующих собственный контроллер. Примером подобного рода средств может служить программно-аппаратный комплекс «Аккорд-АМДЗ», представляющий собой плату расширения, которая устанавливается в материнскую плату компьютера. Основным принципом работы «Аккорд-АМДЗ» является выполнение процедур, реализующих функции системы защиты информации, до загрузки операционной системы. Процедуры идентификации/аутентификации пользователя, контроля целостности аппаратных и программных средств, администрирования, блокировки загрузки операционной системы с внешних носителей информации размещены во внутренней памяти микроконтроллера платы «Аккорд». Таким образом пользователь не имеет возможности изменения процедур, которые влияют на функциональность системы защиты информации[1].

Разграничение доступа. Разграничение доступа осуществляется с целью предоставить каждому зарегистрированному в компьютерной системе пользователю возможность доступа к информации, обрабатываемой в компьютерной системе, и исключить возможность превышения пользователем предоставленных ему полномочий.

Выделяют две основные модели разграничения доступа: дискреционная и мандатная.

Дискреционное управление доступом *— это разграничение доступа между поименованными субъектами и поименованными объектами. Субъект*

[1] См.: СЗИ НСД «Аккорд-АМДЗ» [Электронный ресурс]. — Режим доступа: http://www.accord.ru/accord.html. — Загл. с экрана.

с определенным правом доступа может передать это право любому другому субъекту[1].

В рамках данной модели управление доступом осуществляется путем явной выдачи полномочий на проведение действий с каждым из объектов системы. Использование данной модели позволяет создать достаточно гибкую, но довольно сложную схему разграничения доступа, особенно в случае наличия значительного количества объектов и субъектов. Одним из возможных путей решения данной проблемы является группировка пользователей, когда права раздаются не отдельным пользователям, а группам пользователей. Для того, чтобы пользователь получил соответствующие разрешения, нужно просто добавить его в одну или несколько групп.

Расширением данного способа разграничения доступа является *изолированная* (или *замкнутая*) *программная среда*. При использовании *изолированной программной среды* права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту. Можно, например, разрешить обращаться к файлам с расширением .doc только программам Word, Word Viewer и WPview.

Мандатное управление доступом *— это разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности*[2].

Основная идея данной модели заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов. При использовании данной модели разграничения доступа существенно страдает производительность операционной системы, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтения/записи.

Регистрация событий (аудит). Данный способ предполагает автоматическую фиксацию в файле-журнале событий, которые могут представлять опасность для компьютерной системы. Основная цель регистрации подобного рода событий — фиксация информации, необходимой для расследования инцидентов, произошедших с применением компьютерной системы.

Так, например, в операционной системе Windows 10 предусмотрено автоматическое ведение журнала регистрации событий, связанных с безопасностью, которые делятся на успешные или закончившиеся с ошибкой. Они указывают, например, удалось ли пользователю войти в ОС Windows.

Криптографическая защита. Под ***криптографической защитой информации*** *понимается защита информации с помощью ее криптографического*

---

[1] См.: Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/298.

[2] См.: Там же.

преобразования[1]*, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий*.

Вообще, вопросами криптографической защиты информации занимается такая наука как ***криптология*** (от греч.: «*крипто*» — «*тайный*» и «*логос*» — *учение*), которая включает в себя два тесно связанных между собой направления: криптографию и криптоанализ.

Криптография изучает способы преобразования (шифрования) информации, предметом же изучения *криптоанализа* являются методы и способы вскрытия шифров.

Процесс *шифрования* заключается в проведении обратимых преобразований исходной (открытой) информации в некоторую, кажущуюся случайной, последовательность символов.

Основное понятие в криптографии — «шифр».

Под *шифром* понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Под *зашифрованием* информации понимается процесс преобразования открытой информации (исходного текста) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют *расшифровыванием* (дешифрованием)[2].

Обобщенную схему криптосистемы шифрования можно представить так, как это показано на рис. 4.1.

Исходный текст передаваемого сообщения (или хранимой информации) *M* зашифровывается с помощью криптографического преобразования *EK1* в результате чего получается зашифрованный текст *C*.

$$C = EK1 (M),$$

где K1 — параметр функции E, называемый ключом шифрования.

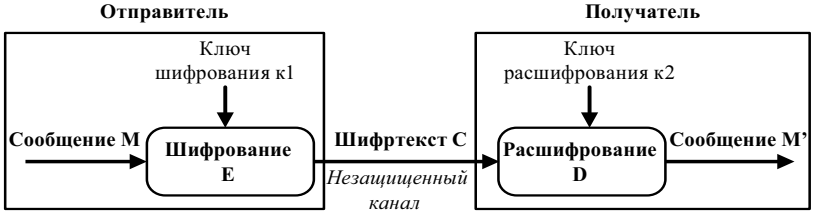


Рис. 4.1. Обобщеннная схема криптосистемы шифрования

[1] См.: Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие. М.; ИД «Форум»: ИНФРА-М, 2010. С. 87.

Шифртекст *C*, называемый еще криптограммой, содержит исходную информацию *M* в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования *k1*.

Ключ шифрования — последовательность символов, управляющая операциями шифрования и дешифрования[1], — является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

Обратное преобразование информации выглядит следующим образом:

$$M' = DK2\ (C)$$

Функция *D* является обратной к функции *E* и производит расшифрование шифртекста. Она также имеет дополнительный параметр в виде ключа *k2*. Ключ расшифрования *k2* должен однозначно соответствовать ключу *k1*. В этом случае полученное в результате расшифрования сообщение M' будет эквивалентно *M*. При отсутствии верного ключа *k2* получить исходное сообщение *M'= M* с помощью функции *D* невозможно[2].

За многовековую историю использования шифрования информации человечеством изобретено множество шифров, которые подразделяются на две основные группы: шифры перестановки и шифры замены.

Шифр перестановки изменяет порядок следования символов исходного сообщения. Это такие шифры, преобразования которых приводят к изменению только порядка следования символов открытого (исходного) сообщения.

Шифр замены меняет каждый символ на другой, не изменяя порядок их следования. Это такие шифры, преобразования которых приводят к замене каждого символа открытого сообщения на другие символы, причем порядок следования символов закрытого сообщения совпадает с порядком следования соответствующих символов открытого сообщения.

Таким образом, шифрование дает возможность преобразовать информацию так, что ее прочтение (восстановление) возможно только при знании ключа, который должен быть известен как отправителю сообщения, так и его законному получателю. Поэтому заранее, до обмена информацией, отправители сообщений и их получатели должны строго конфиденциально договориться об используемых шифрах и ключах.

---

[1] ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации» [Электронный ресурс]. — Режим доступа: http://docs.cntd.ru/document/1200007766. — Загл. с экрана.

[2] См.: Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. С. 112-113.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Соответственно различают два основных класса криптосистем[1]:

– симметричные;

– ассиметричные (с открытым ключом).

В *симметричных* криптосистемах и для зашифрования, и для расшифрования используется один и тот же ключ.

Недостаток симметричного шифрования — трудность распространения секретного ключа, который должен быть и у отправителя, и у получателя; приходится использовать отдельный закрытый канал передачи, например, курьерской почтой.

В *системах с открытым ключом* (*ассиметричных криптосистемах*) у каждого корреспондента есть два ключа: открытый и закрытый. Информация шифруется отправителем с помощью открытого ключа получателя, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптографическая защита информации широко используется в практической деятельности органов внутренних дел. Основное назначение ведомственной системы криптографической защиты информации — обеспечение криптографической защиты сведений, составляющих государственную тайну, а также информации ограниченного доступа, не относящейся к государственной тайне.

Целью развития системы криптографической защиты информации в органах внутренних дел является создание современной системы криптографической защиты информации на качественно новом технологическом уровне, функционирующей с использованием цифровых каналов связи, которая позволит обеспечить:

– устойчивость, безотказность и своевременность многофункционального защищенного информационного обмена между органами внутренних дел на всех уровнях управления МВД России;

– разграничение доступа пользователей к информационным ресурсам ограниченного доступа;

– качественный защищенный информационный обмен между органами внутренних дел и федеральными органами государственной власти, включая интеграцию информационно-телекоммуникационных систем органов внутренних дел в единую защищенную телекоммуникационную инфраструктуру для государственных нужд[2].

Управление политикой безопасности. Данный метод подразумевает осуществление различных настроек параметров компьютерной системы, которые позволяют установить в системе определенное состояние защищенности. В современных операционных системах он может быть реализован как через не-

---

[1] См.: Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. С. 113.

[2] См.: Концепция развития системы криптографической защиты информации в органах внутренних дел Российской Федерации до 2013 года (утв. приказом МВД России от 2 августа 2010 г. № 561) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

посредственное редактирование реестра операционной системы, так и с помощью специального инструмента «Локальная политика безопасности».

Так, например, настраиваемые параметры безопасности операционной системы Windows 10 включают следующие основные группы: политики учетных записей, локальные политики, брандмауэр Windows в режиме повышенной безопасности, политика диспетчера списка сетей, политики открытого ключа, политики ограниченного использования программ, политики управления приложениями, политики IP-безопасности на «Локальный компьютер», конфигурация расширенной политики аудита.

Уничтожение остаточной информации. В процессе обработки в компьютерной системе информации с ограниченным доступом в оперативной памяти, на магнитных носителях неизбежно образуются следы выполнения подобного рода операций, так называемый «технологический мусор». В этой связи в защищенных компьютерных системах предусматривается механизм своевременной и надежной очистки таких следов. Очистка производится путем записи маскирующей информации (последовательности случайных данных) в память при ее освобождении (перераспределении). Для борьбы с остаточной информацией современные средства защиты информации имеют в своем составе ряд специальных утилит, которые по запросу пользователя (например, после окончания работы с конфиденциальными документами) осуществляют очистку всех свободных областей жестких дисков, хвостов файлов и неиспользуемых каталогов.

Говоря о способах и средствах защиты информации в компьютерных системах, особо следует отметить проблему ***защиты компьютерных программ от несанкционированного копирования***, как одного из способов несанкционированного доступа к компьютерной информации.

Необходимо отметить, что по оценкам экспертов уровень использования нелицензионного программного обеспечения в России составляет порядка 62%. При этом, около 75% от всех нарушений авторских прав в области программного обеспечения составляет нелегальное копирование программ[1].

По данным IDC Russia потери российских организаций в связи с использованием вредоносного или нелицензионного программного обеспечения составляют 20 млрд долларов США. Из них 4,9 млрд долларов США тратится на выявление и решение проблем, связанных с использованием нелицензионного программного обеспечения, а потери на общую сумму 15 млрд долларов США связаны с утечками данных[2].

Наиболее распространенными формами незаконного копирования программ являются:

– установка на компьютер нелицензионной копии программы;

– установка программ на компьютеры в количестве, превышающем условия лицензионных соглашений.

---

[1] См.: Тенденции использования нелицензионного программного обеспечения в России [Электронный ресурс]. — Режим доступа: http://ww2.bsa.org/~/media/Files/Research%20Papers/ IDC/WhitePaperUnlicensedSoftwareUseTrendsRussia.ashx. — Загл. с экрана.

[2] Там же.

В целях защиты программного обеспечения от несанкционированного копирования используется целый комплекс мер организационного, правового и технического характера.

Основная идея *организационных мер защиты* заключается в том, что полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя: подробной пользовательской документации, «горячей линии», системы обучения пользователей, обновления версий со скидкой и т.п. Организационные меры защиты применяются, как правило, крупными разработчиками к достаточно большим и сложным программным продуктам.

Правовые меры защиты программного обеспечения заключаются в установлении юридической ответственности за использование нелицензионного программного обеспечения.

Так, в соответствии со ст. 1252 ГК РФ правообладатель может в судебном порядке потребовать возмещения убытков от лица, неправомерно использовавшего результат интеллектуальной деятельности.

Статья 7.12. Кодекса Российской Федерации об административных правонарушениях предусматривает административную ответственность за нарушение авторских и смежных прав, изобретательских и патентных прав. Согласно положениям данной статьи ввоз, продажа, сдача в прокат или иное незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода, если таковые являются контрафактными либо на них указана ложная информация, влечет наложение штрафа с конфискацией контрафактных экземпляров произведений и фонограмм, а также материалов и оборудования, используемых для их воспроизведения, и иных орудий совершения административного правонарушения.

Наступление уголовной ответственности за нелицензионное использование программного обеспечения законодатель связывает с причинением правообладателю крупного ущерба (более 100 тыс. рублей).

В соответствии с ч. 2 ст. 146 УК РФ незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенное в крупном размере, влечет одно из следующих наказаний:

– штраф в размере до 200000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев;

– обязательные работы на срок до 480 часов;

– исправительные работы на срок до 2-х лет;

– принудительные работы на срок до 2-х лет;

– лишение свободы на срок до 2-х лет.

Учитывая масштабы использования нелицензионного программного обеспечения следует признать явно недостаточную эффективность организационных и правовых мер защиты программного обеспечения. В этой связи особую значимость приобретают *технические методы защиты* компьютерных программ.

Можно выделить следующие наиболее распространенные способы защиты программного обеспечения от копирования.

Защита при помощи компакт-дисков. Суть данного метода заключается в привязке программного обеспечения к его носителю (CD- или DVD-дискам). Для защиты от копирования используется: запись информации в неиспользуемых секторах, проверка расположения и содержимого «сбойных» секторов, проверка скорости чтения отдельных секторов. В качестве дополнительной меры защиты в системе может устанавливаться специальный защищенный драйвер, призванный бороться с различными эмуляторами. Этот метод защиты сравнительно дешев и подходит для широко тиражируемых продуктов. К ограничениям можно отнести не самую высокую степень защиты и неудобство, вызванное привязкой к физическому носителю. Самые известные системы защиты по такой технологии: SecuROM, StarForce, SafeDisk, Tages[1].

Защита при помощи электронных ключей. Электронный ключ обычно представляет собой небольшое устройство, которое присоединяется к компьютеру через один из возможных интерфейсов (USB, LPT или COM). Он содержит ключевые данные, записанные в него разработчиком компьютерной программы. Защита программы основывается на том, что только ему (разработчику) известен полный алгоритм работы ключа.

Программа в начале и в ходе выполнения считывает контрольную информацию из ключа. При отсутствии ключа выполнение программы блокируется.

Одним из основных достоинств защиты программных средств с использованием электронных ключей является то, что ключ можно вставлять в любой компьютер, на котором необходимо запустить программу.

