

МВД России
Санкт-Петербургский университет

Н.М. Мельников, А.В. Никишкин, Е.В. Ветрова

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Под общей редакцией Н.М. Мельникова

Санкт-Петербург
2024

УДК 004.5
ББК 32.972.5
Т46

Т46 **Технические средства защиты информации: учебное пособие /**
Н.М. Мельников, А.В. Никишкин, Е.В. Ветрова; под общ.ред.
Н.М. Мельникова. – Санкт-Петербург: СПбУ МВД России, 2024. –
304 с.

Авторский коллектив:

*Мельников Н.М. (введ., гл. 4, 6, закл.), Никишкин А.В. (гл. 1, 2),
Ветрова Е.В. (гл. 3, 5)*

ISBN 978-5-91837-832-8
EDN: YRZLSO

Учебное пособие соответствует разделу учебной программы дисциплины «Специальная техника органов внутренних дел» и содержит материал, раскрывающий основные понятия, классификацию, тактико-технические характеристики технических средств защиты информации органов внутренних дел и организационно-правовые аспекты их использования. Подробно описаны устройство, возможности и указаны сферы применения конкретных образцов технических средств защиты информации, состоящих на вооружении органов внутренних дел, которые изучаются на практических занятиях.

Предназначено для курсантов и слушателей, обучающихся в образовательных организациях системы МВД России.

УДК 004.5
ББК 32.972.5

Рецензенты:

Меняйло Д.В., кандидат юридических наук
(Белгородский юридический институт МВД России);
Кураков Д.В., кандидат юридических наук
(Орловский юридический институт МВД России)

ISBN 978-5-91837-832-8

© Санкт-Петербургский университет
МВД России, 2024

ОГЛАВЛЕНИЕ

Список условных сокращений	4
Глава. 1 НОРМАТИВНО-ПРАВОВАЯ БАЗА В ОБЛАСТИ ПРИМЕНЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	8
1.1. Нормативно-правовые акты в области защиты информации	8
1.2. Указы Президента РФ	39
1.3. Ведомственные приказа в области защиты информации	42
Глава. 2 ОРГАНИЗАЦИОННАЯ ОСНОВА ПРИМЕНЕНИЯ И КЛАССИФИКАЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	78
2.1. Понятие защиты информации	78
2.2. Разновидности организационных методов защиты информации	80
2.3. Особенности и виды технических средств защиты информации	83
Глава 3. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ОПТИЧЕСКИМ КАНАЛАМ	97
3.1. Защита информации от утечки по визуально-оптическому каналу	97
3.2. Характеристики оптического канала утечки информации	98
3.3. Организационно-технические способы защиты от утечки информации по оптическим каналам	105
Глава 4 ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО РАДИОЭЛЕКТРОННЫМ КАНАЛАМ	108
4.1. Информационная безопасность и особенности утечки информации	108
4.2. Беспроводная система предотвращения вторжений в информационных сетях	115
Глава 5 ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ	133
5.1. Понятия и определения средств защиты информации от утечек по акустическим каналам	133
5.2. Средства защиты от утечек по акустическим каналам информации	134
5.3. Средства защиты информации	141
от несанкционированного доступа	141
Глава 6 ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК	186
6.1. Методика оценки угроз безопасности информации	186
6.2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных	214
6.3. Типы изделий электромагнитного зашумления	234
ЗАКЛЮЧЕНИЕ	297
СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ	299

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

АС – автоматизированные системы;
АСПТП – автоматизированные системы управления производственными и технологическими процессами;
АТС – автоматические телефонные станции;
ВсТСС – вспомогательные технические средства и системы;
ВТСС – вычислительные технологические системы и средства;
ГИС – государственные информационные системы;
ЕСМЭД – Единая система межведомственного электронного диалога;
ЗАО – закрытое акционерное общество;
ИВК – информационно-вычислительный комплекс;
ИСПД – информационные системы персональных данных;
МЭ – межсетевое экранирование;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОАО – открыто акционерное общество;
ОС – операционная система;
ОТСС – основные технические средства и системы;
ПАК – программно-аппаратный комплекс;
ПД – персональные данные;
ПК – персональный компьютер;
ПО – программное обеспечение;
ПЭМИН – побочные электромагнитные излучения и наводки;
САЗ – система автоматической защиты;
СВР – служба внешней разведки;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации;
СЗИ НСД – система защиты информации от несанкционированного доступа;
СКН – средства контроля съемных машинных носителей информации;
СКУД – система контроля и управления доступом;
СОВ – система обнаружения вторжения;
ТСЗИ – технические средства защиты информации;
ТКУИ – технические каналы утечки информации;
ТСВР – технические средства ведения разведки;
ТСОИ – технические средства обработки информации;
ТСПИ – технические средства получения информации;
ТСР – технические средства разведки;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ВВЕДЕНИЕ

Профессионал своего дела должен умело использовать в своей деятельности специальные технические средства. К таким профессионалам относятся и сотрудники полиции. Личный состав подразделений органов внутренних дел должен не только знать тактико-технические характеристики специальных технических средств (СТС), но и умело их применять на практике при выполнении служебных и оперативных задач.

Злоумышленники всё чаще применяют на практике роботизированные технические и программные средства.

В 21 веке особый интерес представляет информация, и здесь вполне применим лозунг — «Информированный человек — значит вооружённый».

Во все времена человечество уделяло большое внимание информации, её передаче, приёму, обработке, хранению и защите от несанкционированного доступа. Ещё в Древнем Риме проявители понимали, что от того, как организованы работа с информацией и её защита, будет зависеть развитие государства как в промышленной, так и в военной сфере. Если в те далёкие времена хищение информации предполагало лишь физическое проникновение в охраняемое помещение, то в современном мире у злоумышленников появились изощрённые способы незаконного завладения ею. Одним из таких способов является использования цифровых технологий с применением вычислительной техники. Злоумышленников, которые пытаются незаконно завладеть информацией, представляющей определённый интерес, принято называть «хакерами» или «киберпреступниками». Их незаконные действия в некоторых случаях могут привести к различным довольно серьёзным последствиям — от причинённого материального или морального ущерба конкретному физическому лицу, до нанесения существенного вреда, вплоть до подрыва государственного строя целого государства.

Развитие современного общества неизбежно связано с развитием цифровизации. В свою очередь, в 21 веке цифровизация немыслима без информации. Цифровизация — это внедрение современных цифровых технологий в различные сферы жизни и производства. Информатизация — это системный, междисциплинарный процесс внедрения достижений методов информатики и новых информационных технологий в общественную жизнь, в научно-технические, социаль-

но-экономические, правовые и другие институты государства с целью повышения их эффективности, всестороннего развития личности.

Информатизация — одно из важнейших направлений научно-технического прогресса, основанное на широком применении микроэлектронной вычислительной техники, средств связи, автоматизированных банков данных, взаимоувязанных между собой в информационно-вычислительные системы. Эти два понятия настолько взаимосвязаны, что в современных реалиях не могут существовать по отдельности. Развитие цифровизации требует от человечества обработки колоссального объема информации. В современном мире люди научились проводить с информацией различного рода манипуляции. Принимая, обрабатывая, проводя различного рода манипуляции и передавая информацию, пользователь различные технические средства. Такими средствами могут быть компьютеры, гаджеты, устройства хранения и обработки информации. Использование любых технических средств в области манипуляций с информацией неизбежно ведёт к возникновению различного рода рисков, связанных с незаконным хищением как служебной, так и оперативно значимой информации. У каждой информационной системы, какой бы совершенной она не была, есть уязвимости. Серьёзными угрозами хищения информации являются субъективные и объективные причины. Поэтому ни одна система не гарантирует стопроцентной гарантии защиты информации. Такого рода риски могут привести к серьёзным последствиям.

В данном учебном пособии рассмотрены различные способы хищения информации и меры по борьбе или противодействию с ними. Цель работы — раскрытие всевозможных рисков, связанных с незаконным завладением информацией, и анализ мер и способов противодействия, исключения или минимизации таких рисков с учётом применения организационно-технических мер, направленных на защиту служебной и оперативно значимой информации органов внутренних дел.

Активное развитие информационных технологий, а также использование в человеческой жизнедеятельности информации формирует новые проблемы, сопряженные с формированием новых угроз в виде утечки конфиденциальных данных, их кражи, создания вирусных угроз. Подобные процессы преобразовали информацию в приоритетный товар, который является весьма ценным, вследствие чего она стала специфическим стратегическим ресурсом. При этом повысилась важность информации в различных областях жизнедеятельно-

сти человека, что обуславливается изменениями в социальной и экономической сферах, формированием новых достижений в сфере технологий, научных исследований.

Совершенствование технологий спровоцировало быстрое формирование и развитие киберпреступлений, преступности в сети Интернет, что затронуло также сферу интеллектуальной собственности и информационных технологий.

В настоящее время существует обширное число всевозможных угроз информационной безопасности, которые создаются человеком, а также без его участия. При этом ущерб, наносимый подобными угрозами, весьма серьезен, вследствие чего было сформировано понятие «киберпреступления», которые базируются на взломе и краже данных из корпоративных сетей, компьютеров пользователей, что подтверждает необходимость регулярного совершенствования сферы защиты информации, а также самих средств её защиты.

Эффективность технических средств защиты информации напрямую оказывает влияние на эффективность функционирования систем информационной безопасности, соответственно, от них зависит надежность хранения данных, сохранение конфиденциальности.

Глава 1

НОРМАТИВНО-ПРАВОВАЯ БАЗА В ОБЛАСТИ ПРИМЕНЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Нормативно-правовые акты в области защиты информации

*Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
(извлечения)*

Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персо-

нальных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

4) автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 7. Конфиденциальность персональных данных

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся

расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года № 8-ФЗ «О Всероссийской переписи населения»;

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными ор-

ганами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

Статья 11. Биометрические персональные данные

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных:

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных

информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке:

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для

выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным

данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (извлечения)

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

1) информация — сведения (сообщения, данные), независимо от формы их представления;

2) информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации — возможность получения информации и ее использования;

7) конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) электронный документ — 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;

12) оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети «Интернет» — совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

14) страница сайта в сети «Интернет» (далее также – интернет-страница) — часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет»;

15) доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет»;

16) сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

17) владелец сайта в сети «Интернет» — лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте;

18) провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет»;

19) единая система идентификации и аутентификации — федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законода-

тельством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

20) поисковая система — информационная система, осуществляющая по запросу пользователя поиск в сети «Интернет» информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети «Интернет» для доступа к запрашиваемой информации, расположенной на сайтах в сети «Интернет», принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных

технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 6. Владелец информации

1. Владелелем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования полномочия владельца информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Владелец информации, если иное не предусмотрено федеральными законами, вправе:

- 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
- 3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2.1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности

(профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В государственных органах, органах местного самоуправления документирование информации осуществляется в соответствии с правилами делопроизводства, установленными уполномоченным федеральным органом исполнительной власти в сфере архивного дела и делопроизводства.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 11.1. Обмен информацией в форме электронных документов при осуществлении полномочий органов государственной власти и органов местного самоуправления

1. Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

2. Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулирующими правоотношения в установленной сфере деятельности.

3. Требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия, и порядок такого взаимодействия устанавливаются Правительством Российской Федерации в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются, модернизируются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд либо законодательством Российской Федерации о государственно-частном партнерстве, о муниципально-частном партнерстве, законодательством о концессионных соглашениях.

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления — Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», государственные информационные системы должны обеспечивать размещение такой информации в сети «Интернет» в форме открытых данных.

4.1. Правительство Российской Федерации определяет случаи, при которых доступ с использованием сети «Интернет» к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе идентификации и аутентификации, а также порядок использования единой системы идентификации и аутентификации.

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

5.1. В случае создания или модернизации государственной информационной системы на основании концессионного соглашения или соглашения о государственно-частном партнерстве функции оператора данной системы в пределах, в объемах и в сроки, которые предусмотрены соответствующим соглашением, осуществляются концессионером или частным партнером.

6. Правительство Российской Федерации утверждает требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, дальнейшего хранения содержащейся в их базах данных информации, включающие в себя перечень, содержание и сроки реализации этапов мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, дальнейшему хранению содержащейся в их базах данных информации.

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в слу-

чаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Статья 14.1. Применение информационных технологий в целях идентификации граждан Российской Федерации

1. Государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при личном присутствии гражданина Российской Федерации с его согласия на безвозмездной основе размещают в электронной форме:

1) сведения, необходимые для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и иные сведения, если такие сведения предусмотрены федеральными законами, – в единой системе идентификации и аутентификации;

2) биометрические персональные данные гражданина Российской Федерации – в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее – единая биометрическая система).

2. Правительство Российской Федерации по согласованию с Центральным банком Российской Федерации устанавливает требования:

1) к фиксации действий при размещении сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи;

2) к проведению государственными органами и организациями, указанными в части 1 настоящей статьи, идентификации гражданина Российской Федерации, за исключением организаций, проводящих такую идентификацию в порядке, установленном Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

3. Федеральные законы, устанавливающие обязанность государственных органов и организаций по размещению сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи, должны предусматривать осуществление контроля и надзора за соответствующими дей-

ствиями, а также определение органа государственной власти или организации, уполномоченных на их осуществление.

4. Сведения, указанные в пунктах 1 и 2 части 1 настоящей статьи, размещаются соответственно в единой системе идентификации и аутентификации и в единой биометрической системе уполномоченным сотрудником государственного органа или организации и подписываются усиленной квалифицированной электронной подписью такого государственного органа или организации.

5. Форма согласия на обработку персональных данных и биометрических персональных данных, указанных в пунктах 1 и 2 части 1 настоящей статьи, утверждается Правительством Российской Федерации.

6. Порядок регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, включая состав сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, порядок и сроки проверки и обновления сведений, размещаемых в единой системе идентификации и аутентификации с использованием государственных информационных систем, устанавливаются Правительством Российской Федерации. Федеральные органы исполнительной власти, в том числе федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, органы государственных внебюджетных фондов направляют в единую систему идентификации и аутентификации сведения о гражданах Российской Федерации в целях их обновления в соответствии с указанным порядком.

7. В случаях, установленных федеральными законами, государственные органы и организации вправе обновлять информацию о гражданах Российской Федерации, идентифицированных в соответствии с частью 18 настоящей статьи, с использованием сведений, полученных из единой системы идентификации и аутентификации.

8. Состав сведений, размещаемых в единой биометрической системе, включая вид биометрических персональных данных, определяется Правительством Российской Федерации.

9. Обработка биометрических персональных данных в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в том числе с использованием единой биометрической системы, осуществляется в соответствии с требо-

ваниями к защите биометрических персональных данных, установленными в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», при обработке персональных данных в единой биометрической системе, за исключением контроля и надзора за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий, установленных законодательством Российской Федерации о персональных данных.

11. Контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы осуществляются Центральным банком Российской Федерации.

12. Правительство Российской Федерации определяет федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных.

13. Федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных:

1) определяет порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации (в банковской сфере и иных сферах финансового рынка указанные требования устанавливаются по согласованию с Центральным банком Российской Федерации);

2) определяет формы подтверждения соответствия информационных технологий и технических средств, предназначенных для об-

работки биометрических персональных данных в целях проведения идентификации, требованиям, определенным в соответствии с пунктом 1 настоящей части, и публикует перечень технологий и средств, имеющих подтверждение соответствия (в банковской сфере и иных сферах финансового рынка формы подтверждения соответствия устанавливаются по согласованию с Центральным банком Российской Федерации);

3) разрабатывает и утверждает методики проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе, а также определяет степень взаимного соответствия указанных биометрических персональных данных, достаточную для проведения идентификации, предусмотренной настоящим Федеральным законом.

14. Центральный банк Российской Федерации совместно с оператором единой биометрической системы определяет перечень угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в единой биометрической системе с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и согласовывает указанный перечень с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

15. Государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи, оператор единой биометрической системы при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и определении степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации:

1) осуществляют свои функции в соответствии с законодательством Российской Федерации о персональных данных и требованиями настоящего Федерального закона;

2) осуществляют обработку, включая сбор и хранение, биометрических персональных данных с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом;

3) обеспечивают проверку соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным согласно методикам, утвержденным в соответствии с настоящим Федеральным законом.

16. Оператор единой биометрической системы:

1) осуществляет передачу информации о результатах проверки соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в единой биометрической системе, в государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи;

2) предоставляет в федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, и федеральный орган исполнительной власти в области обеспечения безопасности в целях обеспечения обороны страны, безопасности государства, охраны правопорядка и противодействия терроризму сведения, содержащиеся в единой биометрической системе, в порядке, установленном Правительством Российской Федерации.

17. Функции оператора единой биометрической системы возлагаются Правительством Российской Федерации на оператора, занимающего существенное положение в сети связи общего пользования на территориях не менее чем двух третей субъектов Российской Федерации.

18. Идентификация гражданина Российской Федерации с применением информационных технологий осуществляется без его личного присутствия в случаях, установленных федеральными законами, путем предоставления государственным органам и организациям:

1) сведений о гражданине Российской Федерации, размещенных в единой системе идентификации и аутентификации, в порядке, установленном Правительством Российской Федерации;

2) информации о степени соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его

биометрическим персональным данным, содержащимся в единой биометрической системе.

19. При предоставлении биометрических персональных данных физического лица по каналам связи в целях проведения его идентификации без личного присутствия посредством сети «Интернет» должны применяться шифровальные (криптографические) средства, позволяющие обеспечить безопасность передаваемых данных от угроз безопасности, актуальных при обработке биометрических персональных данных, определенных в соответствии с частью 14 настоящей статьи, и имеющие подтверждение соответствия требованиям, установленным в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Государственный орган, банк или иная организация, указанные в абзаце первой части 1 настоящей статьи, обязаны предложить использовать указанные средства физическим лицам, обратившимся к ним в целях проведения идентификации без личного присутствия, и указать страницу сайта в сети «Интернет», с которой предоставляются эти средства.

20. В случае если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия посредством сети «Интернет» использует мобильный телефон, смартфон или планшетный компьютер и отказывается от использования шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первой части 1 настоящей статьи, обязаны отказать такому лицу в проведении указанной идентификации.

21. В случае, если физическое лицо при предоставлении своих биометрических персональных данных в целях проведения идентификации без личного присутствия посредством сети «Интернет» использует иные устройства, в том числе персональный компьютер, и отказывается от применения шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первой части 1 настоящей статьи, уведомляет его о рисках, связанных с таким отказом. После подтверждения физическим лицом своего решения государственный орган, банк или иная организация, указанные в абзаце первой части 1 настоящей статьи, может провести соответствующую идентификацию физического лица посредством сети «Интернет» без

использования им указанных шифровальных (криптографических) средств.

22. Государственные органы, банки и иные организации при проведении идентификации гражданина Российской Федерации с применением информационных технологий в соответствии с частью 18 настоящей статьи вправе подтверждать достоверность сведений, предусмотренных пунктом 1 части 18 настоящей статьи, с использованием информационных систем государственных органов, в том числе федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования и (или) государственной информационной системы, определенной Правительством Российской Федерации.

23. Согласие гражданина Российской Федерации на обработку персональных данных, содержащихся в единой системе идентификации и аутентификации, и биометрических персональных данных для проведения его идентификации с применением информационных технологий в соответствии с частью 18 настоящей статьи может быть подписано его простой электронной подписью, ключ которой получен в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации. Указанное согласие, подписанное простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного гражданина Российской Федерации.

24. Размер и порядок взимания оператором единой биометрической системы платы за предоставление государственным органам и организациям сведений, указанных в пункте 2 части 18 настоящей статьи, определяются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, по согласованию с оператором единой биометрической системы и иными государственными органами и организациями в случаях, установленных федеральными законами.

*Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»
(извлечения)*

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) *электронная подпись* — 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;

2) *сертификат ключа проверки электронной подписи* — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) *квалифицированный сертификат ключа проверки электронной подписи (далее — квалифицированный сертификат)* — сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее — уполномоченный федеральный орган);

4) *владелец сертификата ключа проверки электронной подписи* — лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) *ключ электронной подписи* — уникальная последовательность символов, предназначенная для создания электронной подписи;

6) *ключ проверки электронной подписи* — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее — проверка электронной подписи);

7) *удостоверяющий центр* — юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) *аккредитация удостоверяющего центра* — признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

9) *средства электронной подписи* — шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций — создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) *средства удостоверяющего центра* — программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) *участники электронного взаимодействия* — осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

12) *корпоративная информационная система* — информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) *информационная система общего пользования* — информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

14) *вручение сертификата ключа проверки электронной подписи* — передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

15) *подтверждение владения ключом электронной подписи* — получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки элек-

тронной подписи, указанному таким лицом для получения сертификата.

Статья 3. Правовое регулирование отношений в области использования электронных подписей

1. Отношения в области использования электронных подписей регулируются настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия. Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации.

Статья 4. Принципы использования электронной подписи

Принципами использования электронной подписи являются:

1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической

силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Статья 5. Виды электронных подписей

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее — неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее — квалифицированная электронная подпись).

2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3. Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

5. При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неква-

лифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами

1. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.

2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права.

Статья 8. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи

1. Уполномоченный федеральный орган определяется Правительством Российской Федерации.

2. Уполномоченный федеральный орган:

1) осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в том числе требований, на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае выявления несоблюдения этих требований выдает предписания об устранении выявленных нарушений;

2) осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров.

3. Уполномоченный федеральный орган обязан обеспечить хранение следующей указанной в настоящей части информации и круглосуточный беспрепятственный доступ к ней с использованием информационно-телекоммуникационных сетей:

1) наименования, адреса аккредитованных удостоверяющих центров;

2) реестр выданных уполномоченным федеральным органом квалифицированных сертификатов;

3) перечень удостоверяющих центров, аккредитация которых досрочно прекращена;

4) перечень аккредитованных удостоверяющих центров, аккредитация которых приостановлена;

5) перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;

6) реестры выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов, переданные в уполномоченный федеральный орган в соответствии со статьей 15 настоящего Федерального закона.

4. Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, устанавливает:

1) порядок передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов и иной информации в уполномоченный федеральный орган в случае прекращения деятельности аккредитованного удостоверяющего центра;

2) порядок формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов, а также предоставления информации из таких реестров;

3) правила аккредитации удостоверяющих центров, порядок проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в том числе требований, на соответствие которым эти удостоверяющие центры были аккредитованы.

4) требования к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности;

5) формат электронной подписи, обязательный для реализации всеми средствами электронной подписи, по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности.

5. Федеральный орган исполнительной власти в области обеспечения безопасности:

1) по согласованию с уполномоченным федеральным органом устанавливает требования к форме квалифицированного сертификата и правила подтверждения владения ключом электронной подписи;

2) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра;

3) осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с настоящим Федеральным законом, и публикует перечень таких средств;

4) по согласованию с уполномоченным федеральным органом устанавливает дополнительные требования к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, а также к обеспечению информационной безопасности аккредитованного удостоверяющего центра.

Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

1.2. Указы Президента РФ

Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»

1. 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.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

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

4. 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, телеграфных или иных сообщений и так далее).

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

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

7. 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».

**Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах
информационной безопасности Российской Федерации»**

В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации постановляю:

1. Преобразовать сегмент международной компьютерной сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, в российский государственный сегмент информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), являющийся элементом российской части сети «Интернет» и обеспечивающий:

а) подключение к сети «Интернет» предназначенных для взаимодействия с ней государственных информационных систем и информационно-телекоммуникационных сетей государственных органов, а также информационных систем и информационно-телекоммуникационных сетей организаций, созданных для выполнения задач, поставленных перед федеральными государственными органами;

б) размещение (публикацию) в сети «Интернет» информации государственных органов и названных в подпункте «а» настоящего пункта организаций.

2. Утвердить прилагаемый порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет».

3. Федеральной службе охраны Российской Федерации обеспечивать поддержание, эксплуатацию и развитие российского государственного сегмента сети «Интернет».

4. Администрации Президента Российской Федерации, Аппарату Правительства Российской Федерации, Следственному комитету Российской Федерации, федеральным органам исполнительной власти и органам исполнительной власти субъектов Российской Федерации осуществить до 31 декабря 2017 г. подключение находящихся в их ведении государственных информационных систем и информа-

ционно-телекоммуникационных сетей к российскому государственному сегменту сети «Интернет» и обеспечить размещение (публикацию) информации в сети «Интернет» в соответствии с порядком, утвержденным настоящим Указом.

5. Рекомендовать Совету Федерации Федерального Собрания Российской Федерации, Государственной Думе Федерального Собрания Российской Федерации, судебным органам Российской Федерации, органам прокуратуры Российской Федерации, Счетной палате Российской Федерации, а также организациям, созданным для выполнения задач, поставленных перед федеральными государственными органами, осуществить подключение находящихся в ведении названных органов и организаций информационных систем и информационно-телекоммуникационных сетей к российскому государственному сегменту сети «Интернет» и обеспечить размещение (публикацию) информации в сети «Интернет» в соответствии с порядком, утвержденным настоящим Указом.

6. Признать утратившими силу:

пункты 2 и 3 Указа 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» (Собрание законодательства Российской Федерации, 2008, № 12, ст. 1110);

пункт 22 приложения к Указу Президента Российской Федерации от 21 октября 2008 г. № 1510 «О внесении изменений в некоторые акты Президента Российской Федерации в связи с образованием Следственного комитета при прокуратуре Российской Федерации» (Собрание законодательства Российской Федерации, 2008, №43, ст. 4919);

пункт 26 приложения к Указу Президента Российской Федерации от 14 января 2011 г. № 38 «Вопросы деятельности Следственного комитета Российской Федерации» (Собрание законодательства Российской Федерации, 2011, № 4, ст. 572);

пункт 23 приложения № 1 к Указу Президента Российской Федерации от 1 июля 2014 г. № 483 «Об изменении и признании утратившими силу некоторых актов Президента Российской Федерации» (Собрание законодательства Российской Федерации, 2014, №27, ст. 3754);

пункт 24 приложения № 1 к Указу Президента Российской Федерации от 25 июля 2014 г. № 529 «Об изменении и признании утратившими силу некоторых актов Президента Российской Федерации» (Собрание законодательства Российской Федерации, 2014, № 30, ст. 4286).

1.3. Ведомственные приказа в области защиты информации

Приказы ФСТЭК России

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

I. Общие положения

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее — информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

В электронном документе нумерация пунктов соответствует официальному источнику.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328).

II. Состав и содержание мер по обеспечению безопасности персональных данных

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с

учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее — машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее — инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и приви-

легиями субъектов доступа, разграничение доступа субъектов доступа объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности

информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее — средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством

применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечива-

ющими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

- проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

- тестирование информационной системы на проникновения;

- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

- в информационных системах 1 уровня защищенности персональных данных применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 2 уровня защищенности персональных данных применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 3 уровня защищенности персональных данных применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 4 уровня защищенности персональных данных применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса.

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

При использовании в информационных системах средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение мер по обеспечению безопасности персональных данных, содержащихся в настоящем документе.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются сертифицированные средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (извлечения)

I. Общие положения

2. В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее — информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее — защита информации) при обработке указанной информации в государственных информационных системах.

Настоящие Требования могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

3. Настоящие Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

Настоящие Требования не распространяются на государственные информационные системы Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации.

4. Настоящие Требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на

создание государственной информационной системы (далее — заказчики) и операторов государственных информационных систем (далее — операторы).

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее — уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с настоящими Требованиями.

5. При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации

от 1 ноября 2012 г. № 1119.

6. По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах.

7. Защита информации, содержащейся в государственной информационной системе (далее — информационная система), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

II. Требования к организации защиты информации, содержащейся в информационной системе

8. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой,

графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

9. Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

10. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. 99-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2011, № 19, ст. 2716; № 30, ст. 4590; № 43, ст. 5971; № 48, ст. 6728; 2012, № 26, ст. 3446; № 31, ст. 4322; 2013, № 9, ст. 874).

11. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, № 52, ст. 5140; 2007, № 19, ст. 2293; № 49, ст. 6070; 2008, № 30, ст. 3616; 2009, № 29, ст. 3626; № 48, ст. 5711; 2010, № 1, ст. 6; 2011, № 30, ст. 4603; № 49, ст. 7025; № 50, ст. 7351; 2012, № 31, ст. 4322; 2012, № 50, ст. 6959).

12. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее — система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информаци-

онной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

13. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее — аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

*Формирование требований к защите информации,
содержащейся в информационной системе*

14. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется владельцем информации (заказчиком).

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ

HYPERLINK
«<https://normativ.kontur.ru/document?moduleId=1&documentId=219322>»

«<https://normativ.kontur.ru/document?moduleId=1&documentId=219322>» 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее — ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее — ГОСТ Р 51624) и в том числе включает:

- принятие решения о необходимости защиты информации, содержащейся в информационной системе;

- классификацию информационной системы по требованиям защиты информации (далее — классификация информационной системы);

- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

- определение требований к системе защиты информации информационной системы.

14.1. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

- анализ целей создания информационной системы и задач, решаемых этой информационной системой;

- определение информации, подлежащей обработке в информационной системе;

- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

- принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации (заказчика), оператора и уполномоченных лиц.

14.2. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней

информации. Самый низкий класс — третий, самый высокий — первый. Класс защищенности информационной системы определяется в соответствии с приложением № 1 к настоящим Требованиям.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее — ГОСТ 34.602), ГОСТ 51583 и ГОСТ Р 51624.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

14.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 53, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211) (далее — банк данных угроз безопасности информации ФСТЭК России), а также иные источники, содержащие сведения об уязвимостях и угрозах 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.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818).

14.4. Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

класс защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

стадии (этапы работ) создания системы защиты информационной системы;

требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

функции заказчика и оператора по обеспечению защиты информации в информационной системе;

требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).

Разработка системы защиты информации информационной системы

15. Разработка системы защиты информации информационной системы организуется обладателем информации (заказчиком).

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием

(частным техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее — ГОСТ 34.601), ГОСТ 51583 и ГОСТ Р 51624 и в том числе включает:

- проектирование системы защиты информации информационной системы;

- разработку эксплуатационной документации на систему защиты информации информационной системы;

- макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также применение вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

15.1. При проектировании системы защиты информации информационной системы:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

- определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

- выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы;

- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Результаты проектирования системы защиты информации информационной системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы), разрабатываемых с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее — ГОСТ 34.201).

Проектная документация на информационную систему и (или) ее систему защиты информации подлежат согласованию с оператором информационной системы в случае, если он определен таковым в соответствии с законодательством Российской Федерации к моменту окончания проектирования системы защиты информации информационной системы и не является заказчиком данной информационной системы.

При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством

Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

15.2. Разработка эксплуатационной документации на систему защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы.

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ 51624 и должна в том числе содержать описание:

- структуры системы защиты информации информационной системы;

- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;

- правил эксплуатации системы защиты информации информационной системы.

15.3. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

- проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

- проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы;

- корректировка проектных решений, разработанных при создании информационной системы и (или) системы защиты информации информационной системы;

Макетирование системы защиты информации информационной системы и ее тестирование может проводиться в том числе с использованием средств и методов моделирования информационных систем и технологий виртуализации.

Внедрение системы защиты информации информационной системы

16. Внедрение системы защиты информации информационной системы организуется обладателем информации (заказчиком).

Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

- установку и настройку средств защиты информации в информационной системе;

- разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее — организационно-распорядительные документы по защите информации);

- внедрение организационных мер защиты информации;

- предварительные испытания системы защиты информации информационной системы;

- опытную эксплуатацию системы защиты информации информационной системы;

- анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

- приемочные испытания системы защиты информации информационной системы.

К внедрению системы защиты информации информационной системы привлекается оператор информационной системы в случае, если он определен таковым в соответствии с законодательством Российской Федерации к моменту внедрения системы защиты информации информационной системы и не является заказчиком данной информационной системы.

16.1. Установка и настройка средств защиты информации в информационной системе должна проводиться в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

16.2. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

- управления (администрирования) системой защиты информации информационной системы;

выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее — инциденты), и реагирования на них;

управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;

контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

16.3. При внедрении организационных мер защиты информации осуществляются:

реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

16.4. Предварительные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем» (далее — ГОСТ 34.603) и включают проверку работоспособности системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.

16.5. Опытная эксплуатация системы защиты информации информационной системы проводится с учетом ГОСТ 34.603 и включает проверку функционирования системы защиты информации информационной системы, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

16.6. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы за-

щиты информации информационной системы и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

16.7. Приемочные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы.

Аттестация информационной системы и ввод ее в действие

17. Аттестация информационной системы организуется обладателем информации (заказчиком) или оператором и включает проведение комплекса организационных и технических мероприятий (атте-

стационарных испытаний), в результате которых подтверждается соответствие системы защиты информации информационной системы настоящим Требованиям.

Проведение аттестационных испытаний информационной системы должностными лицами, осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается (в ред. приказа ФСТЭК России от 15.02.2017 № 27).

17.1. В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями.

17.2. Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации информационной си-

системы установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования информационной системы;

анализ уязвимостей информационной системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации.

17.3. Допускается аттестация информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

В этом случае распространение аттестата соответствия на другие сегменты информационной системы осуществляется при условии их соответствия сегментам информационной системы, прошедшим аттестационные испытания.

Сегмент считается соответствующим сегменту информационной системы, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

Соответствие сегмента, на который распространяется аттестат соответствия, сегменту информационной системы, в отношении которого были проведены аттестационные испытания, подтверждается в ходе приемочных испытаний информационной системы или сегментов информационной системы.

В сегментах информационной системы, на которые распространяется аттестат соответствия, оператор обеспечивается соблюдение эксплуатационной документации на систему защиты информации информационной системы и организационно-распорядительных документов по защите информации.

Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты информационной системы определяют-

ся в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

17.4. Повторная аттестация информационной системы осуществляется по окончании срока действия аттестата соответствия, который не может превышать 5 лет, или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

17.5. Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

17.6. Информационные системы, функционирующие на базе общей инфраструктуры (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, подлежат аттестации в составе указанной инфраструктуры.

В случае, если информационная система создается на базе центра обработки данных уполномоченного лица, такой центр обработки данных должен быть аттестован по классу защищенности не ниже класса защищенности, установленного для создаваемой информационной системы.

При аттестации информационной системы должны использоваться результаты аттестации общей инфраструктуры оператора информационной системы.

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

18. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

управление (администрирование) системой защиты информации информационной системы;

выявление инцидентов и реагирование на них;

управление конфигурацией аттестованной информационной системы и ее системы защиты информации;

контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

18.1. В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;

управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

централизованное управление системой защиты информации информационной системы (при необходимости);

регистрация и анализ событий в информационной системе, связанных с защитой информации (далее — события безопасности);

информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;

сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации;

18.2. В ходе выявления инцидентов и реагирования на них осуществляются:

определение лиц, ответственных за выявление инцидентов и реагирование на них;

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору ин-

формации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

18.3. В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются:

поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации);

определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению

изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;

определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;

принятие решения по результатам управления конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

18.4. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

контроль за событиями безопасности и действиями пользователей в информационной системе;

контроль (анализ) защищенности информации, содержащейся в информационной системе;

анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (мо-

дернизации) системы защиты информации информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

19. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

архивирование информации, содержащейся в информационной системе;

уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

19.1. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

19.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

III. Требования к мерам защиты информации, содержащейся в информационной системе

20. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, ис-

пользуемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защиту машинных носителей информации;

регистрацию событий безопасности;

антивирусную защиту;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

целостность информационной системы и информации;

доступность информации;

защиту среды виртуализации;

защиту технических средств;

защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении № 2 к настоящим Требованиям.

20.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

20.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

20.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

20.4. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

20.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

20.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

20.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

20.8. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

20.9. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

20.10. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной

системе, в штатном режиме функционирования информационной системы.

20.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

20.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее — средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

20.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

21. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации, приведенными в приложении № 2 к настоящим Требованиям;

адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информаци-

онной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении № 2 к настоящим Требованиям, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №1085.

22. В информационной системе соответствующего класса защищенности в рамках ее системы защиты информации должны быть реализованы меры защиты информации, выбранные в соответствии с пунктом 21 настоящих Требования и обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации.

При этом в информационной системе должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

23. При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие)

меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

24. Меры защиты информации выбираются и реализуются в информационной системе в рамках ее системы защиты информации с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации и облачных вычислений.

25. Организационные меры и средства защиты информации, применяемые в информационной системе, должны обеспечивать:

в информационных системах 1 класса защищенности — защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом;

в информационных системах 2 класса защищенности — защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже усиленного базового;

в информационных системах 3 класса защищенности — защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже базового.

Потенциал нарушителей определяется в ходе оценки их возможностей, проводимой при определении угроз безопасности информации в соответствии с пунктом 14.3 настоящих Требований.

Оператором может быть принято решение о применении в информационной системе соответствующего класса защищенности мер защиты информации, обеспечивающих защиту от угроз безопасности информации, реализуемых нарушителями с более высоким потенциалом.

26. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При этом:

в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей.

Классы защиты определяются в соответствии с нормативными правовыми актами ФСТЭК России, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение настоящих Требований.

27. В случае обработки в информационной системе информации, содержащей персональные данные, реализуемые в соответствии с пунктами 21 и 22 настоящих Требований меры защиты информации:

для информационной системы 1 класса защищенности обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных;

Устанавливается в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Вопросы и задания для самоконтроля

1. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных.
2. Формирование требований к защите информации, содержащейся в информационной системе.
3. Методы проверок информационной системы при проведении аттестационных испытаний.
4. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним.
5. Уровни защищенности персональных данных в информационных системах.
6. Основные направления обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства.
7. Задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности.

Глава 2

ОРГАНИЗАЦИОННАЯ ОСНОВА ПРИМЕНЕНИЯ И КЛАССИФИКАЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Понятие защиты информации

Защита информации представляется направлениями применения всевозможных средств и методов, мероприятий, нацеленных на системное обеспечение надежности информации, которая проходит этапы передачи, обработки и хранения.

В современном мире выделяются приоритетные задачи, при решении которых в рамках информационных систем (далее ИС), а также телекоммуникационных сетей (далее ТС) обеспечивается эффективная защита информации. К данным задачам причисляются:

- реализация направлений организации доступа к данным лишь определенных лиц;
- подтверждение подлинности данных;
- реализация мер по защите от перехвата данных при передаче по каналам связи;
- реализация мер защиты от искажения и ввода ложных данных¹ [1, с. 31].

Под защитой информации понимается также обеспечение физической ее целостности, то есть не допущения искажения или уничтожения составляющих данных, при этом подразумевается недопущение подмены составляющих данных, а также недопущение несанкционированного доступа к данным со стороны лиц или процессов, которые не обладают полномочиями на это. Немаловажным представляется и то, что пользователи и владельцы данных должны обладать уверенностью в том, что передаваемая информация будет применена, лишь опираясь на условия применения.

Ниже приведены приоритетные методы и средства защиты информации (рис. 2.1).

¹ Здесь и далее в квадратных скобках указан порядковый номер источника из списка рекомендуемой литературы и конкретные страницы.



Рис. 2.1. Основные методы и средства защиты информации [11, с. 104]

Под угрозой безопасности понимается единство условий и факторов, посредством которых формируются возможные или существующие в действительности опасности, сопряженные с утечкой данных, связанных с несанкционированным и преднамеренным влиянием на них (рис. 2.2) [2, с. 57].

Приоритетными разновидностями угроз, существующих при наличии уязвимости в отношении особенностей данных, представляются:

- наличие конфиденциальных данных, вследствие чего осуществляется несанкционированный доступ к ним и их дальнейшее доведение до потребителя, который не обладает правами доступа к подобным данным;
- реализация несанкционированного доступа, подразумевающего получение защищенных данных заинтересованными лицами, что подразумевает нарушение определенных правовой документацией, а также владельцами данных прав или стандартов доступа к данным;
- осуществление непреднамеренных или несанкционированных действий, сопряженных с изменением, искажением, копированием, уничтожением данных, а также блокированием доступа к ним;
- уничтожение, а также сбои в функционировании носителей информации, сопряженных с непреднамеренным или несанкционированным воздействием [3, с.314].



Рис. 2.2. Разновидности угроз безопасности информации

Таким образом, разрешение проблем, сопряженных с защитой информации, возможно посредством применения современных методов, средств защиты, а также криптографических методов, позволяющих надежно защищать данные. При этом существующие методы и средства позволяют удерживать эффективность функционирования автоматизированных систем на высоком уровне, что значимо вследствие обширного распространения электронной информации.

Использование комплекса методов и средств (организационных мер и технических средств) позволяют формировать требуемый уровень защиты информации от современных угроз и утечки.

2.2. Разновидности организационных методов защиты информации

Современные организационные мероприятия и методы защиты подразумевают под собой использование мер и способов организационной направленности, которыми регламентируются процессы работы систем обработки информации, а также применения ресурсов, деятельности сотрудников, в том числе порядка взаимодействия пользователей с системой, которые позволяют минимизировать или ис-

ключить возможности формирования утечки данных или угроз безопасности [4, с.243].

Приведенные организационные методы базируются на принципе управления предприятиями, учреждениями, коллективами, а также принципе законности, при этом они подразумевают:

- реализацию мер, направленных на проектирование, создание и оборудование вычислительных центров и иных объектов, связанных с обработкой информации;
- реализацию мер, связанных с созданием правил доступа к информационным ресурсам (формирование политики безопасности);
- реализацию мер, связанных с подбором и подготовкой сотрудников, обладающих доступом к информационной системе;
- осуществление направлений организации защиты информации и пропускного режима;
- осуществление направлений организации учета, хранения, применения, уничтожения документации и носителей с данными;
- реализацию распределения реквизитов разграничения доступа, подразумевающую использование ключей шифрования, паролей;
- реализацию направлений организации скрытого и явного контроля над деятельностью пользователей в системе;
- меры, которые сопряжены с проектированием, разработкой, модификацией оборудования и программного обеспечения.

Под организационными мерами в рамках защиты информации понимаются направления в ситуациях, когда прочие методы и средства защиты информации отсутствуют, либо ими не обеспечивается необходимый уровень защиты. При этом система защиты не должна выстраиваться лишь на основе организационных мер, поскольку значимым представляется и использование современных технических средств.

Ниже приведены основные направления организационной защиты информации (рис. 2.3).