Привязка к параметрам компьютера и активация. Данный способ защиты предполагает привязку программного обеспечения к информации о пользователе и (или) конфигурации компьютера и последующую интернет-активацию программного обеспечения. Данный метод защиты компьютерных программ получил в настоящее время наиболее широкое распространение, поскольку многие ведущие производители программного обеспечения отказались от распространения своей продукции на физических носителях и перешли к цифровой дистрибуции.

Суть данного метода защиты заключается в том, что приложение вычисляет параметры оборудования, на которое оно установлено (серийные номера материнской платы, процессора и т.д.), и в зашифрованном виде пересылает их на сервер активации. После получение ключа активации программа готова к работе, но оказывается привязанной к «железу» — конкретному компьютеру, на который она установлена. В качестве привязки используются, в основном, серийный номер BIOS материнской платы, серийный номер винчестера. В целях сокрытия от пользователя данные о защите могут располагаться в неразмеченной области жесткого диска.

Достоинство данного метода защиты заключается в том, что не требуется никакого специфического аппаратного обеспечения, программу можно распространять посредством цифровой дистрибуции (по сети Интернет).

---

[1] См.: Современные технологии защиты ПО от нелегального копирования: что выбрать разработчику? [Электронный ресурс]. — Режим доступа: http://www.itsec.ru/articles2/ Oborandteh/sovremennie-tehnologii-zashiti-po-ot-nelegalnogo-kopirovaniya-chto-vibrat-razrabotchiky. — Загл. с экрана.

Основной недостаток заключается в том, что программное обеспечение становится неработоспособным в случае, если пользователь производит модернизацию компьютера (если привязка осуществляется к аппаратной конфигурации компьютера).

Защита программ от копирования путем переноса их в онлайн. подразумевает, что код программы расположен и исполняется на сервере, доступном в глобальной сети, а доступ к программе осуществляется по принципу тонкого клиента.

Обфускация кода. Как известно, компьютерная программа — это набор инструкций для компьютера, которые он должен выполнить для решения определенной задачи. Программа пишется на языке программирования и компилируется в машинный код — язык конкретного компьютера. Сама по себе компиляция в машинный код — это достаточно неплохая защита, однако всегда существует вероятность того, что злоумышленник сможет при наличии времени и сил воспроизвести исходный код программы, то есть произвести своего рода обратную трансляцию. Возможным решением данной проблемы является использование технологий обфускации (запутывания) кода.

Обфускация кода — приведение исходного текста или исполняемого кода компьютерной программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции. Для создания запутанного текста программы могут использоваться специализированные компиляторы, использующие неочевидные или недокументированные возможности среды исполнения программы. Существуют также специальные программы, производящие обфускацию, называемые обфускаторами.

Безусловно, использование рассмотренных методов и средств защиты компьютерной информации от несанкционированного доступа способно значительно снизить риски реализации угроз безопасности информации в компьютерных системах. Однако, ввиду широкого использования сетевых технологий в практической деятельности органов внутренних дел, особое значение приобретает проблема антивирусной защиты компьютерных систем.

4.4. Антивирусная защита компьютерных систем

Переживаемая человечеством информационная революция не только ускоряет развитие цивилизации, но и порождает новые угрозы безопасности личности, общества и государства. К числу этих угроз следует отнести и такое явление, как криминализация современного информационного пространства. Особую актуальность данный вопрос приобретает в связи с появлением и бурным развитием сетевых информационных технологий, в том числе глобальной электронной сети Интернет.

Данные обстоятельства позволяют констатировать неуклонно возрастающий уровень опасности в сфере информационных технологий. По результатам опроса, проведенного специалистами Лаборатории Касперского, за последний год 96% отечественных компаний сталкивались с угрозами информационной

безопасности[1]. Результаты проведенного исследования свидетельствуют о том, что наибольшую опасность для корпоративных информационных систем представляет вредоносное программное обеспечение (компьютерные вирусы, шпионское программы и др.). Второе место — спам, на третьем — фишинговые атаки. За ними идут сбои, вызванные проникновением в корпоративную сеть, и DDoS-атаки.

Также материалы исследования свидетельствуют о том, что представители отечественных компаний хорошо осведомлены об уровне опасности, однако степень защищенности организаций от киберугроз оставляет желать лучшего.

Самые популярные меры, применяемые для защиты от киберугроз в компаниях в мире и в России, — антивирусная защита, клиентские межсетевые экраны, установка обновлений и резервное копирование данных. Тем не менее, 31% компаний в России не полностью внедрили антивирусную защиту. Одна российская компания из ста не имеет вообще никакой защиты (а в мире — 3% организаций).

Таким образом, следует констатировать, что риски, связанные с воздействием на корпоративные информационные системы различного рода вредоносного программного обеспечения, являются одной из наиболее актуальных угроз в сфере информационной безопасности, о чем со всей очевидностью свидетельствуют и данные статистики: ведущими разработчиками антивирусного программного обеспечения в 2014 году было заблокировано 6167233068 вредоносных атак на компьютеры и мобильные устройства пользователей, зафиксировано 123054503 совершенно уникальных вредоносных объектов, не встречавшихся ранее. В России с веб-атаками столкнулся каждый второй пользователь (53,7%)[2]. При этом большинством экспертов в сфере IT-технологий прогнозируется увеличение в течение ближайших нескольких лет роста числа атак на информационные системы, связанных с использованием вирусов, червей и других вредоносных программ. Понимание той опасности, которую представляет вредоносное программное обеспечение, обусловило повышенное внимание к организации эффективной антивирусной защиты корпоративных информационных систем.

По мере нарастания темпов развития компьютерных технологий каждый год появляются тысячи новейших вредоносных программ, не имевших аналогов ранее, либо коренным образом изменившихся. Но у значительного большинства таких программ в сущности можно выделить нечто общее, объединяющее их в определенный вид. Условно специалисты Лаборатории Касперского подразделяют вредоносные программы на следующие основные группы: компьютерные вирусы, черви, трояны, другие вредоносные программы (рис. 4.2).

---

[1] См.: Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс]. — Режим доступа: http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf. — Загл. с экрана.

[2] См.: Кривенцов П.А. Латентная преступность в России: криминологическое исследование: дисс. … канд. юрид. наук. М., 2014.

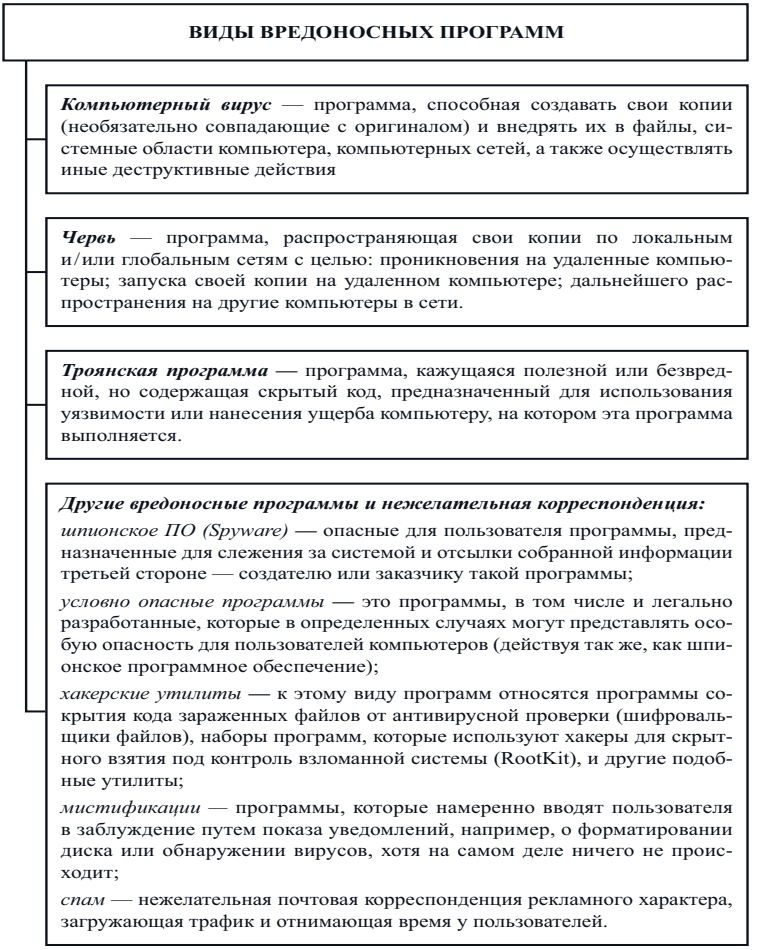


Рис. 4.2. Виды вредоносных программ

Компьютерный вирус — это программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия.

В отличие от вирусов, *сетевые черви* — это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению.

Троянская программа имеет только одно назначение — нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения

работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Кроме вирусов, червей и троянов существует еще много других вредоносных программ и нежелательной корреспонденции. Среди них можно выделить следующие группы: шпионское ПО (Spyware), условно опасные программы, хакерские утилиты, мистификации, спам.

По оценкам экспертов[1] среди источников проникновения вредоносных программ на компьютер наиболее опасными являются:

– Интернет;
– электронная почта;
– уязвимости в программном обеспечении;
– внешние носители информации;
– пользователи.

Интернет

Глобальная информационная сеть является основным источником распространения любого рода вредоносных программ. Достаточно сказать, что лишь в 2014 году решениями «Лаборатории Касперского» было отражено 1432660467 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.

При использовании сети Интернет зловредное программное обеспечение может попасть на компьютер при следующих действиях пользователя:

– при посещении сайта, содержащего зловредный код;
– при скачивании с сайтов зловредного программного обеспечения, маскирующегося под кейгены, крэки, патчи и т.д.;
– при скачивании через peer-to-peer сеть (например, торренты).

Электронная почта

Почтовые сообщения, поступающие в почтовый ящик пользователя и хранящиеся в почтовых базах, могут содержать в себе вирусы. Вредоносные программы могут находиться как во вложении письма, так и в его теле. При открытии письма, при сохранении на диск вложенного в письмо файла вы можете заразить данные на компьютере. Также почтовая корреспонденция может стать источником еще двух угроз: спама и фишинга. Если спам влечет за собой в основном потерю времени, то целью фишинг-писем является конфиденциальная информация пользователя компьютера.

Уязвимости в программном обеспечении

Так называемые «дыры» (эксплойты) в программном обеспечении являются основным источником хакерских атак. Уязвимости позволяют получить хакеру удаленный доступ к компьютеру, а следовательно, к хранящимся на нем данным, к ресурсам локальной сети, к другим источникам информации.

Внешние носители информации

В настоящее время для передачи информации по-прежнему широко используются съемные диски, карты расширения памяти, а также сетевые папки. Запуская какой-либо файл, расположенный на внешнем носителе, можно заразить вирусом хранящиеся на компьютере данные, распространить вирус на другие компьютеры, сети.

---

[1] См.: Лаборатория Касперского. О вирусах: Основные источники проникновения угроз на компьютер [Электронный ресурс]. — Режим доступа: http://support.kaspersky.ru/ viruses#block2. — Загл. с экрана.

Пользователи

Нередко сами пользователи сами устанавливают безобидные на первый взгляд программы, заражая таким образом свой компьютер. Этот метод называется социальной инженерией. С помощью него создатели вредоносных программ могут убедить излишне доверчивого пользователя запустить инфицированный файл или открыть ссылку на зараженный веб-сайт.

Таким образом, несложно заметить, что наибольшие риски, с точки зрения обеспечения информационной безопасности корпоративных систем, несет в себе онлайн активность сотрудников. Ее наиболее опасные виды в рассматриваемом контексте приведены в таблице 1[1].

Таблица 1

Наиболее опасные виды онлайн-активности сотрудников с точки зрения информационной безопасности

Вид активности/Приложение	В целом	США	Россия	Китай
Общий доступ к файлам/P2P	55%	62%	50%	44%
Социальные сети	35%	44%	52%	26%
Загрузка файлов, передача файлов, FTP-сервисы	34%	33%	44%	28%
Доступ к веб-сайтам	32%	35%	42%	29%
Личная электронная почта/веб-почта	31%	36%	22%	28%
Службы мгновенного обмена сообщениями	23%	20%	19%	36%
Онлайн-игры	21%	19%	16%	21%
Потоковое видео/Интернет-ТВ	13%	8%	12%	21%
Сетевой подход в маркетинге	11%	5%	4%	24%
Голосовая связь по IP-протоколу (VoIP)	10%	5%	9%	17%

Самыми эффективными средствами защиты от вирусов являются *специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах*. Такие программы называются ***антивирусами***.

В современных антивирусных продуктах используется два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический.

Сигнатурные методы *— это точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.*

Проактивные/эвристические методы *— приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.*

[1] Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс]. — Режим доступа: http://www.kaspersky.ru/downloads/ pdf/kaspersky_global_it_security_risks_survey.pdf. — Загл. с экрана.

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами.

Главные критерии эффективности сигнатурного метода — это скорость реакции на новые угрозы, частота обновлений, максимальное число обнаруженных угроз. Главный недостаток сигнатурного метода — задержка при реакции на новые угрозы.

Этот недостаток традиционного сигнатурного анализа позволяет преодолеть проактивная антивирусная защита.

Существует несколько подходов к проактивной защите. Рассмотрим два наиболее популярных подхода: эвристические анализаторы и поведенческие блокираторы.

Эвристический анализатор (*эвристик*) — это программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным.

Достоинствами статического анализа являются простота реализации, высокая скорость работы, возможность обнаружения новых, неизвестных вирусов еще до того, как для них будут выделены сигнатуры. Однако уровень обнаружения новых вредоносных кодов остается довольно низким, а вероятность ложных срабатываний — высокой.

Поведенческий блокиратор — это программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия: удаление файла, запись в файл и др. Выполнение каждого такого действия по отдельности не дает повода считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, значит эта программа по меньшей мере подозрительна.

Поведенческий блокиратор может предотвратить распространение как известного, так и неизвестного (написанного после создания блокиратора) вируса, что является неоспоримым достоинством такого подхода к защите. Недостатком поведенческих блокираторов остается срабатывание на действия ряда легитимных программ.

Для оптимальной антивирусной защиты необходимо сочетание проактивных и сигнатурных подходов.

В настоящее время на отечественном рынке присутствует достаточно большое количество как российских, так и зарубежных продуктов обеспечения антивирусной защиты информационных систем. Крупнейшим производителем решений для защиты конечных устройств в пользовательском и корпоративном сегментах в России является «Лаборатория Касперского», в активе которой значится 55,5% рынка. Продукты компании ESET занимают порядка 26% рынка, а вендоры Symantec, Dr. Web, TrendMicro и McAfee — около 20%[1].

Рассмотрим в общих чертах основные решения в области антивирусной защиты корпоративных информационных систем лидеров отечественного рынка — «Лаборатории Касперского» и компании ESET.

Лаборатория Касперского

«Лаборатория Касперского» выпускает широкий спектр решений для обеспечения надежной защиты от вирусов, спама и хакерских атак. В контексте настоящего исследования наибольший интерес представляет линейка Kaspersky

[1] См.: Российский рынок антивирусов находится в стагнации [Электронный ресурс]. — Режим доступа: http://www.dailycomm.ru/m/29960/. — Загл. с экрана.

Security для бизнеса позволяет выбрать именно то решение, которое нужно вашей организации, чтобы вы могли контролировать рабочие места (от рабочих станций до смартфонов и виртуальных машин), серверы и интернет-шлюзы и обеспечить их надежной защитой. Единая консоль управления Kaspersky Security Center позволяет централизованно управлять безопасностью всей вашей IT-инфраструктуры удаленно линейка «Kaspersky Security для бизнеса», позволяющая выбрать оптимальное решение для контроля рабочих мест, серверов и интернет-шлюзов и обеспечения их надежной защитой.

Продукты линейки Kaspersky Security для бизнеса обеспечивают антивирусную защиту, контроль использования устройств, приложений и веб-ресурсов, предоставляют инструменты шифрования и системного администрирования. В него также входят средства управления мобильными устройствами и создания политик безопасности. Управление защитой осуществляется из единого центра.

Технологии антивирусной защиты рабочих станций и сетевой экран образуют единый уровень защиты, формируя первый — СТАРТОВЫЙ — уровень защитного решения Kaspersky Endpoint Security для бизнеса СТАРТОВЫЙ.

В СТАНДАРТНЫЙ уровень защиты, помимо возможностей СТАРТОВОГО уровня, в список защитных функций включены технологии контроля программ и белые списки, контроль устройств и веб-контроль. Кроме них, в этот уровень входит защитное решение для мобильных устройств, состоящее из решения для защиты конечных точек и средства управления мобильными устройствами (смартфонами и планшетами) — Mobile Device Management (MDM).

Помимо возможностей, предусмотренных СТАНДАРТНЫМ уровнем защиты, в РАСШИРЕННЫЙ уровень включена технология шифрования данных, обеспечивающая возможность шифрования как отдельных файлов и папок, так и всего диска.

Еще одна новая функция в составе уровня РАСШИРЕННЫЙ, обеспечивающая более высокий уровень безопасности и эффективности IT-инфраструктуры — Kaspersky Systems Management.

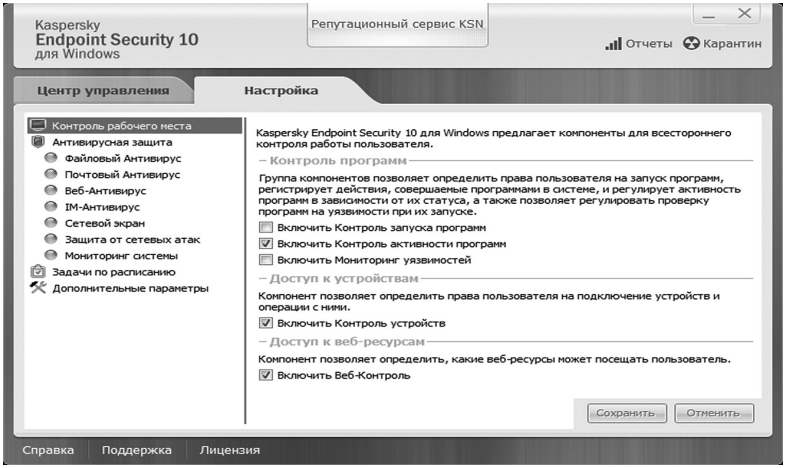


Рис. 4.3. Интерфейсное окно Kaspersky Endpoint Security 10

Kaspersky Systems Management включает несколько функциональных модулей: развертывание операционных систем, удаленная установка программного обеспечения и устранение неполадок, поддержка Microsoft Wsus и Wake-on-lan, управление лицензиями, учет программного и аппаратного обеспечения, мониторинг уязвимостей, управление установкой исправлений, контроль доступа в сеть (Nac).

Все эти технологии составляют решение Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ.

И, наконец, в максимальный уровень защиты — Kaspersky Total Security — добавлено разработанное «Лабораторией Касперского» решение для защиты серверов совместной работы, а также продукты компании для защиты почтовых серверов и интернет-шлюзов.

ESET

В настоящий момент компания предлагает корпоративным пользователям несколько вариантов решений для защиты корпоративной IT-инфраструктуры, отличающихся лишь набором функциональных компонентов. Наиболее полным решением является NOD32 Secure Enterprise — кроссплатформенный комплекс решений для информационной защиты всех узлов корпоративной инфраструктуры: рабочих станций, мобильных устройств, файловых и почтовых серверов, а также HTTP- и FTP-шлюзов. Вся система безопасности централизованно управляется с помощью консоли ESET Remote Administrator.

Для защиты корпоративных мобильных устройств предназначены решения Endpoint Security для Android и Mobile Security. Они не только защищают устройства от мобильных угроз, но и позволяют администратору блокировать нежелательные SMS и MMS, а также (с помощью «черных» и «белых» списков) ограничивать как входящие, так и исходящие вызовы.

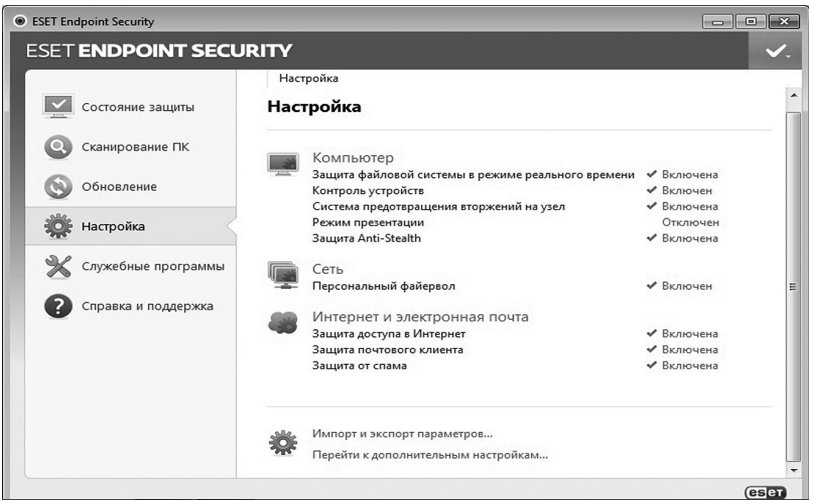


Рис. 4.4. Интерфейсное окно ESET Endpoint Security

Для защиты файловых серверов компании, в зависимости от используемой платформы, предназначены ESET File Security для Microsoft Windows Server и ESET File Security для Linux / BSD / Solaris. Эти решения были оптимизированы для работы в серверных средах.

Помимо этого, комплекс ESET NOD32 Secure Enterprise предлагает ряд решений для защиты почтовых серверов на всех возможных платформах, а также защиту на уровне HTTP- и FTP-шлюзов.

Вся система безопасности управляется с помощью консоли ESET Remote Administrator. Этот инструмент позволяет централизованно разворачивать, настраивать и администрировать решения ESET NOD32 в корпоративных средах любой сложности и разветвленности, обеспечивая работу всех защитных механизмов на всех узлах корпоративной ИТ-инфраструктуры.

Рассмотрев лидеров отечественного рынка антивирусного программного обеспечения, нельзя не упомянуть и такое антивирусное решение, как **Dr.Web Enterprise Security Suite**. Оно представляет несомненный интерес тем, что, наряду с продукцией «Лаборатории Касперского», является полностью отечественным программным продуктом, что в современных условиях представляется крайне важным с учетом реализуемого в России курса на импортозамещение, в том числе и в сфере информационных технологий.

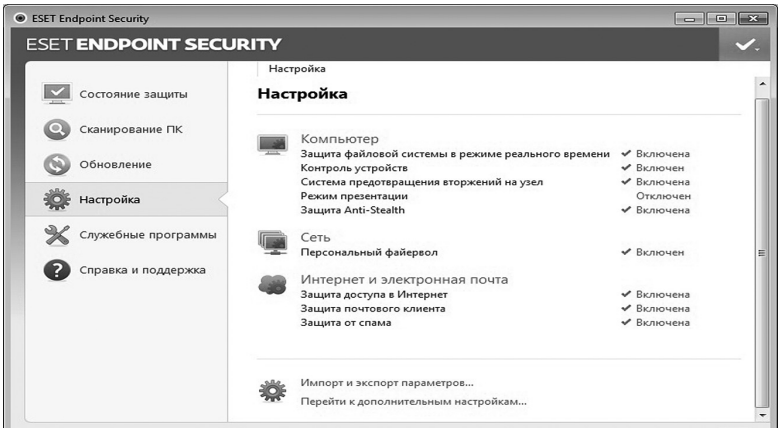


Рис. 4.5. Интерфейсное окно Dr.Web Enterprise Security Suite

– рабочих станций, клиентов терминальных серверов и клиентов встроенных систем;

– файловых серверов и серверов приложений (включая терминальные серверы);

– почтовых серверов;

– интернет-шлюзов;

– мобильных устройств.

Рассмотренные продукты не исчерпывают всего многообразия современного рынка антивирусного программного обеспечения. Однако выбор того или ино-

го программного решения в каждом конкретном случае определяется, прежде всего, спецификой той информационной системы, защиту которой он должен обеспечивать.

В марте 2012 года МВД России была разработана концепция создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Создание ИСОД пришло на смену проекту по созданию единой информационно-телекоммуникационной системы (ЕИТКС) органов внутренних дел, которое велось с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений органов внутренних дел с другими правоохранительными органами и госорганами различных уровней.

ИСОД ОВД представляет собой совокупность используемых в Министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и комплексов программно-технических средств, а также систем связи и передачи данных, необходимых для эффективного обеспечения служебной деятельности МВД России.

Современная антивирусная защита, обеспечивающая безопасность в сложных распределенных информационных системах, таких как ИСОД ОВД, требует своевременной реакции на возникающие угрозы со стороны вредоносного программного обеспечения. Помимо этого, указанная подсистема должна быть централизованно-управляемой и динамически подстраиваемой под требования и изменения, возникающие на всех этапах жизненного цикла ИСОД.

Согласно положений разработанной в 2012 году Базовой модели нарушителя и модели угроз единой системы информационно-аналитического обеспечения деятельности МВД России с учетом особенностей «облачной архитектуры», для использования в ИСОД ОВД средства антивирусной защиты должны быть сертифицированы в соответствии с утвержденными приказом ФСТЭК Росси от 20 марта 2012 г. № 28 «Требованиями к средствам антивирусной защиты», соответствующими методическими документами ФСТЭК России — профилями защиты, правовыми актами ФСБ России.

В соответствии с вышеупомянутыми требованиями выделяют следующие типы средств антивирусной защиты[1]:

тип «А» — средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах);

тип «Б» — средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на серверах информационных систем;

тип «В» — средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автоматизированных рабочих местах информационных систем;

[1] См.: Требования к средствам антивирусной защиты (утв. Приказом ФСТЭК Росси от 20 марта 2012 г. № 28) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/ attachments/download/402. — Загл. с экрана.

тип «Г» — средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автономных автоматизированных рабочих местах.

Средства антивирусной защиты типа «А» не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и(или) «В».

Примерная схема построения антивирусной защиты в информационной системе с применением средств антивирусной защиты разных типов приведена на рисунке 4.6.

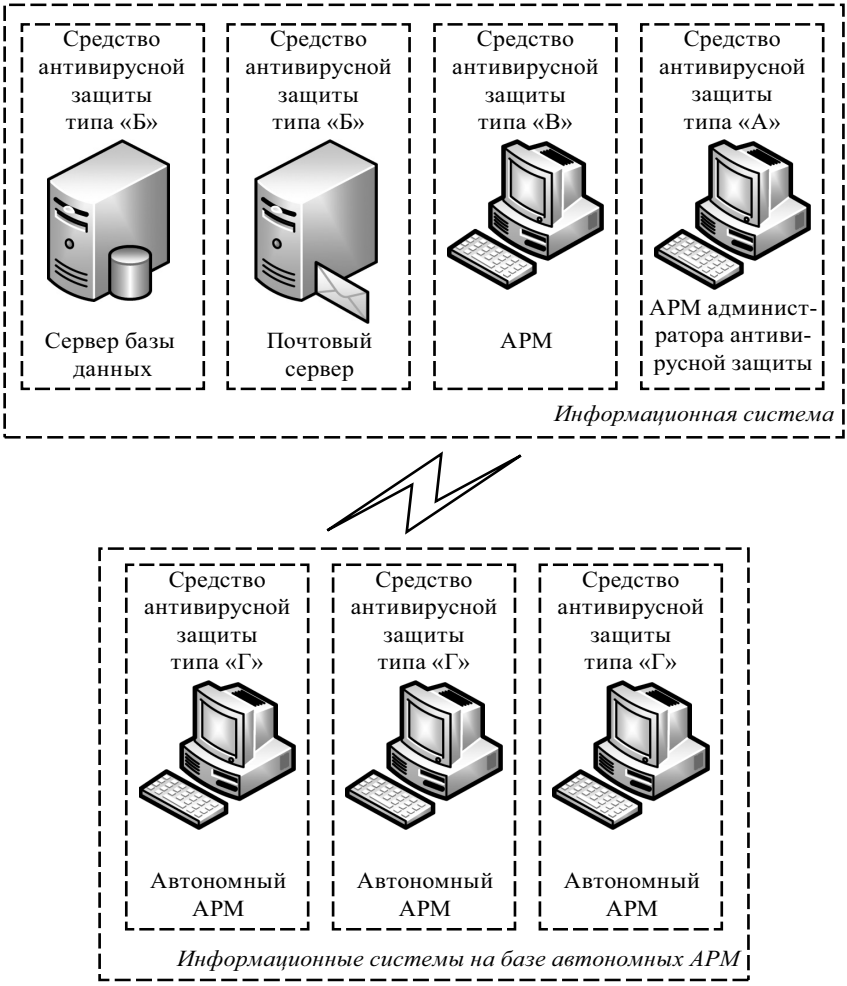


Рис. 4.6. Примерная схема построения антивирусной защиты в информационной системе с применением средств антивирусной защиты разных типов

Для дифференциации требований к функциям безопасности средств антивирусной защиты выделяются шесть классов защиты средств антивирусной защиты. Самый низкий класс — шестой, самый высокий — первый.