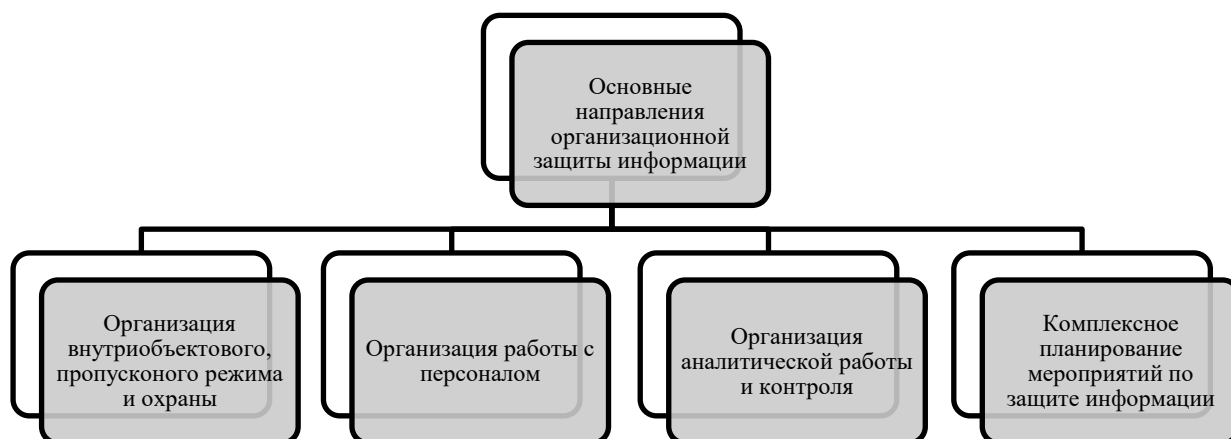


Рис. 2.3. Основные направления организационной защиты информации

Организационные меры требуются, чтобы обеспечивать действенное использование мер и средств защиты, затрагивающих регламентацию действий лиц. При этом организационные меры требуют поддержания посредством более надежных физических и технических средств.

Организационная защита данных является регламентацией производственной деятельности, а также взаимоотношений лиц, основанных на нормативно-правовой базе, что исключает неправомерное овладение конфиденциальными данными, включая организацию режимов защиты, деятельности с персоналом, с документацией, организацию применения технических средств, а также деятельность, связанную с исследованием существующих угроз информационной безопасности [5, с.36].

Обеспечение направлений защиты средств обработки данных, в том числе автоматизированных рабочих мест, от противозаконного доступа возможно посредством разделения доступа лиц к информации. При этом данная система использует программно-технические комплексы, системы управления базами данных, методы контроля доступа, а также криптографические преобразования.

При формировании систем защиты информации значимым представляется то, что система содержит в себе подсистемы, к которым причисляются управление доступом, регистрация и учет, методы криптографической защиты данных, а также обеспечение целостности информации.

Организационные направления защиты данных нацелены на подбор определенных сил и средств, позволяющих на практике осуществлять меры, связанные с защитой данных. При этом данные направле-

ния реализуются, опираясь на определенную обстановку, а также существующие угрозы, которые оказывают влияние на защищаемые данные, что провоцирует их утечку.

Таким образом, к организационным направлениям защиты данных можно причислить:

- осуществление организации взаимодействия с сотрудниками;
- осуществление организации внутриобъектового и пропускного режимов и защиты;
- организация деятельности с носителями информации;
- осуществление комплексного планирования мер, направленных на защиту данных;
- организацию аналитической деятельности и контроля [4, с. 152].

Следует отметить, что организационные методы защиты данных подразделяются на организационно-административные и организационно-технические, при этом ими затрагиваются все составляющие автоматизированных систем.

Таким образом, организационно-техническая защита данных базируется на реализации мер, сопряженных с ограничением доступа сторонних лиц внутрь корпуса оборудования посредством установки механических запорных устройств, отключения компьютеров от локальных сетей или сетей удаленного доступа при осуществлении обработки конфиденциальных данных.

2.3. Особенности и виды технических средств защиты информации

Основные методы и виды технических средств защиты информации

Методы и средства организационной защиты информации содержат в себе как организационно-технические, так и организационно-правовые меры, которые реализуются при формировании и использовании информационных систем, подразумевающих необходимость защиты данных. Ниже приведены основные методы защиты информации (рис. 2.4).

Организационные меры базируются на применении и подготовке законодательной и нормативной документации в сфере информационной безопасности, которые с позиции права регулируют доступ к данным со стороны пользователей. При этом немаловажным представляется исследование средств защиты информации.



Рис. 2.4. Основные методы защиты информации

Направления инженерно-технической защиты являются единственным специальными органами, техническими средствами и мерами, направленными на их использование для защиты конфиденциальных данных.

На современном этапе существуют различные цели, задачи, а также объекты и меры защиты, что подразумевает необходимость исследования классификации средств по видам, характеристикам, к примеру, средства инженерно-технической защиты исследуются по объектам их воздействия, при этом они используются как для защиты лиц, так и для защиты материальных средств, данных и финансов.

Существует множество характеристик, на которых основывается классификация. При этом наиболее подходящим представляется разделение инженерно-технических средств по объектам воздействия, специфике мер, методам реализации, масштабам охвата, разновидности злоумышленников.

Следует отметить, что, опираясь на функциональное назначение, средства инженерно-технической защиты подразделяются:

- на физические средства, которые содержат средства и сооружения, формирующие барьеры для проникновения злоумышленников к объектам защиты;
- аппаратные средства, к которым причисляются приборы, устройства, оборудование и прочие технические решения, которые применяются для защиты данных.

С позиции практики обширно используется аппаратура, а также автоматизированные системы, которыми обеспечивается определенный уровень защиты данных. При этом аппаратные средства нацелены на обеспечение надежной защиты данных от утечки и несанкционированного доступа.

Также к рассматриваемой группе причисляются программные средства, которыми затрагивается специализированное программное обеспечение, системы определенного назначения и средства обработки данных. Существуют и криптографические средства, являющиеся специальными математическими и алгоритмическими средствами защиты данных, которые передаются по системам и каналам связи, а также хранятся и обрабатываются на компьютерах, что подразумевает применение определенных шифровальных методов.

Также существуют физические методы и средства защиты информации, под которыми понимается использование всевозможных устройств, конструкций, аппаратов, изделий, необходимых для формирования барьеров на пути злоумышленников.

Физическими средствами являются электронные, механические, электронно-оптические, радиотехнические и прочие устройства, препятствующие незаконному доступу, а также выходу средств и информации. При этом данные средства используются для решения определенных задач, к которым причисляются:

- защита территорий учреждений, компаний, предприятий и контроль за ними;
- защита зданий, помещений, а также осуществление контроля над ними;
- защита оборудования, продукции, финансовых средств, данных;
- реализация контролируемого доступа в здания и помещения.

Приведенные физические средства защиты информации подразделяются на группы, а именно средства предупреждения, обнаружения и ликвидации угроз, то есть охранные системы причисляются к средствам выявления угроз, а возведение заборов вокруг секретных объектов причисляется к средствам предупреждения несанкционированного доступа на территории.

Также существуют и аппаратные методы и средства защиты данных (таб. 2.1).

Классификация аппаратных средств защиты информации [12, с.125]

Классификация	
По функциональному назначению	Средства обнаружения Средства поиска Детальных измерений Активного противодействия Пассивного противодействия
По техническим возможностям	Общего назначения Профессиональные комплексы

Аппаратными средствами защиты данных являются всевозможные средства разного принципа функционирования, устройства и возможностей технических конструкций, которыми пресекаются утечка и разглашение информации, а также формируются меры противодействия несанкционированному доступу к конфиденциальным данным.

Аппаратные средства защиты данных базируются на реализации направлений для разрешения определенных задач, к которым можно причислить [6, с.52]:

- осуществление специализированных исследований технических средств;
- деятельность, сопряженную с выявлением каналов утечки данных;
- определение каналов утечки на различных объектах;
- осуществление обнаружения средств шпионажа;
- реализацию направлений противодействия несанкционированному доступу к источникам закрытых данных.

Аппаратными средствами защиты данных являются электронные и электронно-механические устройства, которые входят в структуру технических средств корпоративной сети, которые выполняют определенные функции по обеспечению информационной безопасности. Критерием включения устройств в аппаратные средства, а не инженерно-технические средства защиты является обязательное включение в структуру технических средств корпоративной сети [5, с.33].

Главными аппаратными средствами защиты данных являются:

- устройства ввода идентифицирующих пользователей данных (пластиковые и магнитные карты, отпечатки пальцев);
- устройства шифрования данных;

- устройства для создания препятствий несанкционированному включению станций и серверов (блокираторы, электронные замки).

Примерами вспомогательных аппаратных средств защиты данных являются:

- устройства по уничтожению данных на магнитных носителях;
- устройства сигнализации о попытках несанкционированного доступа пользователей корпоративной сети.

Аппаратные средства акцентируют на себе внимание ученых и специалистов, поскольку они легко поддаются защите от повреждений или иных злоумышленных действий, а также потому, что аппаратная реализация функций является более высокой по быстродействию в сравнении с программной, а стоимость — доступной.

Осуществление контроля целостности предназначается для того, чтобы определить, что файлы и программы пользователей, а также системные файлы оперативной системы не модифицировались злоумышленниками или используемыми ими программными закладками. Для чего функционирует разборщик файловой системы оперативной системы: проводится расчет эталонных показателей, осуществляется контроль при загрузке, которые реализуется в «Соболе» на аппаратном уровне. Формирование списков контроля целостности объектов осуществляется посредством утилит операционных систем, что предоставляет возможность программам-перехватчикам изменять данные списки.

Аппаратные средства являются техническими средствами, которые применяются для обработки информации [7, с.268].

Аппаратными средствами защиты являются всевозможные электронные, механические, электронно-оптические устройства. В современном мире сформировано множество аппаратных средств разного назначения, однако значительным распространением обладают:

- специальные регистры для хранения реквизитов защиты: пароля, коды идентификации, грифа, уровня секретности;
- генератор кодов, которые необходимы для автоматического генерирования кодов идентификации устройств;
- устройства, измеряющие персональные характеристики людей (голос, отпечатки), что позволяет проводить идентификацию;
- специализированные биты секретности, значение которых устанавливается посредством уровня секретности данных, которые хранятся в запоминающем устройстве, обладающем данными битами.

К значимой и распространенной группе аппаратных средств защиты относятся устройства шифрования данных (методы криптографии). В простых случаях для работы сетей требуются сетевые карты и кабели. Если требуется сформировать сложные сети, то необходимо специализированное сетевое оборудование.

Аппаратным обеспечением средств защиты операционных систем является единство средств и методов, которые применяются для решения задач:

- по управлению оперативной и виртуальной памятью компьютеров;
- по распределению процессорного времени между задачами в многозадачных операционных системах;
- по синхронизации исполнения параллельных задач в многозадачных операционных системах;
- по обеспечению общего доступа задач к ресурсам операционных систем [8, с.145].

Представленные задачи в большей мере решаются посредством аппаратных функций процессора, а также иных компьютерных узлов. Следует отметить, что для решения подобных задач используются программные средства, по этой причине понятие «аппаратное обеспечение защиты» и «аппаратная защита» являются не совсем верными, однако данные понятия являются общепринятыми.

Аппаратные устройства криптозащиты являются PrettyGoodPrivacy(PGP), которые реализуются на уровне «железа». Нередко подобные устройства являются платами, а также отдельными системами, которые используют алгоритмы шифрования. Ключи в подобном случае «железные», к которым можно отнести смарт-карты, а также идентификаторы Touch Memory. Производится загрузка ключей в устройство напрямую, в обход памяти и системной шины компьютеров, что предотвращает возможность перехвата данных.

Программными средствами защиты информации являются специализированные программы, которые входят в состав программного обеспечения компьютерной сети, выполняя при этом функции защиты.

Главным программным средством защиты данных являются:

- программы по идентификации и аутентификации пользователя компьютерной сети;
- программы по разграничению доступа пользователя к ресурсам компьютерной сети;
- программы по шифрованию данных;

– программы по защите информационных данных от несанкционированного изменения, применения и копирования.

Следует отметить, что идентификация относительно обеспечения информационной безопасности компьютерной сети является осуществление распознавания уникальных имен субъектов компьютерной сети. Аутентификация является подтверждением, что предъявленные имена соответствуют определенным субъектам, то есть подтверждается подлинность субъектов.

Программными средствами защиты данных являются:

- программы по уничтожению остаточных данных;
- программы по аудиту событий, которые связаны с безопасностью компьютерной сети, позволяющие обеспечить возможность восстановления и доказательства фактов происшествия событий;
- программы по имитации взаимодействия с нарушителями (отвлечения их на получение якобы секретных данных);
- программы по тестовому контролю защищенности компьютерной сети.

Преимуществами приведенных программных средств защиты данных являются:

- наличие простоты в тиражировании;
- наличие гибкости (то есть настройка на всевозможные условия использования, которые учитывают особенности угроз);
- наличие простоты в использовании;
- наличие неограниченных возможностей по развитию посредством изменений, которые учитывают новейшие угрозы безопасности данных.

Недостатками программных средств защиты данных являются:

- понижение продуктивности компьютерных сетей посредством потребления ресурсов, которые необходимы для работы защитных программ;
- наличие низкой производительности (в сравнении с аппаратными средствами, которые выполняют схожие функции);
- наличие пристыкованности различных программных средств защиты, что формирует для злоумышленников возможности их обхода;
- наличие возможности намеренного изменения программных средств защиты при использовании компьютерных сетей.

Операционные системы представляют собой значимую программную составляющую различных компьютеров, по этой причине от показателей осуществления политики безопасности в определен-

ных операционных системах зависят общие показатели безопасности информационных систем.

Семейство современных операционных систем Windows являются аналогами иных операционных систем, которые первоначально были рассчитаны на работу в домашних компьютерах. Данные операционные системы применяют уровни привилегий защищенного режима, однако не проводятся дополнительные проверки, а также не поддерживаются системы дескрипторов безопасности. Вследствие этого различные приложения обладают возможностью на получение доступа к объекту оперативной памяти. Меры сетевой безопасности имеются в данной операционной системе, однако их использование не слишком надежно.

За продолжительное время разработки различных операционных систем учитывались всевозможные сетевые атаки и ошибки в системе безопасности. Исправления к ним нередко выходят в форме блоков обновления.

Также существуют криптографические средства защиты данных. Как отмечалось ранее, криптография является наукой об обеспечении безопасности информации, занимающаяся подбором решений значимых проблем безопасности (конфиденциальности, аутентификации, целостности). Шифрование является преобразованием информации в нечитаемый вид с использованием ключей шифрования, что даёт возможность обеспечивать конфиденциальность при сохранении данных в тайне.

Современные криптографические методы подразделяются на группы:

- симметричные криптосистемы;
- криптосистемы с открытыми ключами;
- системы электронной подписи;
- управление ключами.

Приоритетными направлениями при использовании методов криптографии являются осуществление передачи секретных данных по каналам связи, определение подлинности передаваемой информации, осуществление хранения данных на носителе в зашифрованном виде.

В настоящее время существуют методы идентификации пользователей, которые обширно используются как частными лицами, так и компаниями.

Для получения доступа к сети, пользователи проходят идентификацию, а защитные механизмы сети осуществляют подтверждение

подлинности пользователей, то есть проверку, являются ли пользователи теми, за кого себя выдают. Опираясь на логическую модель, механизмы защиты сети размещаются на рабочих компьютерах, подключенных к пользователям посредством терминалов или иными методами. По этой причине процесс идентификации, а также подтверждения подлинности осуществляются в начале сеанса на рабочем компьютере.

Специализированные программные средства защиты данных от несанкционированного доступа также имеют наилучшие возможности и показатели в сравнении со встроенными средствами сетевых операционных систем. Помимо шифровальных программ, имеются различные внешние средства защиты данных, к которым относятся следующие.

Брандмауэры. Между локальной и глобальной сетями формируются промежуточные серверы, инспектирующие и отсеивающие трафик сетевого уровня, который проходит через них, что предоставляет возможность понижать угрозы несанкционированного доступа снаружи в компьютерную сеть, не устраняя при этом опасность.

Прокси-серверы. Трафик сетевого уровня локальной и глобальной сетей запрещается полностью, то есть не имеется маршрутизации, а запросы локальной сети в глобальную осуществляются посредством серверов-посредников. При подобном методе обращение из глобальной сети в локальную является невозможным. Однако представленный метод не дает требуемую защиту против атак более высокого уровня (вирусы).

Развитие информационных технологий постоянно ускоряет темпы, вследствие чего одновременно с ростом вирусов происходит совершенствование антивирусного программного обеспечения, а также формируется необходимость систематизации классификации антивирусных программ.

Все антивирусные программы сложно подразделить на группы, поскольку существует множество особенностей, однако возможно предоставить основную классификацию вирусов, по которой формируются антивирусные программы по основным особенностям (таб. 2.2).

Классификация антивирусных программ

<i>Вредоносность</i>	– безвредные, которые распространяются в сети, не выполняющие деструктивных функций; – неопасные, которые являются вредоносными программами, перегружающими память компьютеров; – опасные, которые наносят ущерб системе; – крайне опасные, которые уничтожают данные, приводят к поломке механических элементов компьютеров
<i>Среда обитания</i>	– файловые, которые поражают исполняемые файлы, среда обитания — файлы com. и exe.; – загрузочные, при которых поражаются секторы загрузки (boot) жестких дисков; – сетевые, которые поражают компьютерные сети и системы; – макро, которые поражают файлы программы MS office
<i>Способы заражения</i>	– резидентные вирусы — остающиеся в оперативной памяти после исполнения работы инфицированной программы; – нерезидентные вирусы — не занимающие оперативную память, которые выполняются однократно
<i>Особенности алгоритма действия</i>	– companion-вирусы — поражение файлов exe.; – worm-вирусы — распространение в сети посредством вычисления адресов подключенных к сети устройств; – вирусы-паразиты — способные изменять содержимое файлов; – stealth-вирусы — способные перехватывать обращения дисковой операционной системы к пораженным участкам диска; – вирусы-полиморфы — вирусы, не имеющие повторяющихся частей кода, вследствие чего являются трудно обнаруживаемыми – макровирусы — поражающие макросы в файловых редакторах – самошифрующиеся вирусы – вирусы, обладающие нестандартным алгоритмом

К приведенной выше классификации основных вирусных угроз можно добавить пораженную операционную систему, а также отдельные функции (слежку за пользователями, уничтожение данных).

Наиболее значимым при исследовании антивирусных программ является обнаружение вредоносного программного обеспечения, которое в определенных ситуациях представляется несложной задачей.

Нередко пользователи самостоятельно понимают, что компьютер заражен вирусами, к примеру, когда интернет-браузер не позволяет получить доступ к веб-сайтам, либо происходит постоянное изменение домашних страниц.

Существующие антивирусы позволяют предотвращать ущерб, а также ликвидировать последствия вирусных угроз и атак, вследствие чего обычные пользователи нуждаются в просвещении относительно грамотного применения антивирусных программ, а также переходов по незнакомым ссылкам в сети Интернет, которые нередко оказываются вредоносными.

В отношении разработчиков антивирусных программ существует необходимость их совершенствования, подбора новых методов сбора данных, поскольку сейчас методы сканирования, выявления и ликвидации вирусов не являются идеальными, как и методы перехвата сетевого трафика, вследствие чего многие компьютеры обладают потенциальной угрозой атаки вирусами.

Проведенное сравнение методов защиты информации показало, что на современном этапе существуют определенные программные и аппаратные средства защиты, которые предоставляют возможность получения наилучшей защиты информации, однако существующие средства несовершенны, поскольку обладают как своими достоинствами, так и недостатками.

Особенности российских технических средств защиты информации

Опираясь на недавнюю приостановку деятельности множества зарубежных компаний в сфере информационных технологий в России, требуется раскрыть специфику отечественной кибербезопасности, при этом необходимо раскрыть специфику технического обеспечения информационной безопасности с позиции программного обеспечения отечественного производства, а также всевозможных программно-аппаратных средств защиты данных.

В настоящее время в России приостановилось множество бизнес-процессов, которые сопряжены с информационными технологиями, что затронуло компании и фирмы, взаимосвязанные с банковской сферой, интернет-торговлей, игровыми сервисами, а также сферой защиты дан-

ных. При этом в государственных учреждениях активно применяются отечественные средства защиты данных, а также соответствующее программное обеспечение [9, с.61].

Согласно статистическим показателям, из зарубежного программного обеспечения активно используется лишь операционная система Windows. При уходе с рынка различных IT-компаний необходимо использовать иные средства защиты информации, для чего следует изучить существующие средства, а также их эффективность в сравнении с зарубежными аналогами.

Значимым представляется, что данные размещаются на аппаратных средствах, при этом они сопряжены с множеством проблем, а именно свободным доступом к программам, информации, использованием множества современных вирусов для получения доступа к закрытым данным, вследствие чего требуется использовать наиболее эффективные решения, которые при этом не будут подразумевать использования зарубежных производителей, которыми осуществляется обслуживание и вывоз комплектующих для российского рынка.

При рассмотрении возможностей программно-аппаратных средств вычисления и защиты данных в России необходимо раскрыть информацию о серверном оборудовании, однако в современном государстве не имеется серверов, которые полноценно базируются на отечественном оборудовании, однако в России имеются серверные процессоры «Эльбрус», которые в настоящее время активно испытываются, что в дальнейшем окажет влияние на развитие импортозамещения в сфере защиты информации [9, с.62].

Нуждается в разработке оперативная память, а также блоки питания, которые в дальнейшем будут устанавливаться на системы защиты. В настоящее время определенные комплектующие поставляются из Китая, а в будущем допускается возможность разработки российских микросхем.

При изучении устройств необходимо отметить, что «Байкал» устанавливается в компьютерные системы МВД России¹.

Что касается накопителей информации, то в России существуют аналоги зарубежных накопителей, которые обладают определенным уровнем защиты. К ним причисляются накопители GS panotech, которые базируются на элементах Micron, Kioxia и SK Hynix.

¹Следует отметить, что данные системы функционируют нестабильно, а также являются весьма медлительными. В связи с этим к 2024 г. с позиции дорожной карты планируется повысить производительность данного процессора.

В настоящее время в России существует множество ведущих компаний, которые производят и настраивают технические средства, связанные с защитой информации. Примером может послужить ViP net Coordinator серии HW от компании «ИнфоТеКС». Следует отметить, что поставкой серверов занимается сторонняя компания, однако данные серверы функционируют на основе процессоров Intel Core, что сопряжено с проблемой замены отдельных комплектующих на аналоги (поскольку таковых пока не имеется).

К техническим средствам защиты данных можно причислить также средства доверенной загрузки, которые активно применяются в России, например средства «Конфидент», а именно «Даллас лок», которые используются в некоторых государственных учреждениях.

Существует также прикладное программное обеспечение, производимое в России, например, «Астра линукс», которое представляется операционной системой, являющейся основой «Байкала», при этом она обладает несколькими вариациями: «Смоленск» и «Орел».

Как отмечалось выше, для работы с документами существует полностью свободное программное обеспечение «LibreOffice». В этом пакете есть обработка документов формата docx, xlsx, pptx и др. Однако следует заострить внимание на реализации собственных офисных программ с закрытым исходным кодом. Поэтому рекомендация здесь только одна — разработать на основе свободного исходного кода собственные проприетарные программы, чтобы защитить конечных пользователей от большинства атак.

Также существует офисный пакет «Р7-Офис». Он распространяется на «Линукс», а это значит, что возможна будущая поддержка в Astra Linux. Данный пакет программ полностью копирует идеологию интерфейса Microsoft Office, однако у него есть недостатки в работе (например, повышенное потребление ресурсов компьютера). Благо, на защите информации это никак не скажется, так как существует возможность работы с зарубежными форматами файлов.

В России уже работает ViP net Деловая Почта, помогающая отправлять тысячи защищенных писем по выделенной сети. Но если изучать почтовые серверы для домашнего пользования, то компания Mail.ru имеет доступ к сигнатурным базам угроз антивирусной защиты Kaspersky Lab, что позволяет минимизировать угрозы со стороны хакеров.

Необходимо раскрыть базы данных, которые тоже составляют неотъемлемую часть информационных потоков. Тут есть два варианта решений задачи: используем также свободное ПО PostgreSQL, либо же закрытую СУБД под названием РЕД, при этом он представляет собой

ответвление от ядра БД «Firebird», но здесь приводится именно готовое решение для российского сообщества.

Среди средств защиты информации в России выделяются системы защиты данных, например, ViP net Client от компании «ИнфоТеКС», который защищает конечного клиента в сетях общего пользования и ограничивает доступ к локальной сети. Помимо этого, есть криптографическая защита информации от компании «КриптоПРО» с одноименным названием программы. Они позволяют защищать информацию по ГОСТу.

В случае с обнаружениями хакерских атак в российской IT-сфере был разработана ViP net IDS (Intrusion Detection System), которая тоже неплохо работает. У Secretnet также существует модуль обнаружения вторжений. Все они могут работать в режиме обучения, чтобы не блокировать ресурсы, на которые вы обычно входите.

Антивирусная защита обеспечивается Антивирусом Касперского, как отдельная программа, и базы которого входят в модуль антивирусной защиты Secretnet Studio. Антивирусным решением также обладает компания Dr.Web с одноименным названием.

Можно сделать вывод, что в России существуют определенные методы защиты информации, однако технические средства обеспечения информационной безопасности в настоящее время представляются весьма неэффективными и нуждаются в значительной доработке. Также необходимо акцентировать внимание и на отечественном программно-аппаратном обеспечении, которое также требует совершенствования, что позволит активно развивать направления информационной безопасности и защиты информации в России.

Вопросы и задания для самоконтроля

1. Организационные методы по защите информации.
2. Понятие защиты информации.
3. Виды технических средств защиты информации.
4. Классификация антивирусных программ.
5. Криптографические методы защиты информации.
6. Преимущества и недостатки программных средств защиты информации.
7. Основы защиты информации.

Глава 3

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ОПТИЧЕСКИМ КАНАЛАМ

3.1. Защита информации от утечки по визуально-оптическому каналу

Защита информации от утечки по визуально-оптическому каналу — это комплекс мероприятий, которые уменьшают или полностью исключают выход конфиденциальной информации за границы контролируемой зоны за счет распространения света. Самым обычным для человека носителем информации об объектах выступает излучение, которое видит человеческий глаз. Наибольший объем информации человек получает при помощи зрения.

Способность наблюдения объектов устанавливается освещенностью, то есть величиной падающего потока света, который отражается от объекта света (отражающие свойства) и контрастом объекта на фоне предметов, окружающих его. В дневные часы (освещенность создается Солнцем) человеческий глаз имеет наивысшую цветовую и контрастную чувствительность. Когда смеркается, освещенность начинает постепенно сокращаться. Уменьшение освещенности приводит к ухудшению работы зрительного аппарата и, как следствие, к сокращению дальности и слабому различению цветов. При защите данных от утечки по визуально-оптическим каналам важно принять во внимание эти физические особенности.

Для защиты информации от утечки по визуально-оптическому каналу рекомендуется:

- расположить защищаемые объекты таким образом, чтобы исключить возможность отражения света в сторону предполагаемого нахождения злоумышленника;
- уменьшить отражательные свойства защищаемого объекта;
- уменьшить освещенность защищаемого объекта;
- применять преграждающие или ослабляющие средства для отраженного света (жалюзи, шторы, ширмы, ставни, преграды, тонированные стекла);
- использовать для введения злоумышленника в заблуждение маскировочные средства, различные имитации и др.;
- применять активные и пассивные средства защиты объекта от неподконтрольного распространения излученного или отраженного света и других видов излучений;

- производить маскировку объектов защиты, используя контраст фона и отражательные свойства;
- использовать средства маскировки объектов можно при помощи маскирующих сеток, аэрозольных завес, красок и укрытий.

Аэрозольные завесы являются оперативными средствами защиты, препятствующие распространению света, отраженного от защищаемого объекта. Дымообразующие вещества имеют хорошие светопоглощающие свойства. Данные средства маскировки создают индивидуальную или групповую защиту техники и объектов.

3.2. Характеристики оптического канала утечки информации

Один из наиболее часто используемых способов похищения документов, в которых содержится конфиденциальная информация, это их фотографирование. Человек, не имеющий технического потенциала, сделает фото, используя камеру мобильного телефона. Конкурирующая сторона будет использовать более современные методы получения информации с оптических каналов утечки информации, воспользовавшись услугами шпионажа в области бизнеса, которые оказывают определенные фирмы. Идет постоянное совершенствование технических средств. Для получения информации производят фотографирование документов с использованием спутника.

Фотографирование моделей из новой модной коллекции, фотографирование экрана с данными маркетинговых отчетов, выкладывание в интернет основных кадров нового фильма — утечка любой оптической информации способна нанести компании значительный ущерб.

Характеристики оптического канала утечки информации

Любой технический канал утечки информации включает три элемента: объект наблюдения, среда, по которой проходит сигнал, и средство приема информации. Для оптического канала в качестве объекта выступит рисунок, текст, чертеж, изображение на мониторе, прибор. Распространение оптического сигнала в воздушной среде происходит по оптическим каналам связи, в безвоздушной среде (в космическом пространстве) — при наблюдении и фотографировании и со спутника.

«СёрчИнформКИБ» контролирует значительное число каналов передачи информации, защищая компанию от ее утечек.

Длина канала образуется за счет особенностей объекта, мощности освещения, которая направлена на него, свойств среды, передающей сигнал, чувствительности и особенностей приемника оптической информации. Производится наблюдение в видимом спектре и в инфракрасном диапазоне.

Существует несколько стандартных схем формирования канала:

1. Объект наблюдения — экран монитора, документ, полезная модель, находящиеся в помещении. Среда, в которой передается оптический сигнал, — воздух или воздух в сочетании с оконным стеклом. Средство наблюдения — человеческий глаз, фотоаппарат, бинокль, видеокамера.

2. Объект наблюдения — оборудование, различные модели, иные объекты, которые находятся на открытом воздухе, во дворе организации, в кузове грузовика, на железнодорожной платформе. Среда, в которой передается сигнал, — воздух или безвоздушное пространство вселенной при съемках со спутника. Средства наблюдения — фотоаппараты, телевизионные камеры, инфракрасные устройства.

3. Объект наблюдения — человек, который находится на открытом пространстве или в помещении. Среда, в которой распространяется сигнал — воздух или воздух в сочетании со стеклом, если наблюдающий находится за пределами помещения. Средства получения информации — глаз человека, бинокль, технические средства фото или видеофиксации, в отдельных случаях — аналог инфракрасного прицела стрелкового оружия.

Если оптические каналы передачи информации становятся средой распространения, то необходима их модификация, провоцирующая утечку информации:

- сдвиг стыкуемых волокон, не совпадающих по центральной оси кабеля;
- наличие свободного места между соседними волокнами;
- несоблюдение параллельности расположения торцевых стенок волокон;
- соединение волокон под неправильным углом.

Такую модификацию получают, когда на кабель оптоволоконной связи оказывает влияние внешнее механическое воздействие. Это ведет к образованию линейного электрооптического, фотоупругого и квадратичного электрооптического эффектов, трансформация

которых даст информацию о наблюдаемом объекте. Особенности светового канала утечки информации широко представлены в средствах передачи акустических данных за счет ее трансформации в световой сигнал, исходящий от светодиодной лампы. Приемник принимает звуковой сигнал и трансформирует его в световой, настроен он так, что световые колебания, которые исходят от светодиода, не видны глазу человека. Находящийся в зоне видимости передатчик ловит сигнал и трансформирует его в данные. Обнаружить данный прибор трудно, так как он не создает радиоволны. Техническое средство получения данных зачастую встраивается в светодиодные лампы.

При считывании данных с оптических каналов утечки реализуются три функции:

- обнаружение, выявление объекта с еще неизвестными характеристиками;
- различение — выявление крупных деталей, логическое разделение сложных объектов на части;
- опознавание — полный захват важных характеристик.

Оперативность выявления объекта наблюдения при помощи человеческих глаз или оптических технических средств зависит:

- от яркости освещения человека, текста, или оборудования;
- резкости контраста между фоном и объектом;
- состояния воздушной среды, от ясного дня до дождя или тумана, осложняющего фиксацию объекта;
- дефекта изображения, иногда создаваемого специальными маскировочными средствами;
- величины объекта (необходимо отметить, что при увеличении размера объекта в процессе поиска на открытом пространстве в два раза, например, при осмотре видеоискателем площади или поля, скорость его выявления возрастет в восемь раз);
- времени наблюдения;
- скорости изменения характеристик, например, скорости движения или чтения страниц текста на экране монитора.

Возможности оптических каналов утечки информации расширяются за счет использования специальной техники. Убираются помехи, вызванные слабой освещенностью помещения, удаленностью объекта, невысоким углом разрешения.

Традиционные способы использования оптического канала:

- просмотр экрана монитора и документов из окна напротив расположенного здания с помощью применения мощного бинокля;

– фотографирование монитора и документов камерой, установленной в мобильном телефоне.

Достаточно широко используются приемы съема оптических излучений, преобразованных информацией, при задействовании оптических датчиков, которые могут функционировать в обычном или инфракрасном диапазоне. Документирование полученной информации в недалеком прошлом производилось на фотопленку, на современном этапе применяются электронные носители информации.

Наблюдение (снятие оптической информации) является более результативным для получения данных об образцах продукции или чертежах. Съем текстовой информации качественнее производится другими методами. Сложность наблюдения заключается в привлечении масштабных ресурсов технических средств и сил, а также необходимостью находиться рядом с объектом длительное время.

Показатели, характеризующие оптический прибор:

- угол разрешения;
- степень освещенности, необходимая для работы;
- частота смены изображения.

Важно тщательно подойти к техническим параметрам компонентов при выборе системы наблюдения и снятия данных с оптических каналов утечки. Чем дальше расстояние до документа, тем больше должен быть диаметр объектива технического средства наблюдения. Использование длиннофокусных объективов увеличит изображение. При съемке миникамерами нет необходимости в наводке на резкость или установке параметров диафрагмы. При автоматических настройках миникамеры дадут качественное изображение, тем самым предоставляя возможность использовать их непрофессиональными фотографами.

Устройства съема информации

Микрофотокамеры многим известны по фильмам или детективным книгам. Как правило, их применяют, чтобы зафиксировать результаты наблюдения совместно с видеокамерами. Видеокамеры могут быть проводными, установленными внутри помещения, с питанием от сети и автономными, носимыми на теле, питающимися от аккумуляторных батарей. Чаще всего полученные материалы передаются ими по радиоканалу, на находящийся за пределами охраняемого объекта приемник, сигнал часто модулируется или шифруется.

Отличительными особенностями современных технических средств является возможность ведения наблюдения при ночном освещении, при значительной удаленности объекта до нескольких километров, в инфракрасном диапазоне, который дает возможность увидеть исправления, подделки, измененные части документа, прочесть текст на пепле от сожженного документа.

Для получения информации с оптических каналов утечки при слабой освещенности используются приборы ночного видения и тепловизоры. Принцип их работы заключается в преобразовании светового поля слабой интенсивности в поле электронов с последующим усилением получаемого изображения при помощи макроканального усилителя. Усиленное изображение можно увидеть на люминесцентном экране, для большинства приборов оно отображается в зеленой области спектра. Изображение, появившееся на экране, изучается при помощи регистрирующего прибора, при его отсутствии используется обычная лупа.

Наблюдение проводится на границе ближнего инфракрасного диапазона (740–1400 *нм*), дополнительно применяется лазерная инфракрасная подсветка. По этому принципу изготавливаются комплекты для ночного дистанционного наблюдения с использованием инфракрасного лазерного фонаря. Данные технические средства могут быть выполнены в виде биноклей, визиров, устройств прицела для стрелкового оружия.

Тепловизоры применяются для наблюдения за участками спектра с длинными волнами (8–13 *мкм*), здесь происходит концентрация наибольшего теплового излучения от предметов. Данные технические средства дают возможность осуществлять наблюдение при обильных осадках.

Технические средства для документирования информации — отдельная группа средств для получения данных с оптических каналов утечки.

В устройство входит:

- штатив, обеспечивающий опору и поворот объектива;
- ночной визир, обеспечивающий высокое качество наблюдения;
- устройство регистрации изображения — фото- или видеокамеры;
- инфракрасный прожектор.

Прибор применяется для наблюдения с большого расстояния, мини-видеокамеры чаще устанавливаются в помещениях. В комплект современного устройства входит двухметровый провод опто-

волоконной связи, выведенный за границы контролируемого объекта. Камера устанавливается внутри охраняемой зоны через большого размера замочные скважины, отверстия, при помощи которых в помещении прокладываются трубы систем отопления или кабели связи, через вентиляционные отверстия, отверстия для приборов освещения в подвесных потолках. Камеры, обеспечивающие угол обзора до 65°, дают практически неограниченную возможность фокусировки, позволяя фиксировать очень мелкие изображения. Слабое освещение не мешает фотографировать документы, экраны мониторов, доски для размещения записей — флипчарты.

Предотвращение утечки информации по оптическим каналам

Основной способ для борьбы с утечкой — это создание затруднений для доступа злоумышленника к охраняемой зоне, содержащей секретную информацию. Следующая задача — обнаружение закладных технических средств.

Способы выявления:

- фиксация радиосигнала;
- фиксация повышенного электромагнитного излучения;
- поиск, неизвестно куда ведущих проводов;
- обнаружение проводников, просвечиванием рентгеновскими лучами.

Чаще всего применяется поиск побочных электромагнитных излучений или метод нелинейной локации. Любая микросхема, которая применяется в закладном техническом средстве, обладает собственным спектром побочного излучения. Распознать радиоустройство можно, зная используемые спектры. Электронные схемы управления матрицами камер тоже излучают определенный спектр, который способствует поиску. Осложнить процесс поиска может наличие большого количества побочных электромагнитных излучений, исходящих от сотовых телефонов, различного оборудования, компьютеров, линий связи.

Обследование помещения для обнаружения технических средств получения оптической информации лучше доверить фирме, специализирующейся на этом виде деятельности и имеющей соответствующую лицензию. В некоторых случаях это уменьшает риск незапланированного взаимодействия с органами правопорядка при условии обнаружения легально установленного ими специального технического

средства. Большой риск привлечения к ответственности за незаконное использование или оборот электронных средств съема информации имеется при задержании со снятым специальным техническим средством в руках.

Необходимые действия для обнаружения специальных технических средств, преобразующих работу светодиодной лампы и трансформирующих свет в информационный сигнал:

- использование чувствительных фотосенсоров для измерения изменений уровня светимости светодиода (основой измерения будет коэффициент пульсаций светодиодов, значение которого не должно превышать 4 %);

- зрительная проверка всех ламп в помещении на наличие высокочастотного преобразователя-усилителя цепи;

- обследование структуры помещения, обнаружение всех щелей, отверстий, прозрачных объектов — окон, части дверей в помещении, перегородок в переговорной на наличие каналов распространения света и анализ пространства вокруг них для выявления специальных приемных технических средств.

Для реализации системы защиты оптических каналов необходимо:

1. Выстроить схему расположения защищаемых объектов так, чтобы исключить отражение видимого света в сторону предполагаемого нахождения злоумышленника.

2. Изменить отражающие свойства защищаемого объекта. Например, чехол из оптических метаматериалов делает предметы невидимыми.

3. Уменьшить уровень освещенности предмета или текста, установив энергетический лимит на получение информации.

4. Использовать средства, ослабляющие отраженный свет — жалюзи, шторы, темные или матовые стекла, иные преграды, которые будут препятствовать распространению сигнала.

5. Применять разные маскировочные методы, имитации скрываемых предметов под различные объекты, для введения злоумышленника в заблуждение.

6. Применять пассивные и активные средства защиты источника от неподконтрольного распространения отражаемого или излучаемого света и других излучений.

7. Маскировать защищаемые объекты, используя изменения отражательных параметров и контраста между цветом и освещенностью объекта и фона.

Если злоумышленниками ведется наблюдение за человеком, то его тоже можно замаскировать, используя различные способы видоизменения внешности.

Принимая во внимание технические и финансовые возможности предполагаемых противников – конкурентов, технических разведок, целесообразно разработать план обеспечения защиты информации, основой которых будут действия, затрудняющие доступ к изучаемым объектам. Например, если имеется вероятность съема данных со спутника, то скрываемое современное оборудование нужно защитить прочной упаковкой, расставлять мониторы так, чтобы их не было видно из окон, документы оставлять на столе текстовой стороной вниз. Выполнение элементарных мер поможет значительно снизить вероятность использования злоумышленником оптических каналов утечки информации.

3.3. Организационно-технические способы защиты от утечки информации по оптическим каналам

Процесс утечки информации — это неконтролируемое распространение информации за границы помещения, здания, организации, какой-либо территории, а также конкретного круга лиц, имеющих доступ к этой информации. При обнаружении утечки необходимо своевременно ее пресечь, однако лучше принять заблаговременные меры для защиты конфиденциальной информации.

Возможные причины утечки данных — применение неправильных норм защиты информации, полное их несоблюдение или нарушение. Даже незначительное отступление от правил работы с важными служебными документами, техникой, продукцией и прочими конфиденциальными материалами может привести к возникновению канала утечки конфиденциальной информации.

Канал утечки информации (или технический канал утечки) — это путь, по которому проходит информации от источника до приемника/получателя в результате случайной утечки или целенаправленного несанкционированного доступа. Если мероприятия по защите информации не проводились заблаговременно, то могут быть использованы любые каналы утечки. Если меры по защите информации предприняты — тогда будет использован менее защищенный канал.

В настоящее время имеется только четыре средства передачи информации:

- звуковые волны;
- световые лучи;
- электромагнитные волны;
- материальные носители (фото, бумага, магнитные носители и т. д.).

Из них состоит любая системы связи, в которую еще входят:

- источник информации;
- передатчик;
- канал передачи данных;
- приемник;
- получатель информации.

Человек тоже может быть инициатором (случайным или же намеренным) утечки данных, если пользуется одним или несколькими вышеуказанными средствами передачи данных. Следовательно, функционирование систем связи нужно держать под строгим контролем, как для гарантирования надежной, безопасной и точной передачи данных, так и для защиты ее от несанкционированного доступа. Когда канал не защищен и передача данных из одного места в другое осуществляется без разрешения владельца информации, тогда такой канал называют каналом утечки информации.

Чтобы предотвратить утечку данных необходимо проводить организационные и технические мероприятия с целью обнаружения возможных технических каналов утечки информации, во избежание их несанкционированного использования. Например, для предотвращения утечки данных по акустическому каналу следует уменьшить или полностью исключить выход конфиденциальной информации при помощи контроля звуковых полей. В данном случае специалисты принимают комплекс мер — структурную переустройство помещения (зоны, пространства), улучшение звукопоглощения, звукоизоляции, звукоподавления, проводят режимные меры для строгого контроля нахождения людей в охраняемой зоне.

Для предотвращения утечки данных по визуально-оптическому каналу необходимо уменьшить освещенность объекта защиты и его отражательные свойства, применять всевозможные заграждения (экраны, ширмы, шторы, ставни, темные стекла), использовать маскировку и средства сокрытия объектов защиты (сетки, аэрозольные завесы, краски, укрытия).

Основной способ защиты электромагнитных каналов от утечки данных — экранирование технических средств и их элементов.

Электростатическое, магнитостатическое и электромагнитное экранирование защищает объект от воздействия и акустических, и электромагнитных сигналов. Экранирование гарантирует надежную защиту информации от утечки по побочным электромагнитным излучениям и наводкам.

Материально-вещественные каналы тоже необходимо защищать, потому что на разных материальных носителях может содержаться секретная информация. Например, отходы какого-либо предприятия содержат бракованные детали, различные испорченные документы, газообразные вещества или жидкости, которые могут бесконтрольно вывозиться за границы контролируемой зоны. В целях защиты таких каналов от утечки проводится комплекс организационных мероприятий.

Компетентные специалисты компании «ИРС», осуществляющие мероприятия по защите информации, создают для различных организаций высоконадежную степень защиты от утечек любых данных и обеспечивают строгое контролирование всех вероятных каналов утечки. Чтобы предотвратить утечку любых данных, они выполняют определенные действия по апробированной схеме, суть которой заключается в поиске вероятных каналов утечки и установлении энергетических параметров этих каналов на границе охраняемой зоны (например, здания учреждения). Основная же задача по недопущению утечки любой информации по техническим каналам — сокращение питания данных каналов утечки при помощи специализированных технических средств и организационных мер. После этого важно осуществлять постоянный контроль, имеющихся каналов передачи информации и регулярно анализировать уровень их защищённости.