С учетом классификации средств антивирусной защиты, структуры ИСОД ОВД и циркулирующей в ней информации, наиболее походящими являются средства, соответствующие 4 классу защиты, применяемые в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Проведенный анализ отечественного рынка антивирусных средств при построении подсистемы антивирусной безопасности ИСОД ОВД позволяет сделать выбор в пользу программных продуктов «Лаборатории Касперского», особо принимая во внимание и то обстоятельство, что номенклатура данной компании присутствует в Государственном оборонном заказе и предусматривает поставку средств антивирусной защиты для нужд ОВД.

Система антивирусной защиты «Kaspersky Endpoint Security 10 для Windows» имеет соответствующий сертификат соответствия ФСТЭК России и содержит эффективные инструменты контроля выполнения корпоративных политик безопасности на уровне использования программ, внешних устройств и веб-ресурсов. Эти инструменты снижают риск заражения корпоративной сети, позволяют повысить производительность труда и предотвратить утечку конфиденциальной информации.

Структурно подсистема антивирусной защиты в ИСОД ОВД, как представляется, должна носить централизованный характер. Иными словами, она должна предусматривать наличие единой консоли администрирования, позволяющей эффективно управлять различными аспектами безопасности IT-инфраструктуры. В качестве такого инструмента можно выделить Kaspersky Security Center.

Инструмент управления антивирусной защитой Kaspersky Security Center позволяет удаленно устанавливать программные решения на рабочие станции и серверы, настроить параметры защиты, управлять обновлениями ПО и антивирусных баз, контролировать статус защиты и оперативно реагировать на события. Такие инструменты, как централизованный поиск уязвимостей, поддержка виртуальных сред и иерархическое управление делают управление системой защиты эффективным.

В единой консоли осуществляется управление безопасностью и защита от известного и нового вредоносного программного обеспечения, что позволяет предотвращать риски безопасности и снижает издержки на подсистему антивирусной защиты.

В соответствии с возможностями KSC структура построения подсистемы антивирусной защиты в ИСОД ОВД может выглядеть следующим образом (рис. 4.7).

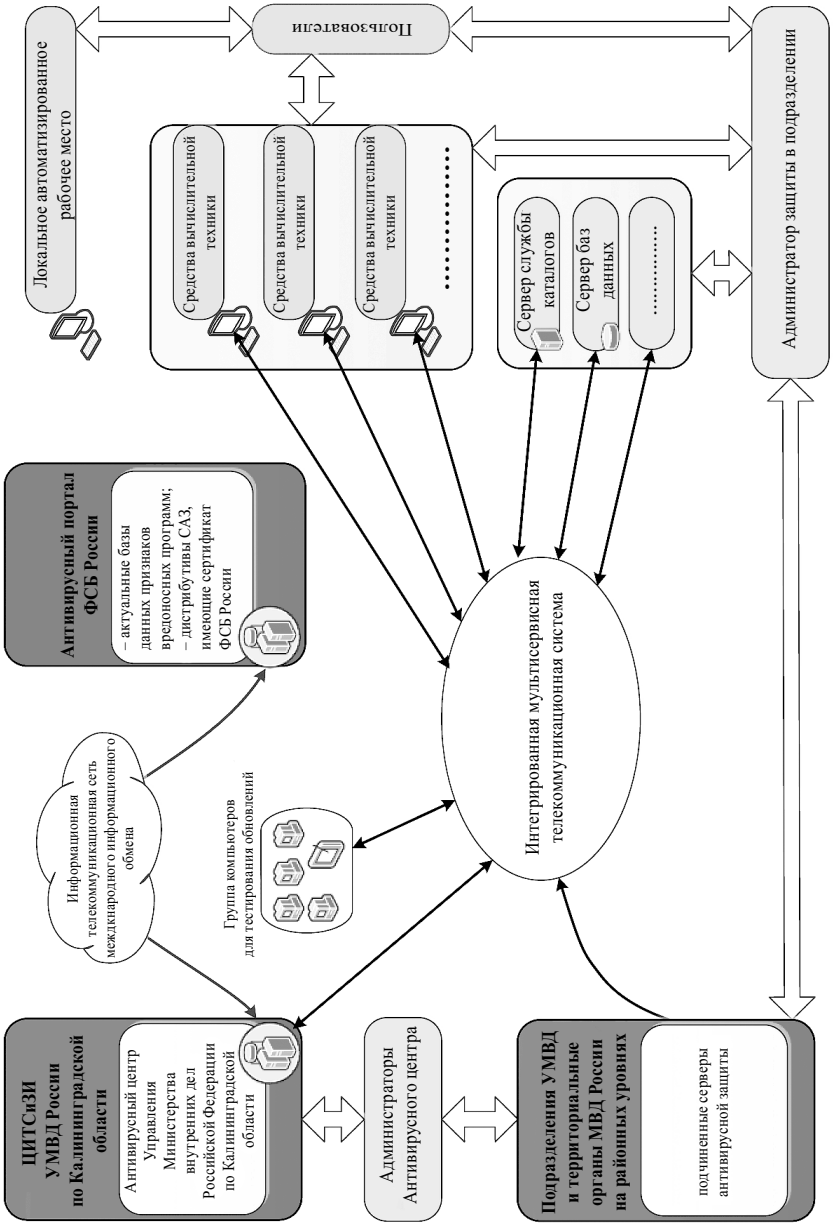


Рис. 4.7. Структура подсистемы антивирусной защиты в ИСОД ОВД

На 1-ом уровне, в соответствии с архитектурой ИСОД ОВД, располагается Антивирусный центр МВД России, который формирует основные политики безопасности, осуществляет распространение ключевых файлов и общее управление подсистемой антивирусной безопасности.

Одновременно с этим Антивирусный центр МВД России, посредством Антивирусного центра ФСБ России, осуществляет формирование верифицированных вирусных баз обновления и последующую их передачу на подчиненные антивирусные центры (2-ой и 3-ий уровень).

Указанные центры осуществляют общий контроль и управление на заданных уровнях.

Как представляется, описанная структура подсистемы антивирусной защиты в единой системе информационно-аналитического обеспечения деятельности МВД России способна обеспечить своевременную защиту от вирусных угроз, единой контроль и управление, успешную реакцию на возникающие инциденты. Однако, для обеспечения заданного уровня информационный безопасности в ИСОД ОВД, необходимо создание интегративной системы, объединяющей основные компоненты системы безопасности.

Рассмотрев вопросы защиты информации в компьютерных системах органов внутренних дел, подведем некоторые итоги.

Интенсивная информатизация правоохранительной сферы общества помимо очевидных преимуществ, порождает и новые вызовы безопасности информации, используемой в деятельности органов внутренних дел. Тревожной тенденцией в сфере кибербезопасности является рост количества атак на российские информационные ресурсы, активизация деятельности иностранных разведок по внедрению в информационные системы органов государственной власти Российской Федерации своих программных средств.

Наиболее распространенным видом нарушения безопасности информации в компьютерных системах является несанкционированный доступ, суть которого состоит в получении пользователем (нарушителем) доступа к объекту в нарушение установленных в организации правил работы с информацией. При этом, несанкционированный доступ к компьютерной системе может быть осуществлен как штатными средствами компьютерной системы, так и специально созданными аппаратными и программными средствами. Наиболее распространенными способами осуществления несанкционированного доступа являются: перехват пароля, подбор пароля, компрометация пароля, маскарад, незаконное использование привилегий, использование вредоносных программ.

Ввиду той опасности, которую представляет совершение неправомерных действий в отношении компьютерных систем и компьютерной информации, действующее уголовное законодательство Российской Федерации предусматривает ответственность за совершение преступлений в сфере компьютерной информации (глава 28 Уголовного кодекса Российской Федерации).

Сопоставление компьютерных преступлений с другими составами правонарушений, предусмотренных уголовным кодексом, позволяет выделить их следующие отличительные особенности: высокая скрытность (латентность), сложность сбора улик по установленным фактам; сложность доказательства в суде подобных дел; «интернациональность» компьютерных преступлений; вы-

сокий ущерб даже от единичного преступления; вполне определенный контингент лиц, совершающих правонарушения в сфере компьютерной информации.

Для обеспечения защиты информации, обрабатываемой в современных компьютерных системах, используется целый комплекс организационных, программных, технических, технологических, правовых и, при необходимости, криптографических средств и мер. Основными способами защиты информации в компьютерных системах от несанкционированного доступа являются: идентификация и аутентификация пользователей, ограничение доступа на вход в систему, разграничение доступа, регистрация событий (аудит), криптографическая защита, управление политикой безопасности, уничтожение остаточной информации, антивирусная защита. Последнее в настоящее время приобретает все большую значимость ввиду того, что риски, связанные с воздействием на корпоративные информационные системы различного рода вредоносного программного обеспечения, являются одной из наиболее актуальных угроз в сфере информационной безопасности.

Контрольные вопросы

1. Что понимается под угрозой безопасности информации в компьютерной системе?
2. В чем заключаются угрозы нарушения целостности, доступности и конфиденциальности компьютерной информации?
3. Перечислите случайные и преднамеренные угрозы безопасности компьютерной информации.
4. Что понимается под несанкционированным доступом к компьютерной информации?
5. Перечислите основные способы несанкционированного доступа к компьютерной информации.
6. Охарактеризуйте наиболее распространенные приемы и способы несанкционированного доступа к компьютерной информации.
7. В чем состоит сущность организационных мер защиты информации в компьютерных системах?
8. Что понимается под аутентификацией и идентификацией пользователей компьютерных систем?
9. Охарактеризуйте криптографические методы защиты компьютерной информации.
10. В чем заключаются различия избирательной (дискреционной) модели разграничения доступа к информации в компьютерной системе от полномочной (мандатной)?

5. ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

5.1. Информационно-телекоммуникационные системы как объект защиты

Информационно-телекоммуникационная система *— организационно-техническая система, реализующая определенную технологию обработки информации (информационную технологию) и объединяющая совокупность программно-аппаратных средств, предназначенных для обработки информации, обмена информацией и взаимодействия между компонентами, физическую среду, персонал и обрабатываемую информацию*[1].

Информационная составляющая информационно-телекоммуникационной системы (*ИТС*) — программно-аппаратные средства, предназначенные для обработки информации, а также сама обрабатываемая информация.

Телекоммуникационная составляющая ИТС — программно-аппаратные средства, предназначенные для обмена информацией и взаимодействия между компонентами.

Технической основой функционирования подавляющего большинства современных ИТС являются компьютерные сети.

В информатике под компьютерной сетью принято понимать группу компьютеров, соединенных при помощи специальной аппаратуры, обеспечивающей совместное использование ресурсов вычислительной системы и обмен данными между любыми компьютерами группы. По своей архитектуре, составу подключенного оборудования и территориальному размещению компьютеров сети делятся на локальные и глобальные[2].

К *локальным сетям* относят системы обработки данных, охватывающие относительно небольшие территории (обычно диаметром не более 5 — 10 км) и расположенные, как правило, в пределах одной организации, предназначенные для решения задач этой организации.

В свою очередь, *глобальные компьютерные сети* объединяют на основе коммуникационного оборудования как отдельные компьютеры, так и локальные сети, расположенные на значительном удалении друг от друга, и характеризуются большим разнообразием каналов передачи данных, программного и аппаратного обеспечения.

Примером глобальной компьютерной сети является сеть Интернет, которая на данный момент прочно занимает положение главной мировой информационной инфраструктуры.

---

[1] См.: Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. — 3-е изд. СПб: Питер, 2006.

[2] См.: Старостенко И.Н., Сопильняк Ю.Н., Шарпан М.В. Информатика и информационные технологии в профессиональной деятельности: курс лекций. Краснодар: Краснодарский университет МВД России, 2012.

Работы по созданию сети Интернет начались в далеком 1969 году. Именно в этом году — 2 января 1969 года — был дан старт проекту разработки сети Агентства перспективных исследований ARPA (Advances Research Projects Agency), получившей название ARPANET. В рамках реализации данного проекта были заложены технологические основы сети, которые позволили 2 сентября 1969 года впервые в истории осуществить по телефонной линии связь между двумя компьютерами, установленными в разных городах США. Именно этот день и считается официальным «днем рождения» сети Интернет.

В 1985 году в Интернете было около двух тысяч компьютеров. Согласно результатам проведенных исследований по состоянию на конец 2017 года *интернет-аудитория составляет 4050247583 человека*[1].

В настоящее время глобальная (общемировая) сеть Интернет представляет собой *совокупность неопределенного множества самых различных компьютеров и их сетей, работающих по согласованным правилам — протоколам*. По своей сути Интернет — это глобальная компьютерная сеть, соединяющая по различным каналам связи (выделенным или коммутируемым) как отдельные локальные сети, так и отдельные компьютеры (рис. 5.1).

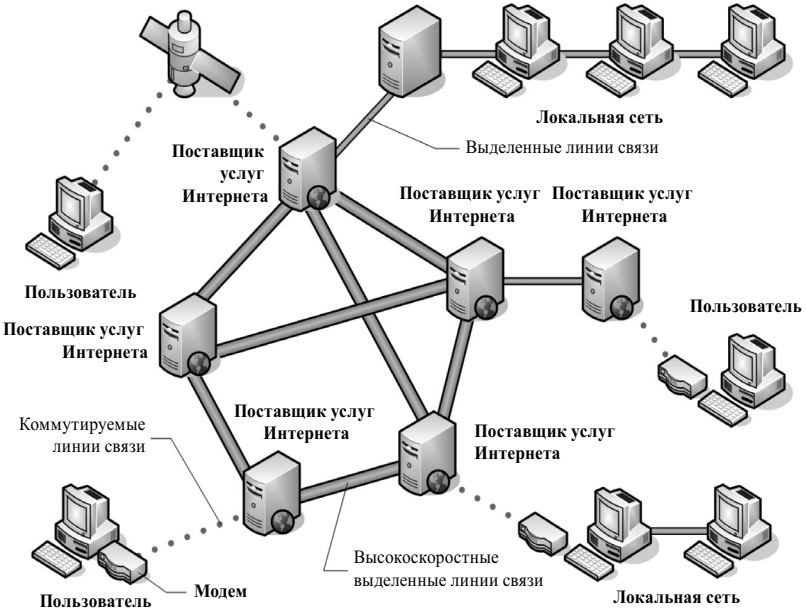


Рис. 5.1. Обобщенная схема глобальной информационно-телекоммуникационной сети «Интернет»

[1] World Internet usage and population statistics. Dec 31, 2017 — Update [Электронный ресурс]. — Режим доступа: https://www.internetworldstats.com/stats.htm. — Загл. с экрана.