Вопросы и задания для самоконтроля

1. Схемы формирования оптических каналов утечки информации.
2. Приборы для документирования изображения.
3. Способы борьбы с утечкой информации по оптическим каналам связи.
4. Комплекс действий для выявления закладных устройств.
5. Мероприятия по предотвращению утечки информации по оптическим каналам.
6. Средства переноса информации по оптическим каналам.
7. Группы способов утечки информации.

Глава 4

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО РАДИОЭЛЕКТРОННЫМ КАНАЛАМ

4.1. Информационная безопасность и особенности утечки информации

Сущность и специфика обеспечения информационной безопасности

Современные информационные технологии являются системой методов сбора, накопления, хранения, обработки и использования данных. Информационные технологии обладают значением для управления организацией, ее деятельности, поскольку базой управления является информация [11, с.74].

Информационные технологии представляют собой процесс, который содержит регламентированные правила исполнения действий, операций разного уровня сложности над информацией, хранящейся в компьютерных системах. Приоритетной целью информационных технологий является переработка первичных данных для получения требуемой пользователю информации, а также для принятия наилучших управленческих решений.

Существуют определенные факторы, которые оказывают значительное влияние на развитие информационных систем организаций:

- совершенствование методов управления организацией;
- улучшение общих возможностей и производительности компьютерных систем и программного обеспечения;
- совершенствование подходов к программной реализации составляющих информационных систем.

Развитие в сфере наращивания мощностей и производительности компьютерных систем, сетевых технологий, а также существование обширных возможностей интеграции компьютерного оборудования с иными видами оборудования предоставляют возможность увеличивать производительность информационных систем.

Развитие аппаратной части информационных систем позволяет осуществлять подбор новых, универсальных методик программной реализации информационных систем.

Развитие информационных систем в последние годы базируется на нововведениях, которые ускорили данные процессы развития:

- использование объектно-ориентированного программирования, посредством которого сократились сроки создания сложных информационных систем;

– развитие сетевых технологий, посредством которых локальные информационные системы были заменены на клиент-серверные и многоуровневые системы;

– активное развитие сети Интернет, позволившее расширить возможности взаимодействия с удаленными подразделениями, предоставляя перспективы развития электронной коммерции, обслуживания потребителей, взаимодействия специалистов из различных стран [8, с.189].

На современном этапе развития общества очевидно, что отличительной чертой современной действительности стала информатизация всех сфер практической деятельности, представляющая собой сложный, комплексный процесс формирования и совершенствования нового постиндустриального общества, в котором информационные ресурсы рассматриваются на одном уровне с важнейшими ресурсами государства — природными, трудовыми, финансовыми и др. Информация в таком обществе выступает в качестве определяющего средства общения и принятия решений.

Персональный компьютер в этих условиях превращается в устройство с возможностями универсальной вычислительной системы, которое позволяет осуществить хранение, обработку и выдачу потребителям огромного объема данных, активно влияющих на происходящие в обществе процессы, особенно на принятие управленческих решений.

Для того чтобы построить действенную системы информационной безопасности, требуется внедрение и выбор адекватного технического средства защиты, которое должно предваряться анализом угроз, а также уязвимостью самой информационной системы на основе анализа рисков информационной безопасности. Основывается выбор программно-аппаратного обеспечения защиты и проектирования системы информационной безопасности на результатах данного анализа и при учете экономической оценки соотношения стоимости контрмер по снижению риска, а также возможных потерь компании от инцидента информационной безопасности (далее ИБ) [1, с.46].

При обследовании и анализе системы информационной безопасности идентифицируются также владельцы ИТ-ресурсов, включающие лиц, которые непосредственно являются ответственными за целостность данных ресурсов. Установленные требования к системе разделения прав доступа включают в себя все правила доступа к информа-

ционной системе. Классифицируются ИТ-ресурсы по степени своей важности и критичности.

Все процедуры безопасности в обязательном порядке проверяются, также проверяется и система информационной безопасности, процесс самого расследования её нарушений, организация системы резервного копирования, процедура удаленного доступа, а также защита учетных записей. Также определяются и сами лица, которые ответственны за развитие и поддержку системы информационной безопасности.

Стратегия организации информационной безопасности определяется несколькими элементами:

- главные принципы создания списка критичных ресурсов, требующих защиты, которые разрабатываются в процессе осуществления анализа безопасности и рисков. Данный список содержит описания программных, физических, информационных ресурсов, а также выявление стоимости данных ресурсов и уровня их критического состояния для предприятий;

- главные основы защиты, определяющие стратегию организации системы безопасности и список правил, которыми руководствуются при формировании системы информационной безопасности предприятий;

- модели нарушителей безопасности, определяемые исследованием ресурсов существующей системы и методов их применения;

- модели угроз безопасности, а также анализ рисков, которые связаны с их осуществлением, формирующиеся на базе списка критичных ресурсов и моделей нарушителей;

- стандарты и требования безопасности, определяемые по итогам проведенного исследования рисков;

- меры обеспечения безопасности программного, технического и организационного уровней, которые предпринимаются для осуществления приведенных требований;

- ответственность персонала предприятий за соблюдение определенных стандартов и требований информационной безопасности при использовании системы безопасности предприятий [13, с.36].

На современном этапе вопросы обеспечения информационной безопасности являются не только актуальными, но и весьма острыми вследствие того, что происходит активная цифровизация, которая формирует новые проблемы, а также угрозы информационной безопасности.

Проблемы информационной безопасности при цифровой трансформации

Согласно информации СМИ, значительно увеличиваются показатели случаев, связанных с нарушением информационной безопасности различных компаний, организаций, отраслей экономики, обусловленных тем, что вследствие активной цифровизации многие компании применяют данные цифровые технологии, однако далеко не все из них активно используют направления и системы обеспечения защиты информации, оборудования, технологий.

Таким образом, существуют определенные проблемы, связанные с обеспечением информационной безопасности в различных экономических сферах, которые сопряжены с активной цифровизацией общества. Именно вследствие цифровизации регулярно образуются риски, угрозы, противоречия в цифровой экономике, что оказывает негативное влияние и на деятельность различных ее субъектов.

На современном этапе практически все направления экономической деятельности принимают участие в цифровой трансформации, в том числе и государственные учреждения, предприятия, поскольку компьютерные технологии повсеместно применяются, облегчая и автоматизируя различные процессы, что позволяет собирать и обрабатывать информацию, обладающую в современном мире определенной ценностью. Это обуславливает постоянную необходимость в защите такой информации.

Как известно, информационная безопасность представляется наиболее значимым элементом современного существования предприятий, компаний, учреждений, организаций, банков, а также является немаловажным аспектом жизни современного человека, поэтому всевозможные угрозы информационной безопасности на различные сферы и субъекты экономической деятельности отражаются на жизни людей.

В связи вышеуказанным наиболее важным остается проблема защиты информации, направления и методы защиты, возможности предоставления в сети Интернет информации, а также аспекты прав доступа к ней. Разрешение данной проблемы предоставляет возможность значительно увеличить надежность информационных систем компаний, банков, объектов инфраструктуры, государственных корпораций, а также сферы предпринимательской деятельности. Это, в свою очередь, обеспечивает защиту информации граждан.

Следует отметить, что, например, в банковской системе вопрос защиты информации стоит весьма остро. Это обусловлено тем, что количество пластиковых карт, в том числе кредитных, участвующих в регулярном обращении, на современном этапе превышает число граждан России (порядка 290 млн штук)[21]. Рассматриваемая ситуация провоцирует множество проблем, связанных с необходимостью обеспечения информационной безопасности в период активной цифровизации общества.

Сама по себе цифровизация нередко воспринимается в качестве оснащения информационными и компьютерными системами. При этом данное понятие намного более обширно, поскольку включает в себя вопросы государственной политики, а также аспекты административных и правовых отношений. Немаловажна и необходимость постоянного развития и совершенствования, поскольку использование устаревших парадигм о том, что конфиденциальная информация имеется лишь в бумажном виде и передается по обычной почте, провоцирует значительные угрозы безопасности, которые также сопряжены с отсутствием оперативности при обмене данными.

В настоящее время происходят изменения, заключающиеся в исчезновении старых укладов, а также использовании инновационных технологий и новшеств, обуславливающие, в свою очередь, изменения в жизни граждан. Цифровая трансформация связана и с формированием новых рабочих мест, профессий, котируемых на рынке. При использовании современных технологий в сфере информации происходит увеличение продуктивности деятельности различных сфер. В экономических отраслях значительно изменяются возможности использования современного компьютерного и сетевого оборудования для различных процессов и операций с позиции количества и качества, а также компаниями активно предоставляются услуги и транзакции, базирующиеся на использовании сети Интернет.

Цифровая трансформация обладает не только достоинствами, но и недостатками, а также проблемами и угрозами, которые в первую очередь сопряжены с вопросом обеспечения информационной безопасности, защиты транзакций, операций.

Следует отметить, что государственные интересы, а также интересы различных организаций и предприятий в области информационного взаимодействия, заключаются в осуществлении приоритетных составляющих безопасности, к которым относится использование конфиденциальной информации, а также применении совре-

менных методов и средств защиты информации от доступа к ней злоумышленников. Следовательно, приоритетным в области защиты информации является предотвращение угроз, ущерба и проблем, связанных с незаконным использованием информации, а также частных данных пользователей.

Немаловажным является то, что многие пользователи современных информационных и цифровых технологий практически не уделяют внимания информационной безопасности, вследствие чего происходит бесконтрольное распространение данных, которые могут нелегальными методами изменяться, либо уничтожаться. При этом злоумышленниками наносится значительный ущерб различным компаниям и организациям, а также нарушается стабильность процессов обработки и передачи информации [7, с.268].

Современные преступники осуществляют деятельность в киберпространстве, вследствие чего сформировался новый вид преступных деяний — киберпреступления, которые обусловили необходимость определения значимых целей и задач специалистами в области информационных технологий, направленных на предотвращение кибератак, киберугроз. Для обеспечения информационной безопасности специалистами решаются задачи в определенных направлениях:

- защиты личных данных пользователей;
- обеспечения безопасности информационных систем коммерческих предприятий;
- обеспечения безопасности информационных систем государственных учреждений, структур, предприятий и организаций;
- защиты рабочей среды.

Современные угрозы киберпространства играют важную роль в современном обществе, а также в сфере предпринимательской деятельности. Опираясь на информацию ЦБ РФ, уже к 2017 г. количество кибератак на отечественные организации банковской сферы с 2021 г. повысились почти в 3 раза (по сравнению с 2014 годом).

Проблемные аспекты обеспечения информационной безопасности находятся под влиянием дополнительных факторов, к которым относится отсутствие унифицированных способов и средств защиты данных, вследствие чего определенные методы, которые могут быть использованы в одной сфере деятельности или компании, не всегда подходят для другой.

На 2022 г. в сфере контроля киберугроз и кибератак было отмечено свыше 400 случаев утечки закрытых данных из различных ком-

паний на территории России, что это оказало весьма существенное негативное влияние на положение компаний, поскольку было скомпрометировано свыше пяти миллионов записей, включавших как персональную и личную, так и финансовую информацию. Ниже приведены показатели утечки данных по странам за 2023 г. (рис. 4.1).

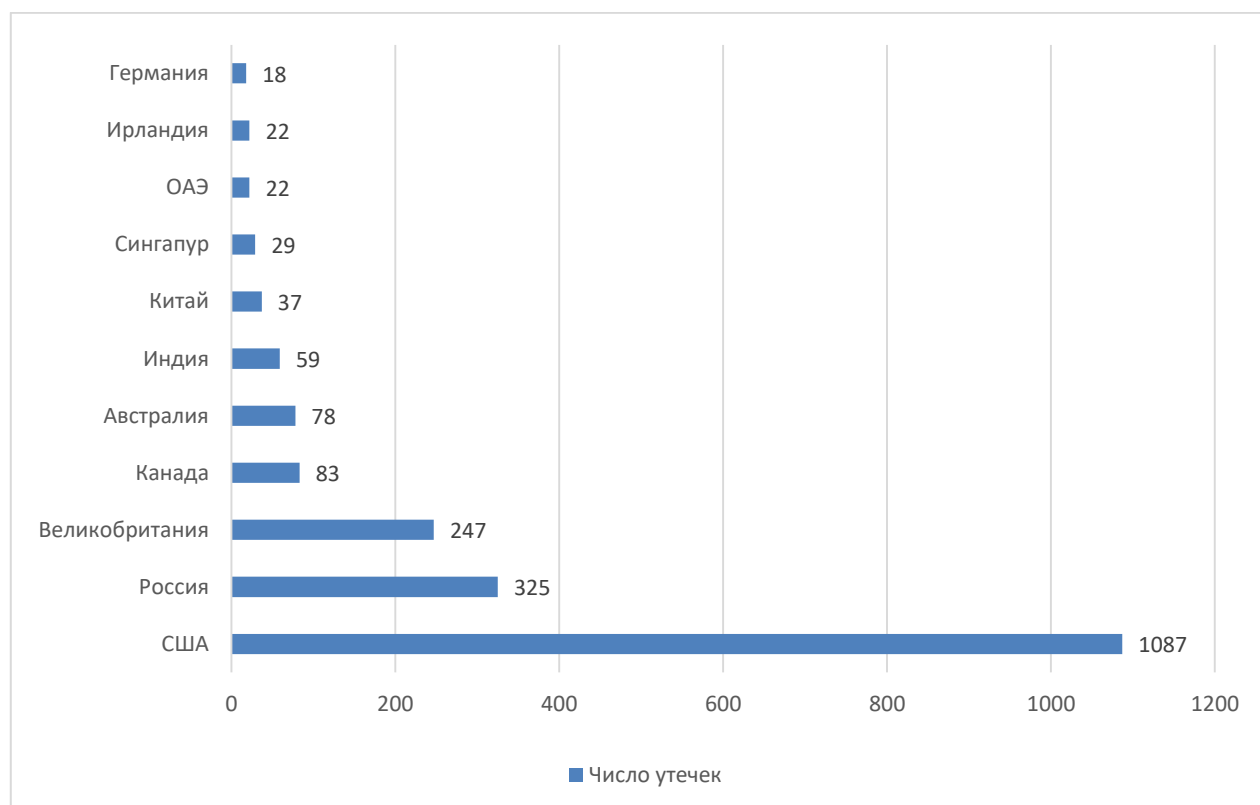


Рис. 4.1. Показатели утечки информации за 2023 г. по различным странам

Наиболее значимым и громкими в средствах массовой информации стала утечка информации одной из известных компаний Фейсбук, когда без согласия компании личные данные множества пользователей были переданы аналитическому агентству Великобритании, что было предпринято для анализа и обработки этой информации. Подобный случай спровоцировал дискуссии в обществе, а также привлек внимание к вопросу необходимости обеспечения конфиденциальности и безопасности информации пользователей, а также данных компаний.

Согласно показателям аналитического агентства, с 2010 г. в Соединенных Штатах Америки, которые считаются наиболее развитым государством, в том числе и с позиции развитие цифровой экономики, была допущена неоднократная утечка закрытой информации из множества крупных компаний, а также государственных предприятий

и корпораций. Опираясь на аналитические данные, предпринимательская деятельность в США не обладает необходимыми методами и средствами защиты от киберугроз, вследствие чего регулярно происходят утечки информации, а также кражи закрытых данных [18].

Анализ статистических показателей по кибератакам компаний в США позволяет сделать вывод о том, что утечке информации, а также организации информационной безопасности уделяется недостаточное внимание, вследствие чего низкий уровень информационной безопасности провоцирует множество проблем и нуждается в повышении.

Специфические риски и угрозы в современном мире сконцентрированы именно в киберпространстве, в сфере IT-технологий, а также информационных системах различных организаций и компаний. При этом современные риски подразумевают не только возможность использования вирусов, но и угрозы, связанные с незаконным управлением, а также нарушением целостности закрытых данных, чем обусловлена необходимость совершенствования цифровой независимости компаний.

4.2. Беспроводная система предотвращения вторжений в информационных сетях

Идея о системе обнаружения вторжений (IDS) и системе предотвращения вторжений (IPS) зародилась в научной статье американского исследователя в области информационной безопасности Дороти Э. Деннинг¹ под названием «Модель обнаружения вторжений», которая побудила Стэнфордский исследовательский институт (SRI) разработать Экспертную систему обнаружения вторжений (IDES) [19]. Следует отметить, что в начале 2000-х организации относились скептически к новому классу защитных решений, поскольку считали, что данная система не эффективна и способна блокировать безвредный аномальный трафик от потенциальных клиентов, однако после 2005 года общество осознало необходимость использо-

¹Дороти Элизабет Деннинг (1945) известна своей системой управления доступом на основе решеток (LBAC)), системой обнаружения вторжений (IDS) и другими инновациями в области кибербезопасности. Введена в Зал славы национальной кибербезопасности в 2012 году, в настоящее время является заслуженным профессором анализа обороны Военно-морской аспирантуры.

вания IPS в виду его различных преимуществ. Так начала развиваться и совершенствоваться новая система обнаружения вторжений.

Система предотвращения вторжений (IPS) — это автоматизированное устройство сетевой безопасности, используемое для мониторинга и реагирования на потенциальные угрозы. IPS размещается на линии, непосредственно в потоке сетевого трафика между источником и получателем. Как и система обнаружения вторжений (IDS), IPS определяет возможные угрозы, анализируя сетевой трафик [20]. Следует отметить, что основное отличие между IDS и IPS заключается в том, что IDS способно лишь обнаружить вредоносную активность и уведомить об этом администратора, в то время как IPS предпринимает какие-либо действия по устранению угрозы, то есть IDS — это пассивная система, которая сканирует трафик и сообщает об угрозах (рис. 4.6).

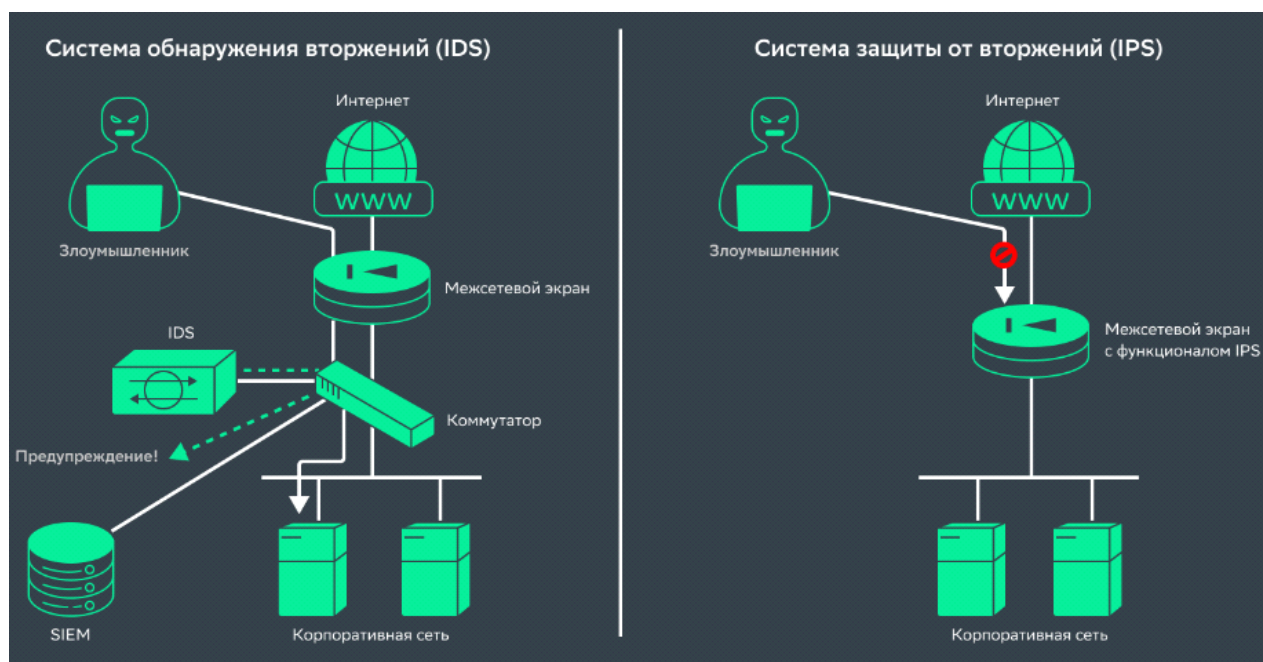


Рис. 4.6. Различия систем IDS и IPS

Обнаружение вторжений — это процесс мониторинга сетевого трафика и его анализа на наличие признаков возможных вторжений, которые могут представлять непосредственную угрозу для организации. *Предотвращение вторжений* представляет собой процесс обнаружения вторжений и последующей остановки обнаруженных инцидентов.

Основными функциями IPS являются выявление подозрительной активности, регистрация соответствующей информации, попытка заблокировать активность и, наконец, сообщение о ней.

IPS включают брандмауэры (межсетевой экран, который представляет собой программный или программно-аппаратный комплекс, предназначенный для фильтрации исходящего и входящего сетевого трафика), антивирусное программное обеспечение и программное обеспечение для защиты от спуфинга (рис. 4.7) [21].

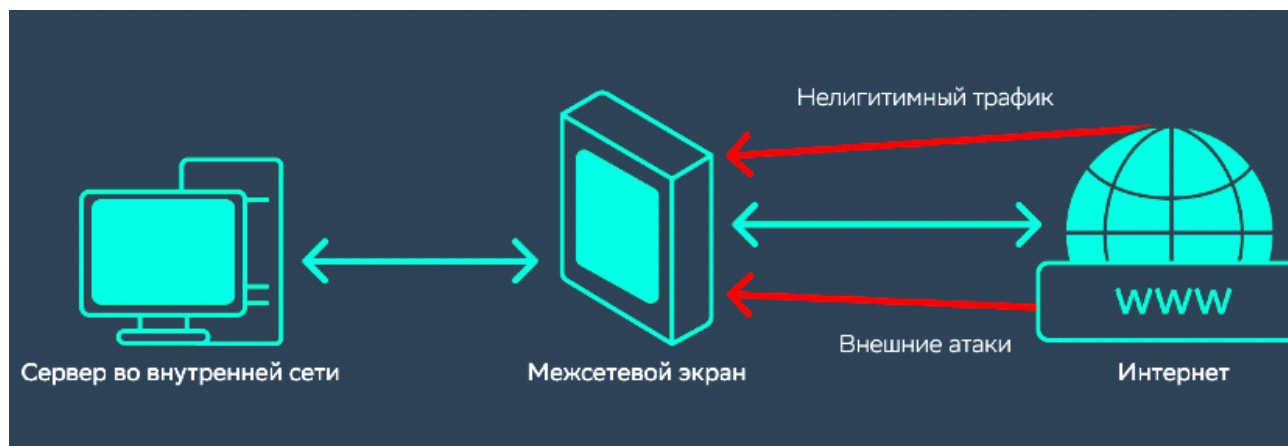


Рис. 4.7. Принцип работы межсетевого экрана

Как правило, система IPS включает в себя несколько элементов, каждый из которых призван выполнять определенную функцию (рис. 4.8).

1. Сенсор (датчики). Датчики *отслеживают активность сети или хоста и предотвращают вторжения.*

2. Сервер управления. Он отвечает за *сбор данных с датчиков*, также способен сопоставлять и анализировать полученные данные. Этот анализ позволяет IPS определить с большей уверенностью, *требуется ли конкретное событие превентивных действий.*

3. Сервер базы данных. На нем *хранятся данные о событиях, которые были записаны датчиками IPS.*

4. Консоль IPS. Консоль предназначена для *выполнения задач администрирования или управления.* В зависимости от поддерживаемых возможностей консоли ее можно использовать для настройки датчиков, а также для мониторинга и анализа.

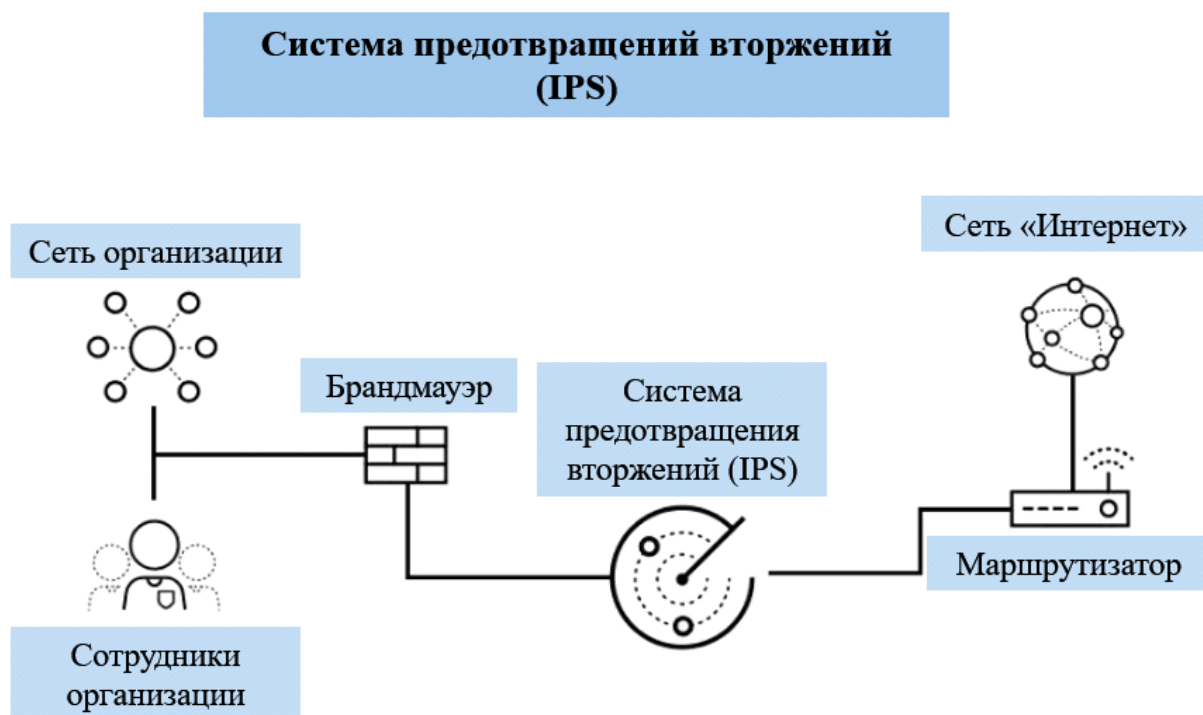


Рис. 4.8. Система предотвращения вторжений (IPS)

Кроме того, организации будут использовать IPS для других целей, таких как выявление проблем с политиками безопасности, документирование существующих угроз и сдерживание отдельных лиц от нарушения политик безопасности. IPS стали важным компонентом всех основных инфраструктур безопасности в современных организациях.

Система предотвращения вторжений работает путем активного сканирования переадресованного сетевого трафика на наличие вредоносных действий и известных шаблонов атак [23]. Механизм IPS анализирует сетевой трафик и постоянно сравнивает битовый поток со своей внутренней базой данных сигнатур на наличие известных шаблонов атак. IPS может отбросить пакет, определенный как вредоносный, и в ответ на это действие заблокировать весь будущий трафик с IP-адреса или порта злоумышленника. Легитимный трафик может продолжаться без каких-либо предполагаемых сбоев в обслуживании.

Системы предотвращения вторжений также могут выполнять более сложное наблюдение и анализ, например, отслеживать и реагировать на подозрительные шаблоны трафика или пакеты. Механизмы обнаружения могут включать [24]:

1. Совпадение адресов.
2. Сопоставление строки HTTP и подстроки.
3. Сопоставление общего шаблона.
4. Анализ TCP-соединения.

5. Обнаружение аномалий пакетов.
6. Обнаружение аномалий трафика.
7. Сопоставление портов TCP/UDP.

IPS обычно записывает информацию, связанную с наблюдаемыми событиями, уведомляет администраторов безопасности и создает отчеты. Чтобы обеспечить безопасность сети, IPS может автоматически получать профилактические обновления и обновления безопасности, чтобы постоянно отслеживать и блокировать возникающие интернет-угрозы.

Многие IPS также могут реагировать на обнаруженную угрозу, активно предотвращая ее. Они используют несколько методов реагирования, которые включают:

- изменение среды безопасности (например, путем настройки брандмауэра для усиления защиты от ранее неизвестных уязвимостей);
- изменение содержания атаки (например, путем замены вредоносных частей электронного письма, таких как ложные ссылки, предупреждения об удаленном содержимом);
- отправка автоматических сигналов тревоги системным администраторам, уведомляющих их о возможных нарушениях безопасности;
- удаление обнаруженных вредоносных пакетов;
- сброс соединения;
- блокировку трафика с исходного IP-адреса.

Системы предотвращения вторжений можно разделить на четыре основных типа (таб. 4.2).

Таблица 4.2

Классификация типов IPS

<i>Тип IPS</i>	<i>Расположение</i>	<i>Что проверяет</i>
IPS	Устанавливается в процессе, по пути сетевого трафика	Проводной сетевой трафик
WIPS	Размещаются в стратегически важных местах на объекте, например, стационарные устройства, мобильные устройства (ноутбуки, мобильные устройства). Встраиваются в беспроводную точку доступа (AP)	Беспроводной сетевой трафик
HIPS	Устанавливается на конечные устройства или хосты, такие как ПК или серверы	Созданные приложением файлы журналов, изменения в реестре и системных процессах
№BA	Развернутый встроенный	Сетевые пакеты либо информация о них, генерируемая маршрутизаторами и другими сетевыми устройствами

I. Сетевая система предотвращения вторжений (NIPS). Анализируется активность протокола во всей сети для мониторинга всего сетевого трафика и упреждающего сканирования на наличие угроз.

Рассмотрим алгоритм работы NIPS более подробно (рис. 4.9):

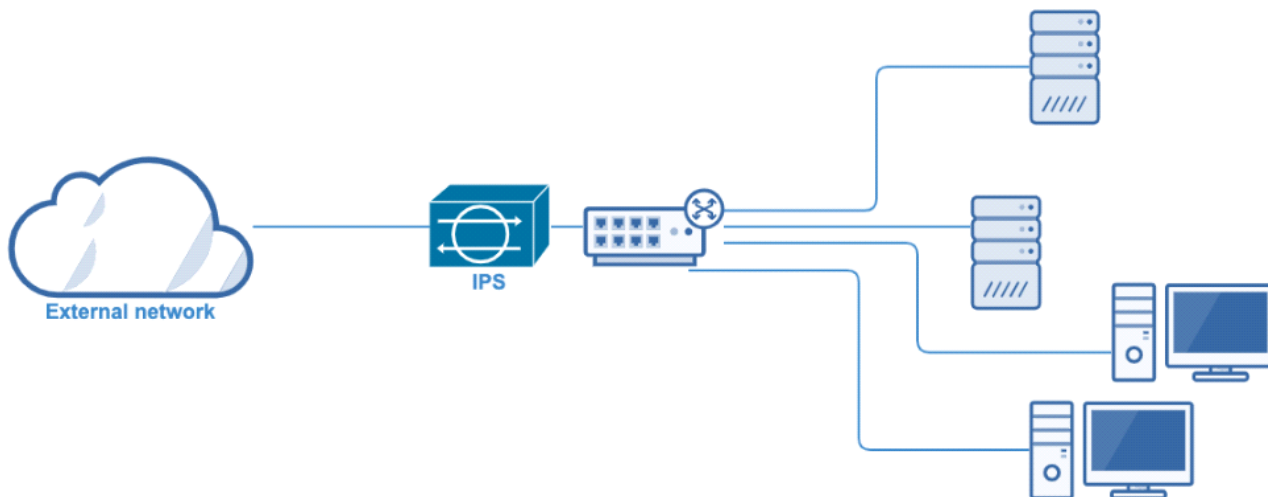


Рис. 4.9. Функционирование NIPS

1. Входящие пакеты из внешней сети поступают на датчик IPS.
2. Датчик IPS проверяет пакеты, применяя методы обнаружения IPS. В качестве альтернативы IPS отправляет данные о событиях на сервер управления, который выполняет проверку.

3. Если после проверки IPS обнаруживает угрозу, она автоматически отбрасывает рассматриваемые пакеты. Он пропускает только те пакеты, которые считает безопасными.

Сенсор IPS обращен во внешнюю сеть. Датчик IPS расположен таким образом, чтобы он находился на пути входящего трафика для обнаружения и блокировки угроз.

II. Хост-система предотвращения вторжений (HIPS). В отличие от NIPS, HIPS устанавливается на конечной точке (например, на ПК) и отслеживает входящий и исходящий трафик на предмет вредоносной активности только с этого устройства. Наиболее эффективно функционирует в сочетании с NIPS, так как служит последней линией защиты от угроз, прошедших через NIPS.

III. Система предотвращения вторжений в беспроводную сеть (WIPS). Производится анализ активности сетевых протоколов во всей беспроводной сети в поисках наличия несанкционированного досту-

па, после чего происходит отключение несанкционированного устройства от сети.

IV. Анализ поведения сети (NBA). Исследуется сетевой трафик для выявления необычных потоков трафика, таких как DDoS-атаки (распределенный отказ в обслуживании).

В большинстве систем предотвращения вторжений используется один из трех методов обнаружения: на основе сигнатур, на основе статистических аномалий и анализа протокола с отслеживанием состояния.

1. *Обнаружение на основе сигнатур.* Метод обнаружения, основанный на словаре уникально идентифицируемых шаблонов (или сигнатур) в коде каждого эксплойта (атака, использующая уязвимость в программном обеспечении для получения контроля над системой). По мере обнаружения эксплойта его сигнатура записывается и сохраняется в постоянно растущем словаре сигнатур. Одним из недостатков этого метода является то, что он может остановить только ранее выявленные атаки, но не сможет распознать новые [6, с.52].

2. *Статистическое обнаружение аномалий.* Происходит отслеживание аномального поведения путем сравнения случайных выборок сетевой активности с базовым стандартом. Он более надежен, чем мониторинг на основе сигнатур, однако иногда может давать ложные срабатывания.

3. *Обнаружение анализа протокола с отслеживанием состояния.* Данный метод выявляет отклонения от протокола путем сравнения наблюдаемых событий с предварительно определенными профилями нормальной активности. Если происходит какое-либо несанкционированное действие, нарушающее политику безопасности организации, срабатывает оповещение, которое отправляется администраторам.

Корпоративные системы предотвращения вторжений в беспроводную сеть уже довольно давно помогают организациям обнаруживать и блокировать атаки на беспроводные локальные сети (LAN). Сначала продукты для предотвращения вторжений в беспроводную сеть чаще всего использовались для обнаружения мошеннических точек беспроводного доступа (AP), но затем они эволюционировали, чтобы справляться с широким спектром атак на беспроводные локальные сети (WLAN). С резким увеличением использования беспроводных технологий организации считают все более важным использовать беспроводные системы предотвращения вторжений.

Существует целый ряд угроз для беспроводных сетей, к которым относятся подслушивание (организуется двумя способами: перехват радиосигнала (анонимное подслушивание) и при помощи MITM-атаки («человек посередине»); DDoS-атаки; подмена MAC-адресов клиентских устройств (злоумышленники подменяют MAC-адрес своего устройства, выдавая его за уже зарегистрированное в сети, и получают к ней доступ) и т. д. (рис. 4.10).

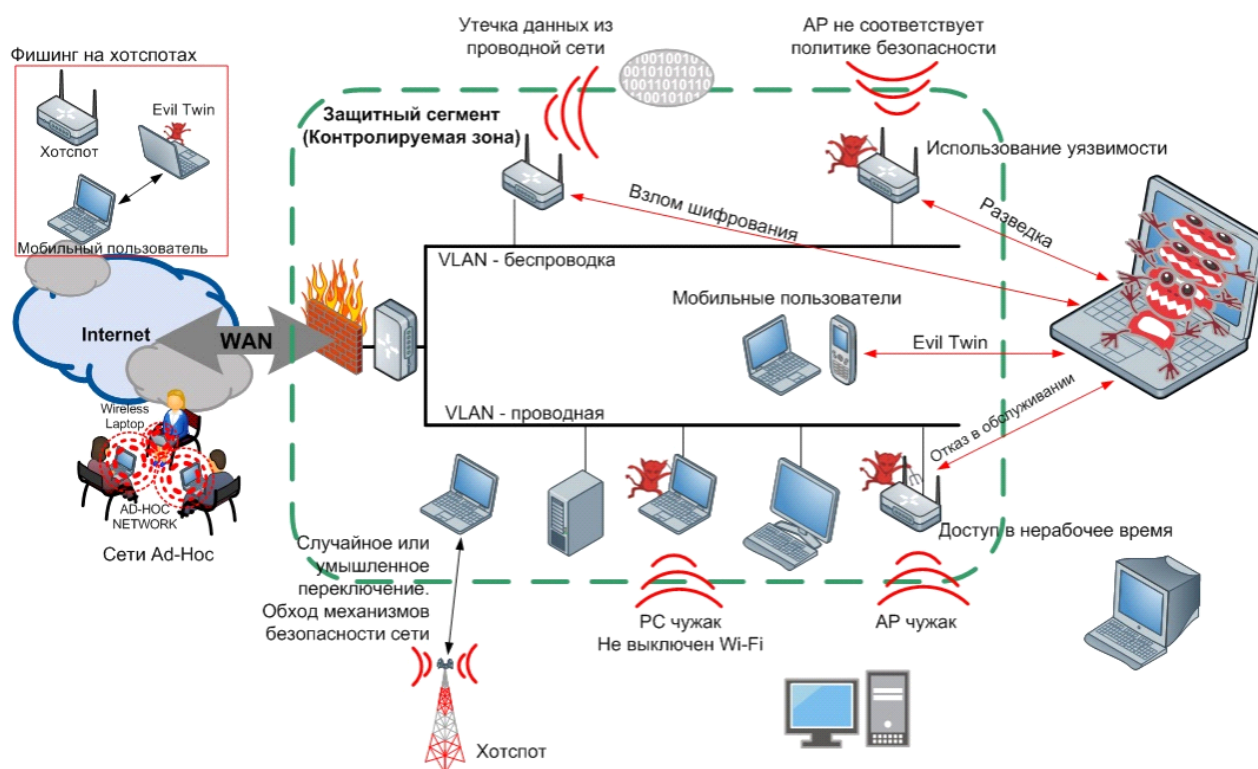


Рис. 4.10. Угрозы для беспроводной сети

Средством защиты данных в беспроводных сетях выступают системы обнаружения беспроводных вторжений (WIDS) и системы защиты от беспроводных вторжений (WIPS), которые используются для постоянной защиты беспроводной сети от неавторизованных пользователей. В WIDS система датчиков используется для мониторинга сети на предмет вторжения неавторизованных устройств, таких как мошеннические точки доступа, в то время как в WIPS система не только обнаруживает неавторизованные устройства, но и предпринимает шаги для снижения угрозы, блокируя устройство и отключая его от беспроводной сети.

В вычислительной технике система предотвращения вторжений в беспроводную сеть (WIPS) представляет собой сетевое устройство, которое отслеживает радиочастотный спектр на наличие несанкцио-

нированных точек доступа (обнаружение вторжений) и может автоматически принимать контрмеры (предотвращение вторжений).

Основной целью WIPS является предотвращение несанкционированного сетевого доступа к локальным сетям и другим информационным ресурсам с помощью беспроводных устройств. Крупные организации с большим количеством сотрудников особенно уязвимы к нарушениям безопасности, вызванным мошенническими точками доступа. Если сотрудник (доверенное лицо) в каком-либо месте подключает легкодоступный беспроводной маршрутизатор, вся сеть может быть открыта для всех, кто находится в пределах досягаемости сигналов.

Система обнаруживает вторжения в беспроводную сеть, то есть отслеживает радиочастотный спектр на предмет наличия несанкционированных, мошеннических точек доступа и использования инструментов беспроводной атаки. Система отслеживает радиочастотный спектр, используемый беспроводными локальными сетями, и немедленно оповещает системного администратора при обнаружении неавторизованной точки доступа, после чего ликвидирует угрозу. Обычно это достигается путем сравнения MAC-адресов участвующих беспроводных устройств.

Мошеннические устройства могут подделывать MAC-адрес авторизованного сетевого устройства как свой собственный. Системе надлежит сравнить уникальные сигнатуры сигналов, излучаемых каждым беспроводным устройством, с известными сигнатурами предварительно авторизованных известных беспроводных устройств [4, с.152].

Для автоматического предотвращения требуется, чтобы WIPS мог точно обнаруживать и автоматически классифицировать угрозу. Так, система WIPS позволяет обнаруживать и устранять:

- сетевые атаки;
- неавторизованный доступ к данным;
- действия вредоносных скриптов и программ;
- функционирование сканеров портов;
- нарушение политик безопасности;
- обращение к центрам управления бот-сетями и майнинг-пулам;
- аномальную активность.

Конфигурации WIPS состоят из четырех компонентов (рис. 4.11):

1. Сенсоры (датчики) — эти устройства содержат антенны и радиостанции, которые сканируют беспроводной спектр на наличие пакетов и устанавливаются в защищаемых зонах.

2. Сервер управления — выполняет задачи управления и настройки системы, анализ сигнатур, поведения и протоколов, а также анализ радиочастотного спектра для обнаружения вторжений. Анализ сигнатур отслеживает трафик на наличие шаблонов, связанных с известными атаками, такими как отказ в обслуживании (DoS) и атаки «человек посередине». Анализ поведения ищет аномалии в поведении сообщений, такие как использование преднамеренно искаженных кадров управления, которые позволяют злоумышленнику наблюдать за результирующим поведением сети. Анализ радиочастотного спектра используется для контроля частоты, на которой работает система, на наличие нежелательных или повреждающих сигналов. Распространенным методом DoS-атаки является передатчик, постоянно передающий на рабочей частоте, что может вывести из строя систему Wi-Fi.

3. Сервер базы данных — хранит и систематизирует информацию, полученную датчиками.

4. Консоль управления — консоль обеспечивает основной пользовательский интерфейс в системе для администрирования и создания отчетов.