В настоящее время использование компьютерных, сетевых технологий является важнейшей составляющей информационного обеспечения органов внутренних дел. По имеющимся данным, в органах внутренних дел установлено свыше 82 тыс. электронно-вычислительных машин, эксплуатируется более 3,2 тыс. автоматизированных информационных систем (далее — АИС), информационные ресурсы которых содержат свыше 870 млн объектов учета. В подразделениях органов внутренних дел установлено свыше 73 тыс. автоматизированных рабочих мест. Ежедневно для получения требуемой информации из АИС поступает около 900 тыс. запросов[1].

Вместе с тем, следует констатировать и тот факт, что рост популярности сетевых технологий сопровождается ростом серьезных угроз безопасности информации, обрабатываемой и передаваемой с помощью информационно-телекоммуникационных систем. Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:

– большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;

– значительная протяженность сети и наличие многих способов проникновения в сеть;

– недостатки в аппаратном и программном обеспечении информационно-телекоммуникационных систем, которые зачастую обнаруживаются лишь в процессе их эксплуатации.

Остроту проблемы, связанной с большой протяженностью сети, иллюстрирует рис. 5.2.

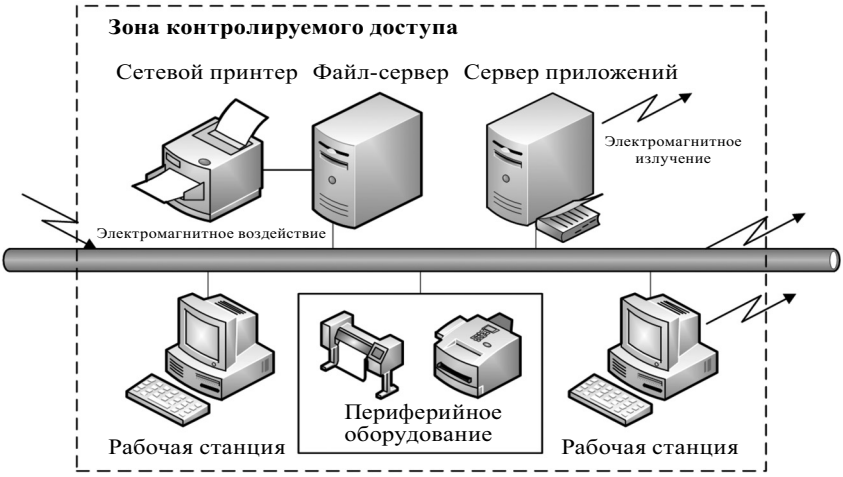


Рис. 5.2. Способы возможного несанкционированного доступа к информации в компьютерной сети

[1] Григорьев А.Н., Фадеева В.В. Использование автоматизированных информационных систем в деятельности органов внутренних дел: учебное пособие. Калининград: Калининградский филиал СПбУ МВД России, 2012.

Нетрудно заметить, что в сети может быть реализовано значительное количество различных способов несанкционированного доступа к циркулирующей в ней информации. Каждое устройство в сети является потенциальным источником электромагнитного излучения из-за того, что соответствующие поля, особенно на высоких частотах, экранированы неидеально. Система заземления вместе с кабельной системой и сетью электропитания может быть использована для получения несанкционированного доступа к информации в сети, в том числе на участках, находящихся вне зоны контролируемого доступа и потому особенно уязвимых. Кроме электромагнитного излучения, потенциальную угрозу представляет и бесконтактное электромагнитное воздействие на кабельную систему.

Наконец возможна утечка информации и по каналам, находящимся вне сети: хищение носителей информации, утечки через элементы строительных конструкций, телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи) и др.

Отмеченное позволяет сделать вывод о том, что поддержание необходимого уровня информационной безопасности при информационно-телекоммуникационном обеспечении органов внутренних дел является одной из важнейших задач информатизации МВД России.

Ранее уже подробно рассматривались угрозы безопасности информации в современных компьютерных системах. Приведенная классификация угроз справедлива и в отношении телекоммуникационных систем. Однако, практическая реализация этих угроз имеет свои особенности, обусловленные технологиями организации и функционирования информационно-телекоммуникационных систем.

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что, наряду с обычными (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые (или удаленные) атаки.

Сетевая атака *— это компьютерная атака с использованием протоколов межсетевого взаимодействия*[1].

Как можно заметить, сетевая атака является частным случаем ***компьютерной атаки***, под которой понимают *целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информацион-*

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств[1].

Рассмотрим классификацию основных сетевых атак[2].

По *характеру атаки*:

– активные — связаны с воздействием на ресурсы компьютерной сети с непосредственным влиянием на работу системы (изменение конфигурации системы или сети, нарушение работоспособности и т.д.) и с нарушением установленных правил разграничения доступа к информации или сетевым ресурсам;

– пассивные — не оказывают непосредственного влияния на работу системы, но их реализация может нарушить установленные правила разграничения доступа к информации или сетевым ресурсам.

По *цели атаки*:

– атаки, направленные на нарушение целостности информации в информационно-телекоммуникационной системе;

– атаки, направленные на нарушение конфиденциальности информации в информационно-телекоммуникационной системе;

– атаки, направленные на нарушение доступности информационно-телекоммуникационной системы.

По условию начала осуществления атаки:

– *атаки по запросу от атакуемого объекта* (атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия);

– *атаки по наступлению ожидаемого события на атакуемом объекте* (атакующий осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие);

– *безусловные атаки* (начало осуществления атаки безусловно по отношению к цели атаки, т.е. атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта).

По наличию обратной связи с атакуемым объектом:

– *атаки с обратной связью* (обратная связь формируется ответом атакуемого объекта на определенный запрос, отправленный к нему злоумышленником, и позволяет последнему реагировать на все изменения, происходящие на атакуемом объекте);

– *атаки без обратной связи* (удаленным атакам не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте).

По расположению субъекта атаки относительно атакуемого объекта:

– *внутрисегментные атаки* (субъект и объект атаки находятся в одном сегменте сети);

– *межсегментные атаки* (субъект и объект атаки находятся в разных сегментах одной сети).

---

[1] См.: Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См.: Основы защиты информации: учебное пособие / под ред. К.М. Бондаря. Хабаровск: Дальневосточный ЮИ МВД России, 2011.

По соотношению количества атакуемых и атакующих субъектов:

– *атаки «один к одному»* — осуществляются одним злоумышленником в отношении одной цели;

– *атаки «один ко многим»* — осуществляются одним злоумышленником в отношении нескольких объектов;

– *атаки «несколько к одному»* — осуществляются несколькими злоумышленниками в отношении одного объекта;

– *атаки «несколько ко многим»* — осуществляются несколькими злоумышленниками в отношении нескольких объектов.

Основываясь на данной классификационной схеме можно выделить типовые сетевые атаки (атаки, характерные для любой распределенной системы), наиболее актуальные в настоящее время.

Анализ сетевого трафика (*Sniffing*). По большей части данные передаются по компьютерным сетям в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в сети, подслушивать или считывать трафик. Анализ перехваченного сетевого трафика позволит извлечь идентификационную информацию, такую как статические пароли пользователей к удаленным хостам, используемые протоколы, доступные порты сетевых служб, активные сетевые сервисы и т.п. В процессе проведения анализа сетевого трафика злоумышленник изучает логику работы сети и, в случае успеха, может получить доступ к конфиденциальной информации удаленного объекта.

Для подслушивания в компьютерных сетях используют сниффер — прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

Сканирование сети. При подготовке атаки против какой-либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. С этой целью им проводится сканирование сети — сбор информации о ней с помощью общедоступных данных и приложений.

Сканирование сети проводится в форме запросов DNS, эхо-тестирования (Ping Sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, злоумышленник использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. В результате добывается информация, которую можно использовать для взлома.

Парольные атаки. Целью этих атак является завладение паролем и логином законного пользователя. Атаки проводятся с помощью ряда методов: простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети и перехват пакетов. При этом в основном используются специальные программы для получения доступа к хосту путем последовательного подбора паролей. В случае успеха нарушитель может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Атаки типа «отказ в обслуживании». Атака «отказ в обслуживании» (Denial-ol-Service, DoS) отличается от атак других типов. Она не нацелена на

получение доступа к сети или на извлечение из этой сети какой-либо информации. DoS-атака делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. По существу, эта атака лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Большинство DoS-атак опирается на общие слабости системной архитектуры.

В случае использования некоторых серверных приложений (таких, как веб- или FTP-сервер) DoS-атаки могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе DoS-атак могут использоваться обычные интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol).

Если атака этого типа проводится одновременно через множество устройств, мы говорим о распределенной атаке «отказ в обслуживании» (DDoS, Distributed DoS).

Простота реализации DoS-атак и огромный вред, причиняемый ими организациям и пользователям, привлекают к этим атакам пристальное внимание администраторов сетевой безопасности.

Подмена доверенного субъекта. Большая часть сетей и операционных систем используют IP-адрес компьютера для того, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом). Такой способ атаки называют фальсификацией адреса, или IP-спуфингам (IP-spoofing).

IP-спуфинг имеет место, когда злоумышленник, находящийся внутри организации или вне ее, выдает себя за законного пользователя.

Атаки IP-спуфинга часто являются отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность хакера.

Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер: правильная настройка управления доступом из внешней сети, пресечение попыток спуфинга чужих сечей пользователями своей сети.

Применение ботнетов. Ботнет (зомби-сеть) — это сеть компьютеров, зараженных вредоносной программой поведения Backdoor. Backdoor позволяет киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя. Такие программы называются ботами.

Ботнеты обладают мощными вычислительными ресурсами, являются грозным кибероружием и хорошим способом зарабатывания денег для злоумышленников. При этом зараженными машинами, входящими в сеть, хозяин ботнета может управлять откуда угодно: из другого города, страны или даже с другого континента, а организация Интернета позволяет делать это анонимно.

Ботнеты могут использоваться злоумышленниками для решения криминальных задач разного масштаба: от рассылки спама до атак на государственные сети.

Рассылка спама. Это наиболее распространенный и один из самых простых вариантов эксплуатации ботнетов. По экспертным оценкам, в настоящее время более 80% спама рассылается с зомби-машин, Многотысячные ботнеты

позволяют спамерам осуществлять с зараженных машин миллионные рассылки в течение короткого времени. Еще одно «преимущество» ботнетов — возможность сбора адресов электронной почты на зараженных машинах. Украденные адреса продаются спамерам либо используются при рассылке спама самими хозяевами ботнета.

Анализ наиболее распространенных угроз, которым подвержены современные информационно-телекоммуникационные системы, показывает, что источники угроз могут изменяться от неавторизованных вторжений злоумышленников до компьютерных вирусов, при этом весьма существенной угрозой безопасности являются человеческие ошибки.

Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов и системных администраторов, обслуживающих информационно-телекоммуникационную систему. Иногда такие ошибки приводят к прямому ущербу (неправильно введенные данные, ошибка в программе, вызвавшая остановку или разрушение системы), а иногда создают слабые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). На втором месте по размерам ущерба располагаются кражи и подлоги. В большинстве случаев виновниками оказываются штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами.

В настоящее время широкое распространение получили технологии построения беспроводных компьютерных сетей, в которых компьютеры вместо проводов и кабелей соединены при помощи радиосигналов. К числу бесспорных преимуществ данного типа сетей следует отнести мобильность и отсутствие соединительных проводов. В тоже время принцип действия беспроводной сети приводит к возникновению большого числа возможных уязвимостей для атак и проникновений.

Беспроводная сетевая технология для обеспечения связи между устройствами, подключенными к сети, использует беспроводные точки доступа AP (Wireless Access Point) — устройства, выполняющие роль базовой станции, которые не только обеспечивают связь между абонентами сети и между собой, но и осуществляют связь с кабельной локальной сетью и с Интернет. Каждая точка доступа может обслуживать несколько абонентов. Несколько близкорасположенных точек доступа образуют зону доступа Wi-Fi, в пределах которой все абоненты, снабженные беспроводными адаптерами, получают доступ к сети.

Каждая беспроводная сеть имеет свое уникальное название и идентификатор (SSID — Service Set Identifier). Идентификатор SSID необходим для подключения устройства к сети. Чтобы связать устройство с точкой доступа, обе системы должны иметь один и тот же SSID. Если устройство не имеет нужного SSID, то оно не сможет связаться с точкой доступа и соединиться с сетью.

Главное отличие между проводными и беспроводными сетями — наличие неконтролируемой области между конечными точками беспроводной сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить ряд нападений, которые невозможны в проводном мире. При использовании беспроводного доступа к локальной сети угрозы безопасности существенно возрастают (рис. 5.3).

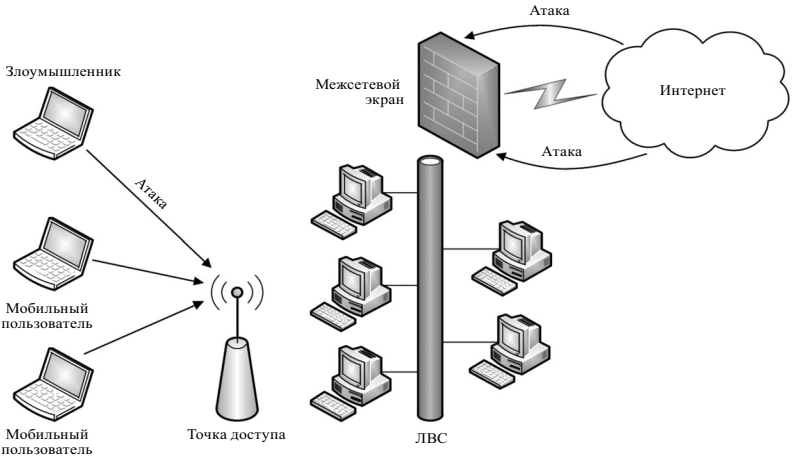


Рис. 5.3. Угрозы при беспроводном доступе
к информационно-телекоммуникационной системе

Перечислим основные уязвимости и угрозы беспроводных сетей[1].

Вещание радиомаяка. Точка доступа включает с определенной частотой широковещательный радиомаяк, чтобы оповещать окрестные беспроводные узлы о своем присутствии. Эти широковещательные сигналы содержат основную информацию о точке беспроводного доступа, включая, как правило, SSID, и приглашают беспроводные узлы зарегистрироваться в данной области. Любая рабочая станция, находящаяся в режиме ожидания, может получить SSID и добавить себя в соответствующую сеть.

Обнаружение WLAN. Для обнаружения беспроводных сетей WLAN используется, например, утилита NetStumber совместно со спутниковым навигатором глобальной системы позиционирования GPS. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней система шифрования WEP. Применение внешней антенны на портативном компьютере делает возможным обнаружение сетей WLAN во время обхода нужного района или поездки по городу. Надежным методом обнаружения WLAN является обследование офисного здания с переносным компьютером в руках.