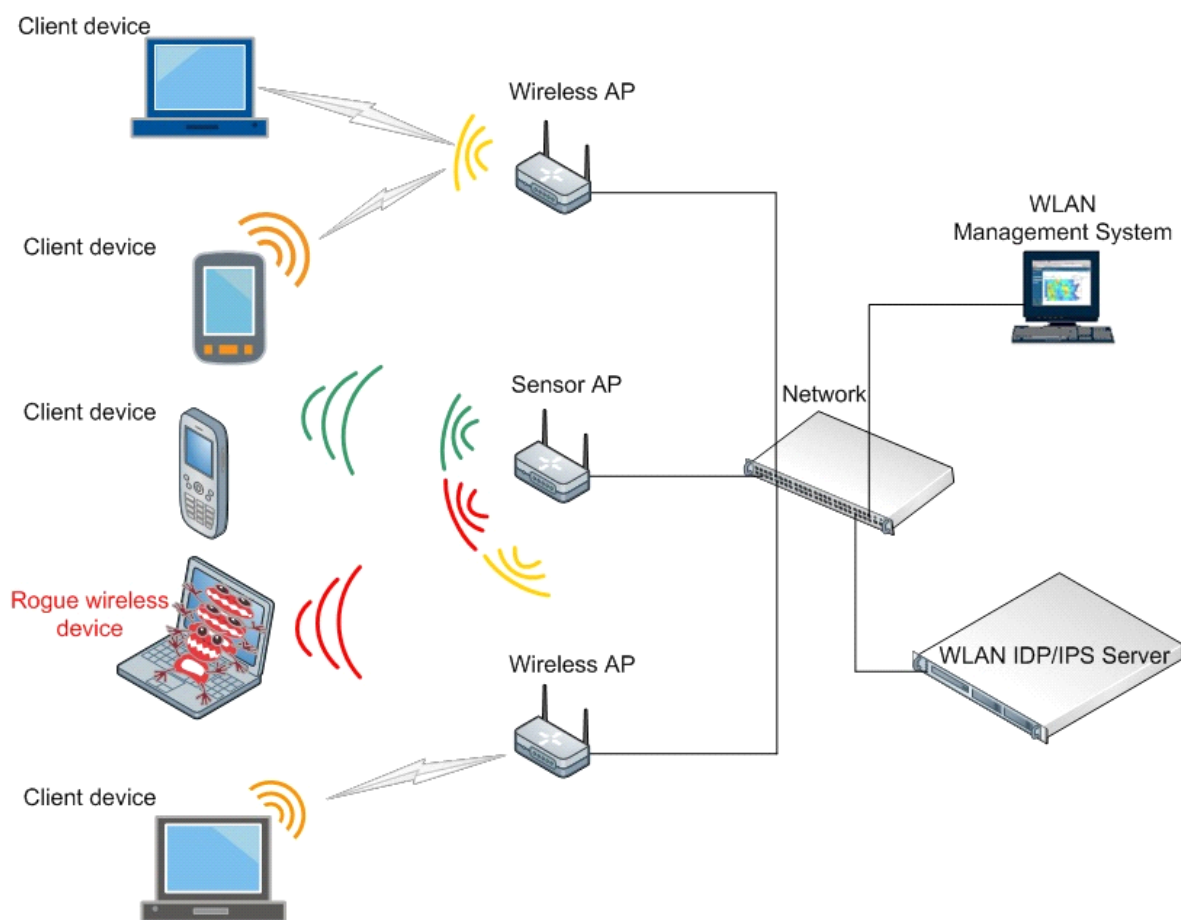


Рис. 4.11. Структура WIPS-сети

Существует несколько типов архитектуры WIPS:

1. Наложенная. Системы наложения используют независимые и специализированные датчики для непрерывного мониторинга спектра в диапазонах 2,4 и 5 ГГц [25]. Датчики не обеспечивают подключения к WLAN; вместо этого они работают в фоновом режиме, отслеживая весь системный трафик. Датчики развертываются по всему зданию для мониторинга радиочастот. Датчики передают собранные данные на централизованный сервер для дальнейшего анализа, принятия мер и архивирования журналов. Этот подход является более дорогим, поскольку требует специального оборудования, но также считается наиболее эффективным (рис. 4.12).

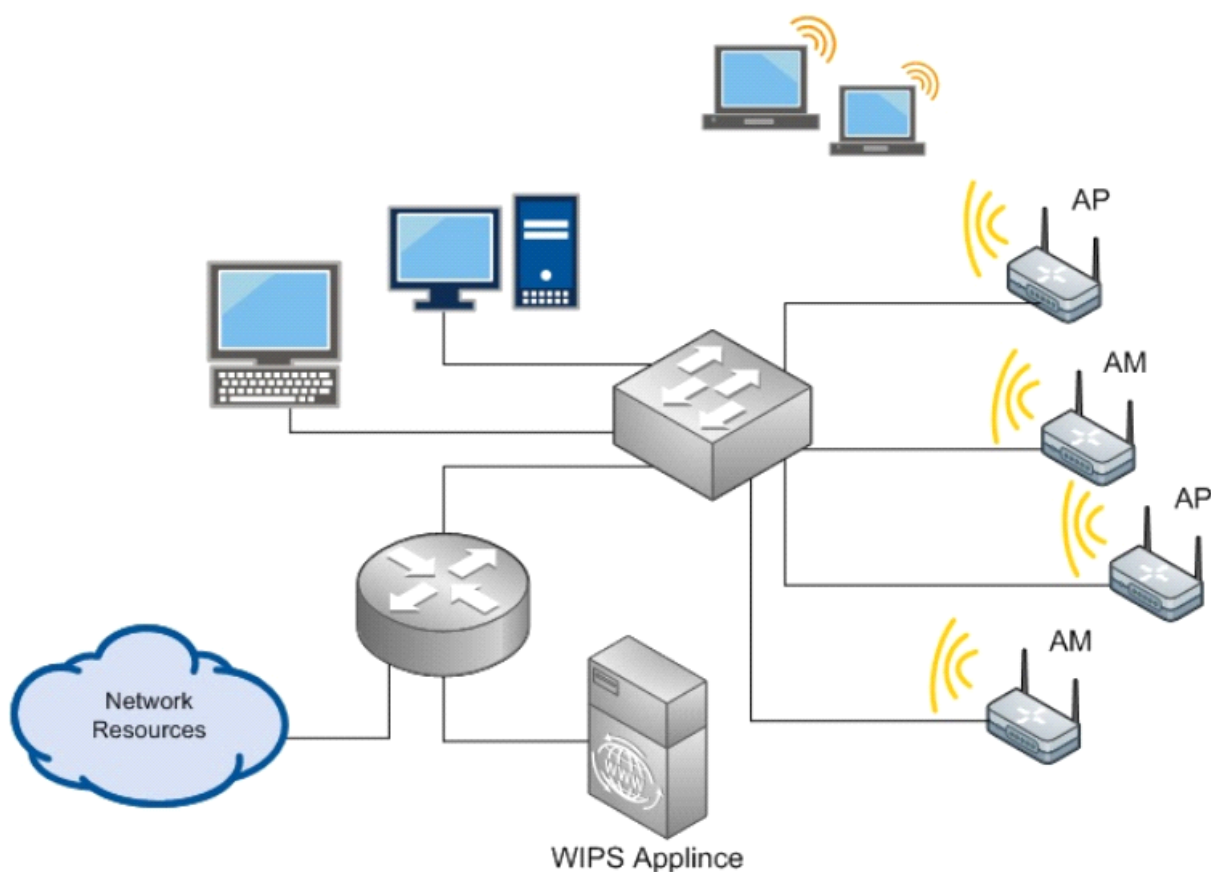


Рис. 4.12. Пример наложенной WIPS-сети

2. Интегрированная. Интегрированные системы обычно представляют собой системы на основе контроллеров, а также системы связи. Эта функция интегрирована в общий режим системы связи, поскольку

точки доступа попеременно функционируют как датчики WIPS и точки доступа на основе временного разделения. Точка доступа перейдет в режим датчика на установленный интервал времени, чтобы отслеживать используемые частотные спектры. Злоумышленник, зная, что фирма использует датчики неполный рабочий день, может начать атаку, достаточно короткую, чтобы попасть в промежутки между периодами сканирования точки доступа (рис. 4.13).

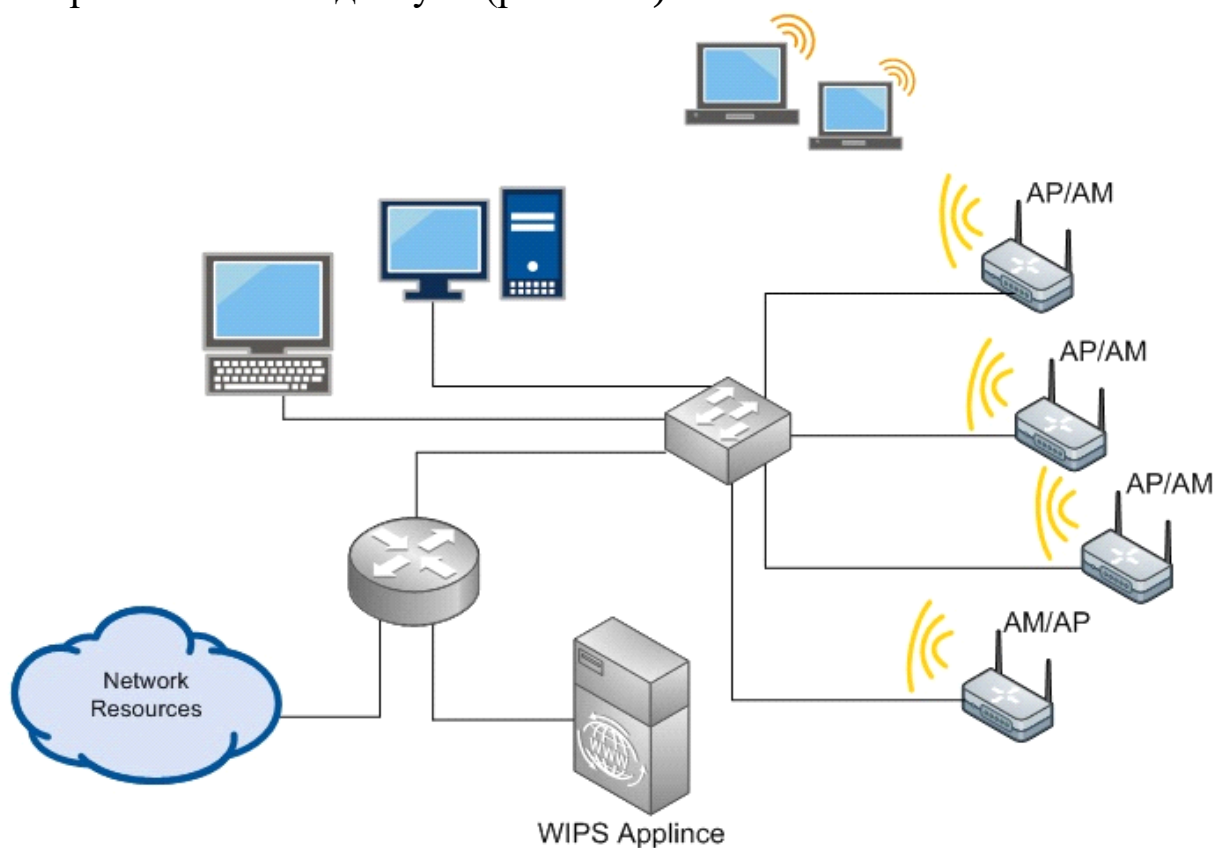


Рис. 4.13. Пример интегрированной WIPS-сети

3. Гибридная. В данной архитектуре точки доступа на основе контроллера используются в качестве выделенных постоянных датчиков в дополнение к выделенным точкам доступа, используемым исключительно для функций WLAN. Это отличается от интегрированных систем тем, что функциональность строго соблюдается; точка доступа обеспечивает подключение к WLAN, а датчик точки доступа обеспечивает мониторинг и смягчение последствий. Каждый тип точки доступа предназначен для определенной функции (рис. 4.14).

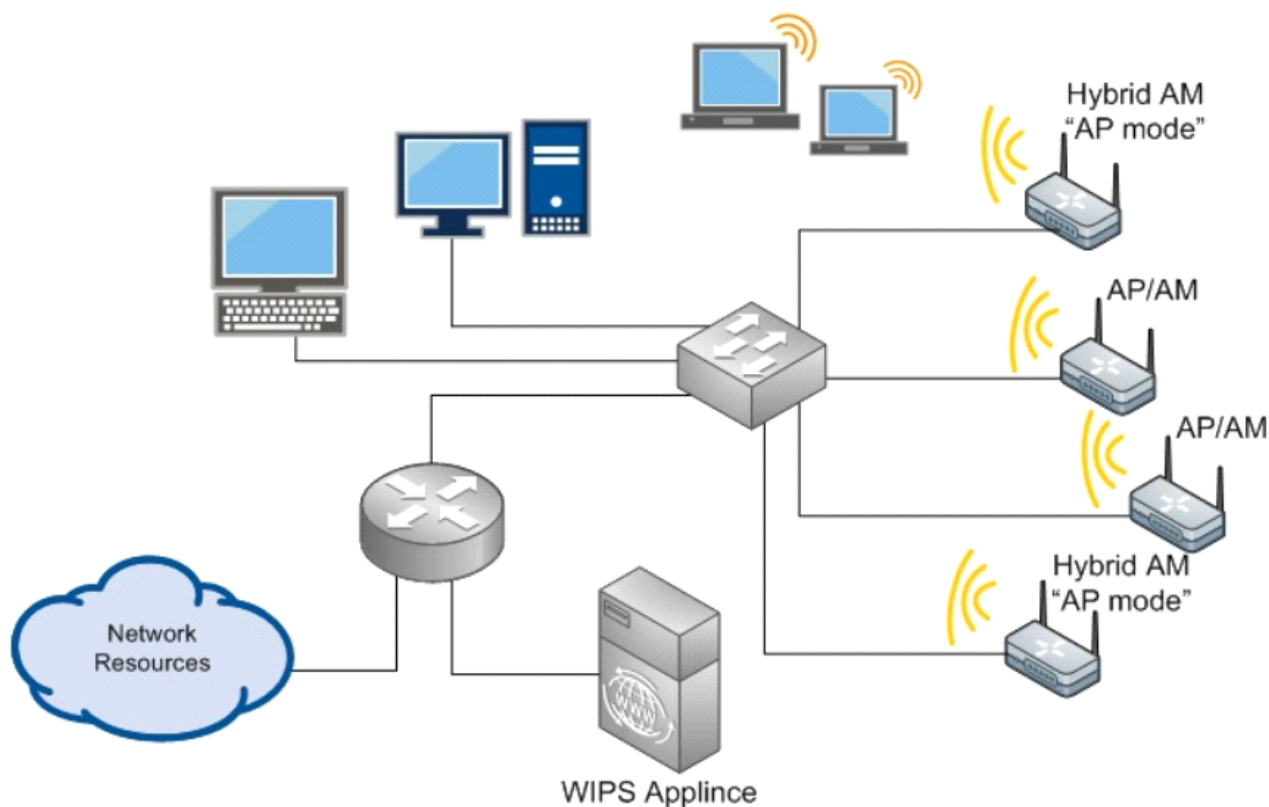


Рис. 4.14. Пример гибридной WIPS-сети

Простая система обнаружения вторжений может представлять собой один компьютер, подключенный к устройству беспроводной обработки сигналов, и антенны, размещенные по всему объекту. Для крупных организаций мультисетевой контроллер обеспечивает централизованное управление несколькими серверами WIPS. В реализации WIPS пользователи сначала определяют рабочие политики беспроводной сети в WIPS. Затем датчики WIPS анализируют трафик в эфире и отправляют эту информацию на сервер WIPS. Сервер WIPS сопоставляет информацию, проверяет ее на соответствие определенным политикам и классифицирует, является ли она угрозой. Затем администратор WIPS уведомляется об угрозе или, если политика настроена соответствующим образом, WIPS автоматически принимает меры защиты [26]. При функционировании WIPS ведение журнала и уведомление о событиях в контролируемом пространстве необходимы для надлежащих операций и поддержания безопасности контролируемого пространства.

Для надлежащего функционирования WIPS и обеспечения того, чтобы WIPS не проводил непреднамеренных DDoS-атак на непреднамеренные беспроводные устройства, требуется надлежащим образом

поддерживаемый и подробный список разрешений. Список разрешений — это подробный список всех устройств, подключенных к системе доступа WLAN, и всех ожидаемых режимов ее работы. С помощью этого списка можно создать правила для защиты устройств, включенных в список разрешенных, от несанкционированных устройств и от подключения к сети в неправильно сконфигурированном или небезопасном состоянии.

Может существовать более одного списка разрешений, который отслеживается системой WIPS. В этом случае каждый список разрешений отделен друг от друга, и никакое взаимодействие между устройствами в отдельном списке разрешений не допускается. «Серый список» — это необязательный список ожидаемых устройств в контролируемом пространстве, которые известны и которым разрешено работать в пределах этой области. Устройствам из серого списка не разрешается подключаться ни к каким устройствам из списка разрешенных. Любому устройству, специально не включенному в список разрешенных, должно быть заблокировано установление любого сетевого подключения к авторизованной системе доступа WLAN, и об этом событии должно быть отправлено уведомление.

Сервисы по обнаружению и предотвращения вторжений в беспроводную сеть имеет множество преимуществ:

1. Дополнительная безопасность. IPS взаимодействует с другими устройствами по обеспечению безопасности и выявляет угрозы.

2. Повышение эффективности других элементов управления безопасностью. IPS отфильтровывает вредоносный трафик до того, как он достигнет других устройств безопасности и элементов управления, что в свою очередь снижает нагрузку на устройства и позволяет им работать более эффективно.

3. Экономия времени. IPS в значительной степени автоматизирована, соответственно, она требует минимальных временных затрат от ИТ-специалистов.

4. Индивидуальная настройка. IPS позволяет самостоятельно осуществить настройку политики безопасности с целью обеспечения элементов управления безопасностью, специфичных для той или иной организации, которая ее использует.

5. Автоматически обнаруживает и блокирует потенциальные угрозы.

6. Функционирует на постоянной основе и не требует участия администратора.

7. Сдерживает и смягчает последствия от мошеннических действий за счет быстрого обнаружения и устранения угрозы.

Однако рассматриваемый сервис имеет ряд недостатков, которые проявляются в ложных срабатываниях, необходимости технического персонала по работе с сервисом, внесение каких-либо изменений на программном уровне требует перезагрузки точек доступа,

Режим WIPS поддерживается многими точками доступа от известных производителей. Они могут выпускаться в виде отдельных продуктов: CiscoAdaptiveWireless IPS, ZebraTechNologiesAirDefeNse, HP MobilitySecurity IDS/IPS, AirTight WIPS, TrellixNSP, TreNd MicroTippingPoint, INfotecsViPNet IDS и т. д. (таб. 4.3).

Краткое описание INfotecsViPNetIDS, TrellixNSP, TreNdMicroTippiNgPoiNt

Система обнаружения и вторжения в беспроводную сеть	INfotecsVIPNetIDS	TrellixNSP	TreNd Micro TippiNgPoiNt	CiscoAdaptiveWireless IPS
Краткая характеристика	Это программно-аппаратный комплекс для обнаружения вторжений в информационные системы, функционирующий на основе динамического анализа сетевого и прикладного трафика стека протоколов TCP/IP	Платформа Trellix (ранее McAfeeNetwork SecurityPlatform (NtSP)) – это решение для предотвращения сетевых угроз и вторжений, которое защищает системы и данные, где бы они ни находились, в центрах обработки данных, в облаке и в гибридных корпоративных средах. Он может поддерживать до 32 млн подключений на одном устройстве	TippiNgPoiNt выявляет и блокирует вредоносный трафик, предотвращает перемещение вредоносных программ, обеспечивает доступность и отказоустойчивость сети, а также повышает производительность сети. Его можно развернуть в сети без IP- или MAC-адреса, чтобы немедленно отфильтровать вредоносный и нежелательный трафик. Решение обеспечивает пропускную способность проверки сетевого трафика до 120 Гбит/с	Адаптивная система предотвращения вторжений в беспроводную сеть (IPS) Cisco обеспечивает расширенную сетевую безопасность для специального мониторинга и обнаружения аномалий беспроводной сети, несанкционированного доступа и радиочастотных атак. Данный сервис полностью интегрирован с унифицированной беспроводной сетью Cisco, обеспечивает интегрированную видимость и контроль по всей сети

Кроме того, сервис IPS предлагает хороший баланс функций обнаружения атак, возможностей криминалистической экспертизы данных, а также вариантов масштабируемости и высокой доступности.

Таким образом, система предотвращения вторжений работает путем активного сканирования переадресованного сетевого трафика на наличие вредоносных действий и известных шаблонов атак. Механизм IPS анализирует сетевой трафик и постоянно сравнивает битовый поток со своей внутренней базой данных сигнатур на наличие известных шаблонов атак.

Средством защиты данных в беспроводных сетях выступает система обнаружения и предотвращения от беспроводных вторжений (WIPS), которая используется для постоянной защиты беспроводной сети от неавторизованных пользователей. Это сетевое устройство, которое отслеживает радиочастотный спектр на наличие несанкционированных точек доступа (обнаружение вторжений) и может автоматически принимать контрмеры (предотвращение вторжений).

Конфигурации WIPS состоят из четырех компонентов: сенсоры (устройства, которые сканируют беспроводной спектр на наличие пакетов и устанавливаются в защищаемых зонах), сервер управления (выполняет задачи управления и настройки системы, анализ сигнатур, поведения и протоколов, а также анализ радиочастотного спектра для обнаружения вторжений), сервер базы данных (хранит и систематизирует информацию, полученную датчиками), консоль управления (обеспечивает основной пользовательский интерфейс в системе для администрирования и создания отчетов).

WIPS имеет множество преимуществ: дополнительная безопасность, повышение эффективности других элементов управления безопасностью, экономия времени, индивидуальная настройка, автоматически обнаруживает и блокирует потенциальные угрозы, функционирует на постоянной основе и не требует участия администратора, сдерживает и смягчает последствия от мошеннических действий за счет быстрого обнаружения и устранения угрозы.

Однако рассматриваемый сервис имеет ряд недостатков, которые проявляются в ложных срабатываниях, необходимости технического персонала по работе с сервисом, внесение каких-либо изменений на программном уровне требует перезагрузки точек доступа.

Информационные системы правоохранительных органов являются весьма чувствительными к воздействию внешних угроз, в связи с чем целесообразно использовать специально предназначенные сер-

висы по обнаружению и предотвращению вторжений в беспроводную сеть органов внутренних дел. При выборе сервиса по обнаружению и предотвращению вторжений необходимо исходить из целей его функционирования (программное обеспечение, тип архитектуры, комплектация сервиса, потенциальные угрозы).