Подслушивание. Подслушивание ведут для сбора информации о сети, которую предполагается атаковать впоследствии. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Ложные точки доступа в сеть. Опытный атакующий может организовать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не подозревая, обращаются к этой ложной точке доступа и сообщают ей свои

[1] См.: Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2011.

важные реквизиты, например, аутентификационную информацию. Этот тип атак иногда применяют в сочетании с прямым «глушением» истинной точки доступа в сеть.

Отказ в обслуживании. Как уже отмечалось, полную парализацию сети может вызвать атака типа DoS (Denial of Service) — отказ в обслуживании. Беспроводные системы особенно восприимчивы к таким атакам. Физический уровень в беспроводной сети — абстрактное пространство вокруг точки доступа. Злоумышленник может включить устройство, заполняющее весь спектр на рабочей частоте помехами и нелегальным трафиком — такая задача не вызывает особых трудностей. Сам факт проведения DoS-атаки на физическом уровне в беспроводной сети трудно доказать.

Анонимный доступ в Интернет. Незащищенные беспроводные сети обеспечивают злоумышленникам наилучший анонимный доступ для атак через Интернет. Злоумышленники могут использовать незащищенную беспроводную сеть организации для выхода через нее в Интернет, где они будут осуществлять противоправные действия, не оставляя при этом своих следов.

Все вышесказанное предопределяет необходимость принятия действенных мер обеспечения безопасности информации в корпоративных информационно-телекоммуникационных системах.

5.2. Особенности защиты информации в информационно-телекоммуникационных системах

Как уже ранее отмечалось, существует два подхода к проблеме обеспечения безопасности компьютерных систем и сетей: фрагментарный и комплексный.

Фрагментарный подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.п. Достоинством такого подхода является высокая избирательность к конкретной угрозе. Существенный недостаток — отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов информационно-телекоммуникационной системы только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Комплексный подход ориентирован на создание защищенной среды обработки информации в системе, объединяющей в единый комплекс разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности информационно-телекоммуникационной системы, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей системы, чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Основываясь на вышесказанном можно выделить четыре основных этапа построения системы защиты информации в информационно-телекоммуникационных системах:

1) анализ возможных угроз безопасности информационно-телекоммуникационной системе;

2) планирование системы защиты;

3) реализация системы защиты;

4) сопровождение системы защиты.

Этап анализа возможных угроз информационно-телекоммуникационной системе необходим для фиксации состояния системы (конфигурации аппаратных и программных средств, технологии обработки информации) и определения учитываемых воздействий на компоненты системы. Практически невозможно обеспечить защиту информационно-телекоммуникационной системы от всех воздействий, поскольку невозможно полностью установить все угрозы и способы их реализации. Поэтому из всего множества вероятных воздействий выбирают только такие воздействия, которые могут реально произойти и нанести серьезный ущерб.

На ***этапе планирования*** формулируется система защиты как единая совокупность мер противодействия угрозам различной природы.

При построении подобного рода системы необходимо учитывать особенности защиты информации в информационно-телекоммуникационных системах, которые обусловлены, главным образом, следующими обстоятельствами:

1. *Совместное использование ресурсов информационно-телекоммуникационной системы.* Основное преимущество сетевых технологий, используемых при построении информационно-телекоммуникационных систем, заключается в возможности совместного использования программных и аппаратных ресурсов этих систем. Однако это несет в себе и определенные сложности в организации защиты информации: так как одни и те же ресурсы используются многими пользователями, значительно повышается риск НСД.

2. *Расширение зоны контроля.* Территориально распределенные сети объединяют большое количество пользователей, которые могут находится не только в разных регионах, но и в разных странах. Это существенно затрудняет возможность контроля за пользователями со стороны администратора сети.

3. *Комбинация различных программно-аппаратных средств*. Соединение нескольких подсистем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Подсистема обычно настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимы с требованиями на других подсистемах. В случае соединения разнородных систем риск повышается.

4. *Неизвестный периметр.* Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей. Более того, для многих из них не всегда можно точно определить, сколько пользователей имеют доступ к определенному узлу и кто они.

5. *Множество точек атаки*. В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Естественно, это не может способствовать повышению защищенности сети. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы и т. д.

6. *Сложность управления и контроля доступа к системе.* Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу — с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, время атаки может оказаться слишком мало для принятия адекватных мер.

Для решения перечисленных задач в информационно-телекоммуникационных системах используются различные аппаратно-программные средства защиты. К ним относятся электронные устройства и специальные программы, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

– идентификацию (распознавание) и аутентификацию (проверка подлинности) субъектов (пользователей, процессов) информационно-телекоммуникационной системы;

– разграничение доступа к ресурсам информационно-телекоммуникационной системы;

– контроль целостности данных;

– обеспечение конфиденциальности данных;

– регистрацию и анализ событий, происходящих в информационно-телекоммуникационной системе;

– резервирование ресурсов и компонентов информационно-телекоммуникационной системы.

Более подробно эти средства, применительно к компьютерным системам вообще, рассматривались в рамках предыдущей темы. Остановимся на рассмотрении особенностей сетевой защиты в компьютерных системах, которая реализуется двумя основными способами: с использованием межсетевых экранов и путем организации виртуальных частных сетей.

Межсетевые экраны. В стратегии защиты от несанкционированного доступа к информационным ресурсам компьютерной сети особое внимание уделяется обеспечению безопасности ее границ. Целостность периметра компьютерной сети обеспечивается использованием тех или иных базовых технологий межсетевого экранирования в точке подключения защищаемой сети к внешней неконтролируемой сети. В качестве внешней сети чаще всего выступает глобальная сеть Интернет. Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном. В переводной литературе также встречаются термины firewall или брандмауэр.

Межсетевой экран *— это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или исходящей из нее*[1].

Межсетевой экран повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды. Это

[1] См.: Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / под ред. В.Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001.

уменьшает уязвимость внутренних объектов, так как сторонний нарушитель должен преодолеть некоторый защитный барьер, в котором механизмы обеспечения безопасности сконфигурированы особо тщательно.

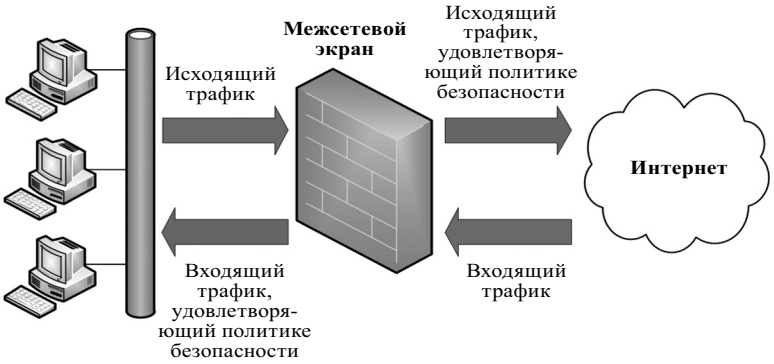


Рис. 5.4. Контроль периметра сети с помощью межсетевого экрана

В общем случае алгоритм функционирования межсетевого экрана сводится к выполнению двух групп функций, одна из которых ограничивает перемещение данных (фильтрация информационных потоков), а вторая, наоборот, ему способствует (посредничество в межсетевом взаимодействии).

Защита информационно-телекоммуникационной системы за счет фильтрации информационных потоков подразумевает анализ содержимого сетевых пакетов, проходящих через межсетевой экран, по совокупности критериев на основе заданных правил и принятия решения о его дальнейшем распространении в (из) информационно-телекоммуникационной системе. Таким образом, межсетевой экран реализует разграничение доступа субъектов из одной автоматизированной системы к объектам другой автоматизированной системы.

Другой вариант алгоритма функционирования межсетевого экрана предполагает, что защита автоматизированной системы обеспечивается с помощью экранирующего агента, который проверяет допустимость полученного запроса субъекта к объекту, при положительном результате этой проверки устанавливает свое соединение с объектом, а затем обеспечивает пересылку информации между субъектом и объектом взаимодействия, осуществляя контроль и/или регистрацию.

Брандмауэры бывают двух видов: программные и аппаратные. Для программных брандмауэров необходим отдельный компьютер на базе традиционных операционных систем Unix либо Windows. Такой брандмауэр может служить единой точкой входа во внутреннюю сеть. Слабость и ненадежность подобной защиты заключается не столько в возможных нарушениях корректной работы самого программного брандмауэра, сколько в уязвимости используемых операционных систем, на базе которых функционирует межсетевой экран. Аппаратные брандмауэры построены на базе специально разработанных для этой цели собственных операционных систем.

Следует отметить, что межсетевой экран не является абсолютной гарантией защиты внутренней сети от удаленных атак, несмотря на то, что осуществляет сетевую политику разграничения доступа к определенным ресурсам. Во множестве случаев достаточно вывести из строя лишь один межсетевой экран, защищающий определенный сегмент, чтобы отключить всю сеть от внешнего мира и при этом нанести достаточный ущерб, вызвав большие сбои в работе организации или компании. Но из всего вышесказанного отнюдь не следует, что их использование абсолютно бессмысленно и неэффективно. Наоборот, применение брандмауэров — необходимое условие обеспечения безопасности сети.

Виртуальные частные сети (Virtual Private Network VPN) — *это технология, объединяющая доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия*[1].

Основной целью создания VPN-сетей является максимально возможное обособление потоков данных одной организации от потоков данных всех других пользователей публичной сети. Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и конфиденциальности передаваемых данных. Таким образом, основными задачами технологий VPN являются обеспечение в публичной сети гарантированного качества обслуживания для потоков пользовательских данных, а также защита их от возможного несанкционированного доступа или разрушения[2].

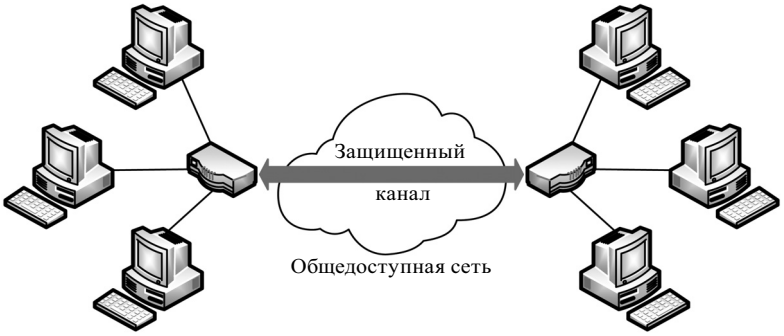


Рис. 5.5. Виртуальная частная сеть (VPN)

VPN состоит из каналов глобальной сети, защищенных протоколов и маршрутизаторов. Для объединения удаленных компьютерных сетей в VPN используются так называемые виртуальные выделенные каналы. Для организации подобных соединений применяется механизм *туннелирования*, или *инкапсуляции*.

---

[1] См.: Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие / науч. ред. д-р техн. наук, проф. Н.А. Гайдамакин. Екатеринбург: УГТУ-УПИ, 2008.

[2] См.: Запечников С.В., Милославская Н.Г., Толстой Л.И. Основы построения виртуальных частных сетей: учебное пособие. М.: Горячая линия-Телеком, 2001.

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть. Инициатор туннеля инкапсулирует пакеты локальной компьютерной сети в IP-пакеты, содержащие в заголовке адреса инициатора и терминатора туннеля. Терминатор туннеля извлекает исходный пакет. Естественно, при подобной передаче требуется решать проблему конфиденциальности и целостности данных, что не обеспечивается простым туннелированием. Конфиденциальность передаваемой корпоративной информации достигается шифрованием (алгоритм одинаков на обоих концах туннеля).

Само по себе туннелирование не защищает данные от несанкционированного доступа или искажения, а только создает предпосылки для защиты всех полей исходного пакета, включая и поля заголовка. Для того, чтобы обеспечить секретность передаваемых данных, исходные пакеты-пассажиры шифруются и/или снабжаются электронной подписью, а затем передаются по транзитной сети с помощью пакетов несущего протокола.

В качестве примера комплексного средства защиты, включающего в себя функцию организации VPN, является отечественное аппаратно-программное средство сетевой защиты ViPNet, разработанное компанией «ИнфоТеКС».

Говоря о методах защиты информации в информационно-телекоммуникационных системах, нельзя не упомянуть ***цифровую стеганографию*** — весьма перспективный метод защиты информации, который позволяет скрыть сам факт хранения или передачи закрытой информации. Данный метод основан на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Обработка мультимедийных файлов в компьютерных системах открыла перед стеганографией практически неограниченные возможности.

Сущность ***этапа реализации*** системы защиты информации в информационно-телекоммуникационных системах заключается в установке и настройке средств защиты, необходимых для реализации запланированных правил обработки информации.

Заключительный ***этап сопровождения*** заключается в контроле работы системы, регистрации происходящих в ней событий, их анализе с целью обнаружения нарушений безопасности, коррекции системы защиты. Ключевую роль в решении данных задач играют ***системы обнаружения вторжений***.

Обнаружение вторжений — это процесс мониторинга событий, происходящих в информационной системе и их анализа на наличие признаков, указы-

вающих на попытки вторжения: нарушения конфиденциальности, целостности, доступности информации или политики информационной безопасности[1].

Исходя из этого, под *системами обнаружения вторжений (IDS — Intrusion Detection Systems) понимают множество различных программных и аппаратных средств, осуществляющих анализ использования ресурсов информационной системы и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способных предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин.*

В общем случае система обнаружения вторжений включает в себя следующие компоненты:

1) сенсорную подсистему, отвечающую за отслеживание событий, затрагивающих безопасность защищаемой системы;

2) подсистему анализа, обеспечивающую выявление среди подозрительных событий тех, которые представляют угрозу или нарушения безопасности (атаки, подозрительные действия);

3) хранилище обеспечивает накопление и хранение данных сенсорной подсистемы и результатов их анализа;

4) консоль управления, используемую для настройки системы обнаружения вторжений, наблюдения за состоянием защищаемой системы, просмотра выявленных подсистемой анализа инцидентов.

Выделяют два основных типа систем обнаружения вторжений:

– защищающие отдельный фрагмент сети;

– защищающие отдельный сервер.

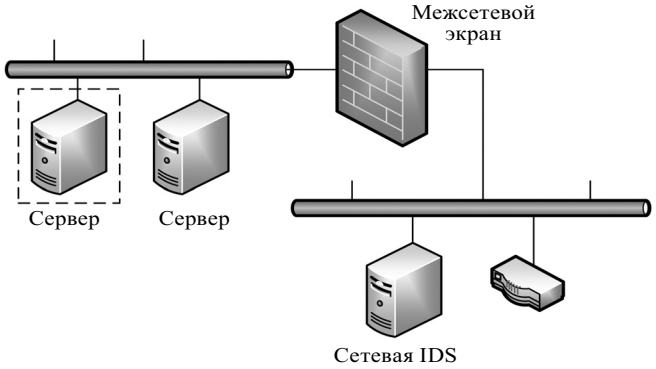


Рис. 5.6. Варианты размещения IDS в сетевой среде

Системы обнаружения вторжений, *защищающие отдельный фрагмент сети*, развертываются на специализированном сервере на котором не работают никакие другие приложения (поэтому он может быть особенно надежно защищен от нападения; кроме того, этот сервер может быть сделан «невидимым» для

[1] См.: Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012.

нападающего). Для защиты сети устанавливаются несколько таких серверов, которые анализируют сетевой трафик в различных сегментах сети. Таким образом, несколько удачно расположенных систем могут контролировать большую сеть.

К недостаткам таких систем относят проблемы распознавания нападений в момент высокой загрузки сети и неспособность анализировать степень проникновения (система просто сообщает об инициированном нападении).

Системы обнаружения вторжений, защищающие отдельный сервер, собирают и анализируют информацию о процессах, происходящих на конкретном сервере. Благодаря узкой направленности эти системы могут проводить высоко детализированный анализ и точно определять, кто из пользователей выполняет злонамеренные действия. Некоторые системы этого класса могут управлять группой серверов, подготавливая централизованные обобщающие отчеты о возможных нападениях. В отличие от предыдущих систем они могут работать даже в сети, использующей шифрование данных. Однако системы этого класса не способны контролировать ситуацию во всей сети, так как видят только пакеты, получаемые «своим» сервером. Кроме того, снижается эффективность работы сервера вследствие использования его вычислительных ресурсов[1].

Таким образом, как можно заметить, обеспечение информационной безопасности современных информационно-телекоммуникационных систем осуществляется путем принятия целого комплекса разноплановых мер. При этом, системный подход к организации защиты информации определяет необходимость построения не только собственно системы защиты, но и системы управления ею, то есть построения системы управления информационной безопасностью.

Следует заметить, что проблема обеспечения безопасности информационных систем в современном мире усложняется отсутствием единой методической базы, позволяющей проводить адекватную оценку угроз информационным ресурсам, а также степени защищенности систем в информационной сфере. В настоящее время для оценки угроз и управления защищенностью зачастую используется аппарат анализа и управления рисками.

В рамках этого подхода требования к информационной безопасности определяются с помощью систематической оценки рисков. Решения о расходах на мероприятия по управлению информационной безопасностью должны приниматься исходя из возможного ущерба, нанесенного деятельности организации в результате нарушений информационной безопасности.

Методы оценки риска могут применяться как для всей организации, так и для какой-либо ее части, отдельных информационных систем, определенных компонентов систем или услуг, а именно там, где это практически выполнимо и целесообразно.

Оценка риска — это систематический анализ:

– вероятного ущерба, наносимого деятельности организации в результате нарушений информационной безопасности с учетом возможных последствий

[1] См.: Безопасность сетей: обнаружение вторжений [Электронный ресурс]. — Режим доступа: http://www.intuit.ru/studies/courses/102/102/lecture/2995/. — Загл. с экрана.

от потери конфиденциальности, целостности или доступности информации и других активов;

– вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью.

Результаты этой оценки помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрению мероприятий по управлению информационной безопасностью с целью минимизации этих рисков.

Таким образом, рассмотрение вопросов, затронутых в настоящем разделе учебного пособия, позволяет сделать следующие выводы.

В настоящее время использование компьютерных, сетевых технологий является важнейшей составляющей информационного обеспечения органов внутренних дел. Вместе с тем, рост популярности сетевых технологий сопровождается ростом серьезных угроз безопасности информации, обрабатываемой и передаваемой с помощью информационно-телекоммуникационных систем.

Рассмотренные ранее угрозы безопасности информации в современных компьютерных системах справедливы и в отношении телекоммуникационных систем. Однако, практическая реализация этих угроз имеет свои особенности, обусловленные технологиями организации и функционирования информационно-телекоммуникационных систем.

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что, наряду с обычными (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые (или удаленные) атаки. К числу наиболее актуальных в настоящее время сетевых атак относят: анализ сетевого трафика, сканирование сети, парольные атаки, атаки типа «отказ в обслуживании», подмена доверенного субъекта, применение ботнетов, рассылка спама.

Анализ наиболее распространенных угроз, которым подвержены современные информационно-телекоммуникационные системы, показывает, что источники угроз могут изменяться от неавторизованных вторжений злоумышленников до компьютерных вирусов, при этом весьма существенной угрозой безопасности являются человеческие ошибки.

В настоящее время широкое распространение получили технологии построения беспроводных компьютерных сетей, в которых компьютеры вместо проводов и кабелей соединены при помощи радиосигналов. Вместе с тем,

принцип действия беспроводной сети приводит к возникновению большого числа возможных уязвимостей для атак и проникновений.

Для решения задач защиты информации в информационно-телекоммуникационных системах используются различные аппаратно-программные средства, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты: идентификацию (распознавание) и аутентификацию (проверка подлинности) субъектов (пользователей, процессов) информационно-телекоммуникационной системы; разграничение доступа к ресурсам информационно-телекоммуникационной системы; контроль целостности данных; обеспечение конфиденциальности данных; регистрацию и анализ событий, происходящих в информационно-телекоммуникационной системе; резервирование ресурсов и компонентов информационно-телекоммуникационной системы. К особенностям сетевой защиты в компьютерных системах следует отнести использование межсетевых экранов и организацию виртуальных частных сетей.

Контрольные вопросы

1. Что понимается под информационно-телекоммуникационной системой?
2. Укажите основные причины, актуализирующие вопросы защиты информации в информационно-телекоммуникационных системах.
3. Что понимается под компьютерной атакой?
4. Приведите классификацию основных сетевых компьютерных атак?
5. Какие сетевые атаки наиболее актуальны в настоящее время?
6. В чем заключаются особенности фрагментарного и комплексного подходов к защите информации в информационно-телекоммуникационных системах?
7. Перечислите и охарактеризуйте основные этапы построения системы защиты информации в информационно-телекоммуникационных системах.
8. Что такое межсетевой экран, какие функции он выполняет?
9. Для каких целей в системе обеспечения безопасности информационно-телекоммуникационных систем используется технология виртуальных частных сетей?
10. В чем заключаются особенности построения системы управления информационной безопасностью на основе управления рисками?

ЗАКЛЮЧЕНИЕ

В настоящее время обеспечение информационной безопасности органов внутренних дел относится к числу наиболее актуальных аспектов проблемы повышения эффективности деятельности служб и подразделений МВД России. Анализ существующего положения дел в данной сфере позволяет констатировать стремительное увеличение количества угроз безопасности информации и информационной инфраструктуре органов правопорядка. Тому есть множество причин:

– значительное повышение вычислительной мощности средств компьютерной техники делает возможным взлом парольной защиты информационных систем методом прямого перебора, повышает уязвимость криптографической защиты информации;

– развитие сетевых технологий, их использование в практической деятельности органов внутренних дел расширяют число потенциальных злоумышленников, имеющих техническую возможность осуществить нападение;

– использование облачной архитектуры построения информационных систем ведет к появлению новых угроз, связанных с использованием облачных сервисов;

– конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки программного обеспечения, что ведет к снижению качества тестирования и выпуску продуктов с дефектами защиты;

– неуклонно возрастающий уровень затрат на развитие информационных систем вступает в противоречие с бюджетными ограничениями, что нередко влечет за собой сокращение ассигнований, выделяемых на обеспечение информационной безопасности и т.д.

Этому также способствуют как общий прогресс информационных технологий, так и неуклонно повышающийся уровень информационно-технического противодействия со стороны криминального мира.

Решение существующих проблемных вопросов в сфере обеспечения информационной безопасности органов внутренних дел предполагает реализацию целого комплекса правовых, научных, организационно-технических, ресурсных и кадровых мероприятий, среди которых наиболее актуальными представляются следующие:

– совершенствование ведомственной нормативной правовой базы, регулирующей деятельность органов внутренних дел в области обеспечения информационной безопасности.

– формирование научно-технической базы системы обеспечения информационной безопасности органов внутренних дел на основе планирования, проведения и внедрения результатов научно-исследовательских и опытно-конструкторских работ, учета передового опыта в области информационной безопасности;

– разработка единой научно-технической политики по созданию, совершенствованию и развитию системы информационной безопасности органов внутренних дел;

– развитие системы лицензирования подразделений органов внутренних дел на осуществление мероприятий и (или) оказание услуг в области защи-

ты государственной тайны (в части технической защиты информации) и проведение работ, связанных с созданием средств защиты информации, а также аккредитации их в качестве органов по аттестации объектов информатизации;

– проведение аттестации объектов информатизации органов внутренних дел;

– разработка правил разграничения доступа к информационным ресурсам ОВД;

– выявление информационно-технических воздействий на информационную сферу ОВД, защиту от них, ликвидацию (нейтрализацию) их последствий;

– обеспечение гарантированной стойкости каналов шифрованной и конфиденциальной связи, межведомственных каналов связи;

– развитие системы удостоверяющих центров органов внутренних дел;

– реализация комплекса мер по поддержанию бесперебойного функционирования информационно-телекоммуникационных систем органов внутренних дел;

– разработка критериев и методов оценки эффективности системы обеспечения информационной безопасности органов внутренних дел;

– проведение комплексного технического контроля и оценки эффективности мероприятий по защите информации;

– обеспечение требуемого объема программных, программно-технических и технических средств защиты информации (включая криптографические), необходимых для организации технической защиты информации;

– организация подготовки и повышения квалификации сотрудников органов внутренних дел в области обеспечения информационной безопасности на базе ведомственных образовательных и иных учреждений.

Обеспечение информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра самых различных средств защиты информации, некоторые из которых находятся только лишь в стадии становления. В этих условиях политика по обеспечению информационной безопасности органов внутренних дел должна быть не только адекватна потребностям практики, но и нацеливать на разработку новых методов и средств защиты информации, отвечающих тенденциям развития новых информационных технологий в современном обществе.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Кодекс поведения должностных лиц по поддержанию правопорядка (принят Резолюцией Генеральной Ассамблеи ООН 34/169 от 17 декабря 1979 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 5 февраля 2018 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Уголовный кодекс Российской Федерации (ред. от 19 февраля 2018 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Уголовно-процессуальный кодекс Российской Федерации (ред. от 31 декабря 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (ред. от 26 июля 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. от 6 июля 2016 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (ред. от 31 декабря 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Федеральный закон от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» (ред. от 7 февраля 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 25 ноября 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 29 июля 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» (ред. от 5 декабря 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

13. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (в ред. от 23 июня 2016 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

14. Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» (ред. от 1 июля 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

15. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» (ред. от 1 января 2018 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

16. Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (ред. от 30 декабря 2000 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 13 июля 2015 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

18. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (ред. от 22 мая 2015 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

19. Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» (ред. от 15 июля 2002 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

20. Постановление Правительства Российской Федерации от 10 марта 2000 г. № 214 «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию» (ред. от 26 января 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

21. Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» (ред. от 30 декабря 2017 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

22. Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» (ред. от 18 марта 2016 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

23. Положение о Министерстве внутренних дел (утверждено Указом Президента Российской Федерации от 21 декабря 2016 г. № 699) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

24. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

25. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

26. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности (утверждено Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233) (ред. от 18 марта 2016 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

27. Положение о сертификации средств защиты информации (утверждено Постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации») (ред. от 21 апреля 2010 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

28. Положение о сертификации средств защиты информации по требованиям безопасности информации (ведено в действие приказом Председателя Гостехкомиссии России от 27 октября 1995 г. № 199) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

29. Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (утв. приказом ФСБ России от 13 ноября1999 г. № 564) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

30. Приказ МВД России от 24 декабря 2015 г. № 1228 «Об утверждении Правил организации доступа к информационно-телекоммуникационной сети «Интернет» в органах внутренних дел Российской Федерации» (ред. от 23 декабря 2016 г.) [Электронный ресурс]. Доступ из СТРАС «Юрист».

31. Приказ МВД России от 14 марта 2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» (ред. от 26 октября 2016 г.) [Электронный ресурс]. Доступ из СТРАС «Юрист».

32. Приказ МВД России от 16 января 2012 г. № 25 «Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры» [Электронный ресурс]. Доступ из СТРАС «Юрист».

33. Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных

системах органов внутренних дел Российской Федерации» (ред. от 20 апреля 2015 г.) [Электронный ресурс]. Доступ из СТРАС «Юрист».

34. Приказ МВД России от 2 августа 2010 г. № 561 «Об утверждении концепции развития системы криптографической защиты информации в органах внутренних дел Российской Федерации до 2013 года» [Электронный ресурс]. Доступ из СТРАС «Юрист».

35. Постановление Конституционного суда Российской Федерации от 31 марта 2011 г. № 3-П/2011 по делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С.В. Капорина, И.В. Коршуна и других [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

36. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

37. Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

38. Национальный стандарт Российской Федерации ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

39. Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 531-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

40. Государственный стандарт Российской Федерации ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (принят постановлением Госстандарта Российской Федерации от 12 сентября 2001 г. № 380-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

41. Государственный стандарт Российской Федерации ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта Российской Федерации от 14 июля 1998 г. № 295) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

42. Государственный стандарт Российской Федерации ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта Российской Федерации от 9 февраля 1995 г. № 49) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

43. Государственный стандарт Российской Федерации ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов» (принят и введен в действие постановлением Госстандарта Российской Федерации от 3 марта 2003 г. № 65-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

44. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g.

45. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/ download/296.

46. Требования к средствам антивирусной защиты (утв. приказом ФСТЭК Росси от 20 марта 2012 г. № 28) [Электронный ресурс]. — Режим доступа: http://fstec.ru/ component/attachments/download/402.

47. ФСТЭК России. Методика определения угроз безопасности в информационных системах (проект) [Электронный ресурс]. — Режим доступа: http://fstec.ru/component/attachments/download/812.

Специальная литература

1. Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г. Основы информационной безопасности в ОВД: учебник для вузов. СПб: Университет МВД РФ, 2010.

2. Ахметшин Р.К. Уголовно-правовые и криминологические меры защиты информации, используемой в правоохранительной деятельности органов внутренних дел: дисс. … канд. юр. наук. М., 2006.

3. Балановская А.В. Концептуальный подход к построению системы информационной безопасности промышленного предприятия//Вестник Самарского государственного университета. 2015. № 5(127). С. 14-20.

4. Баришполец В.А. Основы информационно-психологической безопасности. М.: Знание, 2012.

5. Бедрин В.С. Организационно-технические и программные методы защиты информации в компьютерных системах. Волгоград: ВА МВД России, 2007.

6. Безопасность сетей: обнаружение вторжений [Электронный ресурс]. —Режим доступа: http://www.intuit.ru/studies/courses/102/102/ lecture/2995.

7. Белкин Р.С. Курс криминалистики: учеб. пособие для вузов. — 3-е изд., дополненное. М.: ЮНИТИ-ДАНА, Закон и право, 2001.

8. Блинов А.М. Информационная безопасность: учебное пособие. Часть 1. СПб: Изд-во СПбГУЭФ, 2010.

9. Блокиратор сотовой и беспроводной связи ST 202 «UDAV-M» [Электронный ресурс]. — Режим доступа: http://www.mascom.ru/equipment/sredstva-

zashchity-informatsii /blokiratory-sotovoy-i-besprovodnoy-svyazi/blokirator-sistem-besprovodnoy-svyazi-st-202-udav-m.php.

10. Богдановская В.А., Згадзай О.Э. Расследование преступлений в сфере компьютерной информации. Казань: Казанский юридический институт МВД России, 2012.

11. Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015.

12. Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 1: Технические методы и средства: монография. Изд. 2-е доп. и перераб. / под ред. д-ра юрид. наук, проф. В.М. Мешкова. Калининград: Калининградский ЮИ МВД России, 2003.

13. Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 2: Организационно-правовые методы и средства: монография / под ред. д-ра юрид. наук, проф. В.М. Мешкова. Калининград: Калининградский ЮИ МВД России, 2003.

14. Винер Н. Кибернетика и общество. М.: Изд. ин. лит., 1958. 200 с.

15. Гафнер В.В. Информационная безопасность: учебное пособие. Ростов н/Д: Феникс, 2010.

16. Глушков В.М. Мышление и кибернетика // Вопросы философии. 1963. № 1. С. 36-48.

17. Григорьев А.Н. Информация и информационное взаимодействие в расследовании преступлений: теоретические аспекты: монография. Калининград: Калининградский ЮИ МВД России, 2006.

18. Григорьев А.Н. Организация технической защиты криминалистически значимой информации при производстве предварительного расследования // Вестник криминалистики / отв. ред. А.Г. Филиппов. Вып. 3(11). М.: Спарк, 2004. С. 49-55.

19. Григорьев А.Н. Проблемы обеспечения информационной безопасности России в условиях глобализации и информатизации современного общества // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2013. № 4(34). С. 51-55.

20. Григорьев А.Н. Теоретические аспекты информации и ее защиты в предварительном расследовании преступлений: дисс. ... канд. юрид. наук. Калининград: Калининградский юридический институт МВД РФ, 2002.

21. Григорьев А.Н., Фадеева В.В. Использование автоматизированных информационных систем в деятельности органов внутренних дел: Учебное пособие. Калининград: Калининградский филиал СПбУ МВД России, 2012.

22. Григорьев А.Н., Фадеева В.В. Современные технологии защиты компьютерной информации: учебно-практическое пособие. Калининград: Калининградский ЮИ МВД России, 2011.

23. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями Вена, 10-17 апреля 2000 г. Положение в мире в области преступности и уголовного правосудия. Доклад генерального секретаря A/CONF.187/5.

24. Диалектический и исторический материализм/под общ. ред. А.П. Шептулина. М.: Политиздат, 1985.

25. Дровникова И.Г., Буцынская Т.А. Модель нарушителя в системе безопасности [Электронный ресурс]. — Режим доступа: http://www.aktivsb.ru/ info600.html.

26. Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие; науч. ред. д-р техн. наук, проф. Н.А. Гайдамакин. Екатеринбург: УГТУ-УПИ, 2008. 182 с.

27. Журавленко Н.И., Курбанов Д.А. Основы теории и методологии защиты информации в органах внутренних дел: монография. Уфа: УЮИ МВД РФ, 2001.

Запечников С.В., Милославская Н.Г., Толстой Л.И. Основы построения виртуальных частных сетей: учебное пособие. М.: Горячая линия-Телеком, 2001. 249 с.

28. Ишин А.М., Григорьев А.Н. Информация и расследование преступлений (технические меры обеспечения информационной защищенности деятельности по раскрытию и расследованию преступлений): научно-практическое пособие. Калининград: КЮИ МВД России, 2002.

29. Капсула. Акустический сейф [Электронный ресурс]. — Режим доступа: http://www.mascom.ru/equipment/tekhnicheskie-sradstva-v-zashchishchennom-ispolnenii/akusticheskie-seyfy/kapsula.php.

30. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учебное пособие / под редакцией Ю.Ф. Каторина. СПб: НИУ ИТМО, 2012.

31. Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс]. — Режим доступа: http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf.

32. Князева Е.Н., Курдюмов С.П. Коэволюция: человек как соучастник коэволюционных процессов // Устойчивое развитие. Наука и практика. 2002. № 1. С. 14-22.

33. Колмогоров А.Н. Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 1965. Т. 1. Вып. 1. С. 3-11.

34. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011.

35. Копылов В.А. Информационное право: учебник. Изд. 2-е, перераб. и доп. М.: Юристъ, 2005.

36. Кривенцов, П.А. Латентная преступность в России: криминологическое исследование: дисс. … канд. юрид. наук. М, 2014.

37. Кузнецов И.Н. Информация: сбор, защита, анализ: учебник по информационно-аналитической работе. М., ООО «Изд. Яуза», 2001.

38. Лаборатория Касперского. О вирусах: Основные источники проникновения угроз на компьютер [Электронный ресурс]. — Режим доступа: http://support.kaspersky.ru/ viruses#block2.

39. Лапин В.В. Основы информационной безопасности в ОВД: курс лекций. М.: Московский университет МВД России, 2009.

40. Леверкюн П. Служба разведки и контрразведки // Итоги Второй мировой войны. Выводы побежденных. СПб: Полигон; М.: АСТ, 1998.

41. Леонтьева Н.Н. О содержании Информации // Научно-техническая информация. Сер. 2. Информационные системы и процессы. 1999. № 8. С. 9-14.

42. Луценко Л.М. Информационное общество и его социально-философский аспект: монография. М.: Галлея-Принт, 2011.

43. Мазитов Р.Р. Каналы утечки информации в деятельности органов внутренних дел и способы противодействия ей // Российский следователь. 2010. № 17. С. 32-36.

44. Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки по ТКУИ [Электронный ресурс]. — Режим доступа: http://www.intuit.ru/studies/courses/2291/591/ lecture/12707.

45. Мешкова Т.А. Безопасность в условиях глобальной информатизации: новые вызовы и новые возможности: автореф. дисс. … канд. полит. наук. М., 2003.

46. Мещеряков В.А. Словарь компьютерного жаргона. Воронеж: Изд. ВГУ, 1999.

47. Миронова В.Г., Шелупанов А.А. Модель нарушителя безопасности конфиденциальной информации // Информационная безопасность систем. 2012. № 1(31). С. 28-34.

48. Моделирование угроз — ключевой аспект построения системы безопасности [Электронный ресурс]. — Режим доступа: http://www.cleper.ru/articles/description.php?n=354.

49. Можаева Г.В. Роль исторической информации в современном источниковедении. Открытое и дистанционное образование. 2003. № 1. С. 35-46.

50. Моисеев Н.Н. Универсум, информация, общество. М.: Устойчивый мир, 2001.

51. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: учебное пособие. М.: МИЭТ, 2013.

52. Образцов В.А. Криминалистика: Курс лекций. М.: Юнифир, 1996.

53. Объем мирового рынка киберпреступности достиг 1 трлн. долларов [Электронный ресурс]. — Режим доступа: http://www.plusworld.ru/daily/obem-mirovogo-rinka-kiberprestupnosti-dostig-1-trln-dollarov/.

54. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 3-е изд. СПб: Питер, 2006.

55. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. Заведений / А.А. Стрельцов и др.; под ред. А.А. Стрельцова. М.: Издательский центр «Академия», 2008. 256 с.

56. Основы защиты информации: учебное пособие / под ред. К.М. Бондаря. Хабаровск: Дальневосточный ЮИ МВД России, 2011.

57. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие. 3-е изд., перераб. и доп. М.: ФОРУМ, 2010.

58. Паршина Е.Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании преступлений: дисс. … канд. юрид. наук. Ижевск, 2004.

59. Патрушев рассказал о внедрении разведками вирусов в информационные системы госвласти [Электронный ресурс]. — Режим доступа: http://vz.ru/news/2015/7/8/755034.print.html.

60. Пермяков М.В. Категория «тайна» в системе правового регулирования: монография. Екатеринбург: УЮИ МВД России, 2008.

61. Платонов В.В. Программно-аппаратные средства защиты информации: учебник. М.: Академия, 2013.

62. Плотников Н.И. Информационная разведка: как создается закрытая информация из открытых источников. Новосибирск: Научно-издательский центр ОИГГМ СО РАН, 1998.

63. «Пора поставить действенный заслон информационной войне». Председатель Следственного комитета РФ Александр Бастрыкин — о методах борьбы с экстремизмом в России [Электронный ресурс]. — Режим доступа: http://www.kommersant.ru/Doc/ 2961578.

64. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А. Минаев, А.П. Фисун и др. М.: Маросейка, 2008.

65. Психология человека от рождения до смерти. Полный курс психологии развития/под ред. члена-корреспондента РАО А.А. Реана. СПб: «Прайм-ЕВРОЗНАК», 2003. 416 с.

66. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. М.: Изд. «Щит-М», 1999.

67. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / под ред. В.Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001.

68. Российский рынок антивирусов находится в стагнации [Электронный ресурс]. — Режим доступа: http://www.dailycomm.ru/m/29960/.

69. Система постановки виброакустических и акустических помех «Шорох-5Л» [Электронный ресурс]. — Режим доступа: http://www.mascom.ru/ equipment/sredstva-zashchity-informatsii/zashchita-ot-utechki-za-schet-avak/shorokh-5l.php.

70. Смирнов Н.А. Западное влияние на русский язык в Петровскую эпоху. СПб: Тип. Акад. наук, 1910.

71. Советский энциклопедический словарь / Гл. ред. А.М. Прохоров. 3-е изд. М.: Сов. энциклопедия, 1985.

72. Современные технологии защиты ПО от нелегального копирования: что выбрать разработчику? [Электронный ресурс]. — Режим доступа: http://www.itsec.ru/articles2/Oborandteh/sovremennie-tehnologii-zashiti-po-ot-nelegalnogo-kopirovaniya-chto-vibrat-razrabotchiky.

73. Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений. М.: Собрание, 2004.

74. Старостенко И.Н., Сопильняк Ю.Н., Шарпан М.В. Информатика и информационные технологии в профессиональной деятельности: курс лекций. Краснодар: Краснодарский университет МВД России, 2012.

75. Стационарный шумогенератор ГШ-1000М [Электронный ресурс]. — Режим доступа: http://www.nelk.ru/node/381.

76. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы/под ред. В.А. Садовничего и В.П. Шерстюка. М.: МЦНМО, 2002. 296 с.

77. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. Минск: Беллитфонд, 2005.

78. Тенденции использования нелицензионного программного обеспечения в России [Электронный ресурс]. — Режим доступа: http://ww2.bsa.org/~/media/Files/Research%20Papers/IDC/WhitePaperUnlicensedSoftwareUseTrendsRussia.ashx.

79. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005.

80. Тростников В.Н. Человек и информация. М.: Наука, 1970.

81. Урсул А. Д. Отражение и информация. М.: Мысль, 1973.

82. Урсул А.Д. Природа информации. М.: Политиздат, 1968.

83. «Ученые» с большой дороги / Э.П. Кругляков; Российская академия наук. Комиссия по борьбе с лженаукой и фальсификацией научных исследований. М.: Наука, 2001. 319 с.

84. Ущерб экономики России от киберпреступности в 2015 году [Электронный ресурс]. — Режим доступа: http://www.compulenta.ru/lenta/?id=144811.

85. Филиппова Н.В. Правовое обеспечение информационной безопасности Российской Федерации: учебное пособие. Воронеж: ВИ МВД России, 2012.

86. Хорев П.В. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2005.

87. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008.

88. ЦИКАДА-М. Устройство защиты телефонных переговоров [Электронный ресурс]. — Режим доступа: http://mascom-dv.ru/index.php/katalogi/eqipments/zashchita-rechevoj-informatsii/133-sredstva-zaschiti-telefonnih-peregovorov-ot-nesankcionirovannogo-proslushivaniya.

89. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012.

90. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. М.: ИД «ФОРУМ»; «ИНФРА-М», 2011.

91. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. М.: ИНФРА-М, 2010.

92. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов. М.: Академический Проект: Трикста, 2005.

93. ST 165 Селективный обнаружитель цифровых радиопередающих устройств [Электронный ресурс]. — Режим доступа: http://signal-t.ru/catalog/signal_t/mobilnye-poiskovye-ustroystva.

94. Gregory Bateson. Steps to an Ecology of Mind: collected essays in anthropology, psychiatry, evolution, and epistemology. New York: Ballantine Books, 1972.

95. How Much Information? 2010. Report on Enterprise Server Information [Электронный ресурс]. — Режим доступа: http://hmi.ucsd.edu/pdf/HMI_2010_EnterpriseReport_Jan_ 2011.pdf.

96. Shannon C.E. Information Theory // Encyclopedia Britannica. 1972. Vol. 12. P. 246.

Учебное издание

Анатолий Николаевич Григорьев,
доктор педагогических наук, кандидат юридических наук, доцент
(Калининградский филиал Санкт-Петербургского университета
МВД России)

Павел Юрьевич Иванов
(Управление Министерства внутренних дел Российской Федерации
по Калининградской области)

Максим Александрович Касьянов
(Правительство Калининградской области)

Виолетта Владимировна Фадеева,
доктор педагогических наук, профессор
(Калининградский филиал Санкт-Петербургского университета
МВД России)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Редактор **А.Н. Григорьев.**

Оригинал-макет Калининградского филиала Санкт-Петербургского
университета МВД России

Подписано в печать 28.07.2018.
Формат 60×90 $^{1}/_{16}$. Бумага офсетная. Усл. печ. л. 13,0.
Тираж 1001 экз.. Заказ № 9213.

Макет подготовлен и отпечатан при участии ООО ИПК «Медиа-Принт»
143200, г. Можайск, ул. Мира, 93.

Для заметок

Для заметок

Для заметок

Для заметок