Основываясь на этих критериях, данный сервис должен быть тщательно рассмотрен правоохранными органами, поскольку наличие конфиденциальной информации деятельности подразделений органов внутренних дел имеет потенциальную угрозу по вторжению в беспроводную сеть.

Таким образом, существующие устройства активной защиты информации требуются для защиты от утечки информации, а также радиоэлектронного подавления технических средств съема информации, систем дистанционного управления, которыми используются радиоэлектронные каналы. При этом применяются устройства для маскировки побочных электромагнитных излучений технических средств, что также позволяет блокировать каналы дистанционного управления.

Вопросы и задания для самоконтроля

1. Элементы стратегии организации информационной безопасности.
2. Задачи обеспечения информационной безопасности.
3. Виды радиоэлектронных каналов утечки информации.
4. Организационные меры защиты информации по радиоканалам.
5. Радиоэлектронный канал утечки первого вида.
6. Радиоэлектронный канал утечки второго вида.
7. Технические меры защиты информации.

Глава 5

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ

5.1. Понятия и определения средств защиты информации от утечек по акустическим каналам

Защита информации от утечки по акустическому каналу — это система мероприятий, которые уменьшают или полностью исключают утечку информации ограниченного доступа за границы контролируемого пространства благодаря акустическим полям. Ключевыми мероприятиями здесь являются организационные и организационно-технические меры. К организационным относится: реализация архитектурно-планировочных, пространственных и режимных мероприятий, к организационно-техническим: пассивные (звукопоглощение, звукоизоляция), активные (звукоподавление) мероприятия. Можно проводить и технические мероприятия, используя специальные защищенные ресурсы проведения конфиденциальных переговоров.

Архитектурно-планировочные меры включают в себя конкретные требования, которые должны быть соблюдены в процессе реконструкции или проектирования служебных помещений, чтобы уменьшить или исключить неконтролируемое распространения звука. В качестве примера можно привести особым образом расположенные помещения или оснащение данных помещений компонентами звуковой безопасности (тамбуры, ориентирование окон в сторону контролируемой зоны).

Режимные меры — тщательный контроль нахождения на контролируемой территории штатных сотрудников и посетителей.

Организационно-технические меры — применение средств звукопоглощения, таких как мягкие и пористые материалы вроде ваты, ковры с ворсом, сухая пористая штукатурка, пенобетон, которые обладают высокими звукопоглощающими и звукоизолирующими свойствами. Они имеют большое количество полостей, которые разделяют твердое тело и воздух, а это влечет за собой многократное отражение и поглощение звуковых колебаний (звукопоглощение, отражение и пропускание звука).

Для проверки результативности звукоизоляционной защиты применяются шумомеры. Шумомер — это измерительный прибор, конвертирующий колебания звука в числовые показания. Замер звуковой защищенности проводится с использованием метода образцо-

вого источника звука (заранее известный уровень мощности на конкретной частоте). Использование образцового источника звука и шумомера позволяет выявить поглощающие возможности служебного помещения. Уровень звукового давления образцового источника звука известен. Сигнал, полученный с другой стороны стены, измерен шумомером. За счет разницы между этими двумя параметрами получим коэффициент поглощения.

В ситуациях, когда пассивные меры не могут гарантировать должного уровня безопасности, применяются активные средства. К ним можно отнести генераторы шума — специальную техническую аппаратуру, которая вырабатывает шумоподобные сигналы. Данные сигналы направляются на звуковые или вибрационные датчики. Звуковые датчики служат для образования акустического шума в служебном помещении либо за его пределами, а вибрационные — для маскирующего шума в различных ограждающих конструкциях. Вибрационные датчики прикрепляются к конструкциям, требующим защиты, и создают в них акустические колебания. Генераторы шума дают возможность защитить информацию от утечки через потолки, стены, полы, двери, окна, вентиляционные коммуникации, трубы и другие конструкции, обеспечивая крайне высокий уровень защищенности.

Таким образом, защиту от утечки по акустическим каналам организуют: использование специальных облицовок, поглощающих звук, дополнительных тамбуров в проемах дверей, двойных оконных рам; применение аппаратуры звукового зашумления; закрытие вентиляционных проходов, систем провода в помещении электропитания, отопления, радио- и телефонных коммуникаций; эксплуатация категоризированных служебных помещений.

5.2. Средства защиты от утечек по акустическим каналам информации

Устройство однонаправленной передачи аудиоинформации «Аудиовентиль АД-3»

«Аудиовентиль АД-3» предназначен для обеспечения однонаправленной передачи аудиосигналов в информационных системах, имеющих в своем составе отдельные контуры обработки информации, в которых обрабатывается информация с различной степенью секретности (рис. 5.1).

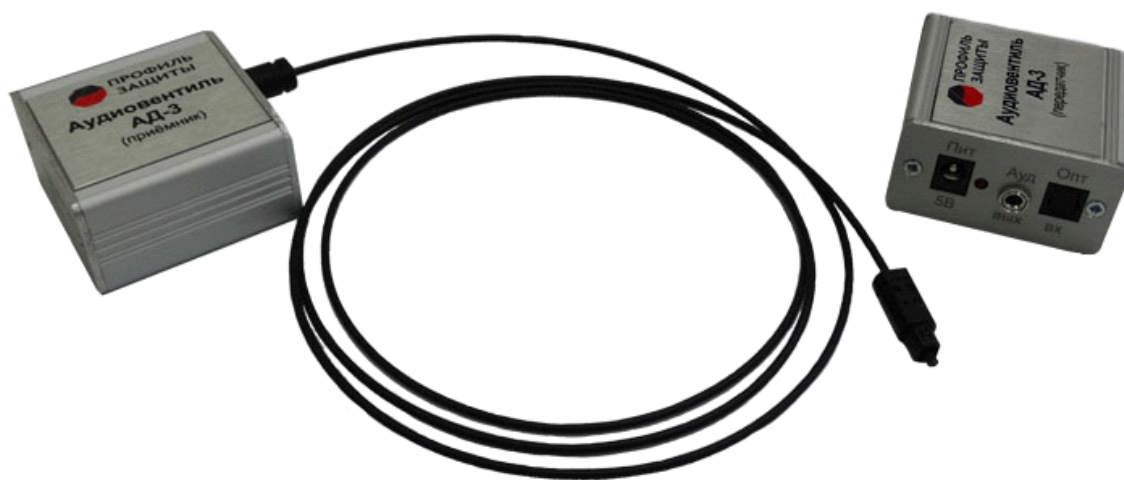


Рис. 5.1. Аудиоventиль АД-3

Это устройство может передавать аудиоинформацию из сегмента информационной системы более низкого уровня конфиденциальности в сегмент информационной системы с более высоким уровнем конфиденциальности (до «совершенно секретно» включительно) [28].

Аудиоventиль применяется в многоуровневых информационных системах, ситуационных и кризисных центрах, работающих с информационными ресурсами различных структур, ведомств или информацией разных категорий секретности.

Реализуемая при изготовлении Аудиоventиля АД-3 технология однонаправленной передачи данных позволяет осуществлять безопасную коммутацию устройств ввода/вывода и обработки аудиоинформации без использования дополнительных устройств и средств активной защиты информации. Однонаправленная передача аудиоинформации реализована за счёт применения схемы оптической развязки между передающим и приёмным модулями устройства (рис. 5.2).

Аудиоventиль АД-3 обеспечивает однонаправленную передачу аудиосигналов в рабочем диапазоне частот от 40 Гц до 15 кГц от технических средств источника аудиоинформации к техническим средствам потребителя. При этом затухание электрических сигналов в обратном канале передачи данных Аудиоventиля АД-3 составляет не менее 60 дБ при размещении передающего и приемного модулей на расстоянии не менее 1 метра друг от друга.

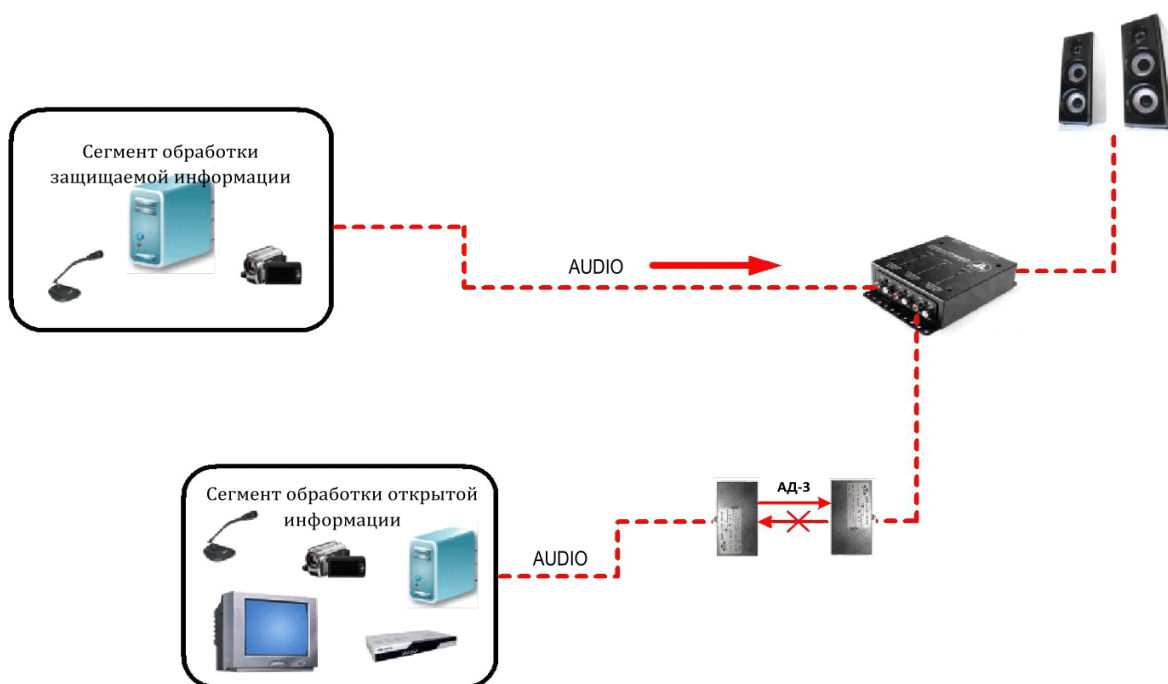


Рис. 5.2. Схема оптической развязки между передающим и приёмным модулями

Генератор акустического шума ЛГШ-304

Генератор акустического шума «ЛГШ-304» предназначен для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, путем формирования акустических маскирующих шумовых помех (рис. 5.3).

ЛГШ-304 соответствует:

- типу «Б» средства акустической защиты информации с активным (содержащим в своей конструкции индивидуальный задающий источник шума) преобразователем, питаемым по линии вторичного электропитания от центрального блока питания;
- требованиям к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) по 1 классу защиты.

Устройство может устанавливаться в выделенных помещениях до 1 категории включительно.



Рис. 5.3. Генератор акустического шума «ЛГШ-304»

ЛГШ-304 оснащен:

- визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа);
- счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы генератора в режиме формирования маскирующих помех.

Конструкция ЛГШ-304 обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.

Портативный анализатор спектра FPH Rohde&Schwarz

Анализатор спектра R&S FPH характеризуется расширенным частотным диапазоном, минимальными показателями погрешностями и богатым набором дополнительных принадлежностей. Полоса пропускания варьируется в интервале до 5 кГц до 2 ГГц. Этого более чем достаточно для решения большинства задач на любом промышленном объекте без применения вспомогательной аппаратуры (рис. 5.4).



Рис. 5.4. Портативный анализатор спектра FPH Rohde&Schwarz

Корпус R&S FPH полностью защищен от влаги и пыли, снижен вес по сравнению с предшественниками. Аккумуляторная батарея увеличенной емкости обуславливает бесперебойную работу в течение полного рабочего дня.

На экран анализатора нанесено матовое покрытие, благодаря которому достигается четкое отображение информации при ярком солнечном свете, а интегрированная подсветка позволяет использовать устройство в условиях плохой освещенности. Высокое разрешение матрицы (800 на 480 пикселей) обеспечивает непревзойденное качество изображения. Кнопки, расположенные на фронтальной панели, также имеют встроенную подсветку. Корпус отвечает требованиям стандарта MIL-PRF-28800F класса II (устойчивость к механическим воздействиям). Система охлаждения без вентиляционных отверстий гарантирует стабильность даже при повышенной влажности воздуха.

Анализатор R&S FPH поддерживает несколько вариантов управления — классический, используя функциональные клавиши, и при помощи сенсорного дисплея. Инновационный емкостный дисплей дает возможность устанавливать общие параметры, такие как опорный уровень, центральная частота и полоса обзора.

Данный измерительный прибор оснащен режимами, помогающими специалистам многих отраслей при обслуживании сложной электронной техники и решении задач, связанных с проведением анализа спектра, а именно: шесть маркеров (как абсолютные, так и относительные), шумовой маркер, две спектральные кривые, предоста-

новленные таблицы каналов, демодуляция электрических сигналов и многое другое.

R&S FPH по умолчанию имеет ряд функций, которые упрощают стандартные методы измерений. Совместное использование с программным обеспечением InstrumentView позволяет ускорить тестирование системы и свести к минимуму вероятность возникновения ошибки. При необходимости предварительные настройки могут быть откорректированы для выполнения специфических заданий.

Антенна измерительная дипольная АИ 5-3

Антенна измерительная дипольная активная АИ5-3 применяется для замера напряженности синусоидальных, импульсных и звуковых электрических полей радиопомех в экранированных камерах, лабораторных помещениях и на открытых площадках в комплексе с измерительными приемниками, селективными микровольтметрами любого типа, анализаторами спектра для гарантирования электромагнитной совместимости радиоэлектронных средств, защиты информации, а также предельно допустимых уровней электромагнитных полей для обеспечения мероприятий экологической защиты (рис. 5.5).

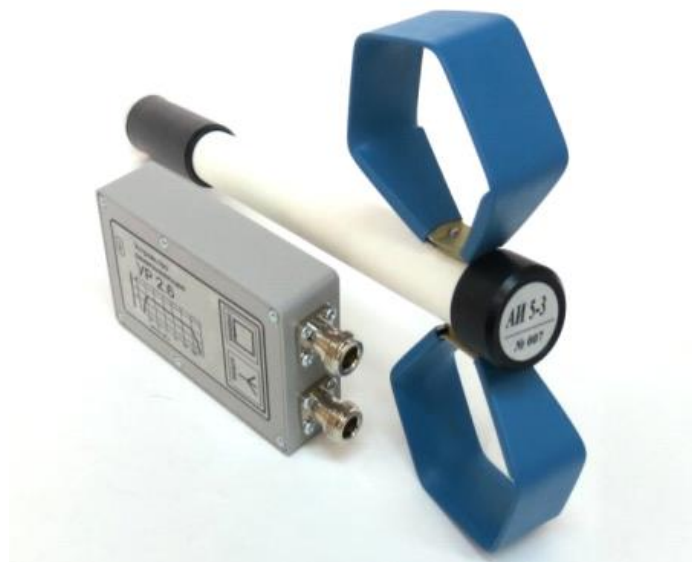


Рис. 5.5. АИ 5-3 антенна измерительная дипольная

Навигатор-П5М

Навигатор-П5М является программно-аппаратным комплексом на базе анализатора спектра FSH13 производства фирмы Rohde&Schwarz, 9 кГц до 13,6 ГГц. Предназначен для поиска и измерения побочных электромагнитных излучений и наводок при контро-

ле защищённости объектов информатизации от утечки информации, оценки эффективности средств защиты информации от утечки за счёт побочных электромагнитных излучений и наводок, автоматизации измерений и расчётов показателей защищённости информации при проведении специальных исследований (СИ) (рис. 5.6).



Рис. 5.6. Навигатор-П5М

Область применения устройства — проведение инструментального контроля защищённости информации от утечки за счёт побочных электромагнитных излучений и наводок при специальных исследованиях, контроле защищённости объектов информатизации, а также оценке эффективности принятых мер защиты информации.

Навигатор-П5М обеспечивает:

- расчёт показателей защищённости информации от утечки за счёт побочных электромагнитных излучений и наводок в ходе стендовых специальных испытаний;
- расчёт показателей защищённости информации от утечки за счёт побочных электромагнитных излучений и наводок в ходе объектовых специальных исследований при отсутствии систем автоматической защиты (САЗ) на объекте информатизации;
- расчёт показателей защищённости информации от утечки за счёт побочных электромагнитных излучений и наводок в ходе объек-

товых специальных исследований при функционировании системы автоматической защиты на объекте информатизации;

- инженерный анализ исследуемых объектов информатизации на присутствие побочных электромагнитных излучений и наводок;

- инженерный анализ систем активной защиты исследуемых объектов информатизации.

5.3. Средства защиты информации от несанкционированного доступа

Secret NetStudio представляет из себя комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.

Ключевые особенности:

- независимый от операционной системы (ОС) контроль внутренних механизмов средств защиты информации и драйверов;

- автоматизированная настройка механизмов для выполнения требований регуляторов;

- удобные графические инструменты мониторинга состояния компьютеров в защищаемой системе;

- комплексная защита на пяти уровнях (защита данных, приложений, сетевого взаимодействия, операционной системы и подключаемых устройств);

- интеграция независимых от ОС защитных механизмов для повышения общего уровня защищенности рабочих станций и серверов;

- создание централизованных политик безопасности и их наследование в распределенных инфраструктурах;

- поддержка иерархии и резервирования серверов безопасности в распределенных инфраструктурах.

Возможности:

- межсетевое экранирование с авторизацией соединений;

- система обнаружения и предотвращения вторжений;

- контроль устройств;

- замкнутая программная среда;

- антивирусная защита;

- паспорт ПО.

Защита данных:

- дискреционный контроль доступа к информации;

- мандатный контроль доступа к информации;

- контроль печати;
- шифрование контейнеров;
- контроль целостности данных;
- затирание данных;
- теневое копирование.

Программно-аппаратный комплекс (ПАК) Соболев

Электронный замок ПАК «Соболь» (рис. 5.7.) может быть использован:

- для предоставления доступа к информации на компьютере только тем сотрудникам, которые имеют на это право;
- возможности своевременного принятия администратором мер по восстановлению информации в случае повреждения ОС или важных информационных массивов, хранящихся на компьютере.

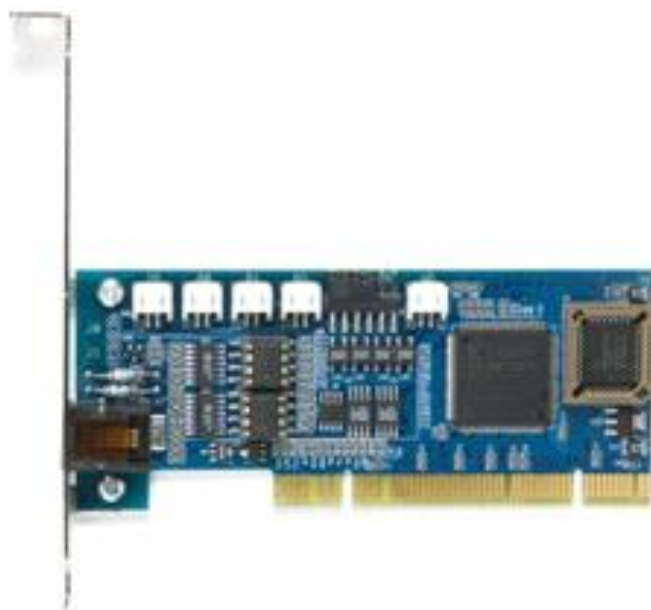


Рис. 5.7. Электронный замок ПАК «Соболь»

ПАК Соболев осуществляет блокировку загрузки операционных систем со съемных носителей.

После включения питания компьютера, замок «Соболь» перехватывает управление всеми устройствами ввода-вывода и не позволяет загрузиться нештатной операционной системе.

После успешной загрузки штатной копии операционной системы доступ к этим устройствам восстанавливается.

Запрет распространяется на всех пользователей компьютера, за исключением администратора.

Аутентификация пользователей. Идентификация и усиленная (двухфакторная) аутентификация пользователей с использованием персональных идентификаторов.

Контроль целостности. Используемая в комплексе «Соболь» система, контролирующая целостность, позволяет отслеживать неизменность файлов и физических секторов жесткого диска до момента загрузки операционной системы. Для этого вычисляются некоторые контрольные значения проверяемых объектов и сравниваются с ранее рассчитанными для каждого из этих объектов эталонными значениями. Формирование списка подлежащих контролю объектов с указанием пути к каждому контролируемому файлу и координат каждого контролируемого сектора производится с помощью программы управления шаблонами контроля целостности.

Использование операционных систем, содержащих файловые системы: №TFS5, №TFS, FAT32, FAT16, FAT12, UFS, EXT2 и EXT3 обеспечивает контроль целостности.

Контроль целостности системного реестра Windows. Данная возможность позволяет контролировать неизменность системного реестра Windows, что существенно повышает защищенность рабочих станций от несанкционированных действий внутри операционной системы.

Сторожевой таймер, позволяющий блокировать доступ к компьютеру, если после включения компьютера и по истечении определенного временного промежутка процесс управления не передан расширению BIOS комплекса «Соболь».

Регистрация попыток доступа к ПЭВМ. Электронный замок «Соболь» ведет системный журнал, в котором записи хранятся в специальной энергонезависимой памяти. Таким образом, он дает администратору информацию обо всех попытках доступа к компьютеру. В системном журнале отражаются следующие события:

- факт входа пользователя и его имя;
- предъявление незарегистрированного идентификатора пользователя;
- введение неправильного пароля;
- превышение числа попыток входа в систему;
- число и дата несанкционированного доступа.

Неизменность конфигурации. ПАК «Соболь» позволяет контролировать неизменность конфигурации компьютера — PCI-устройств,

ACPI, SMBIOS и оперативной памяти. Данная возможность существенно повышает защиту рабочей станции.

Аудиовентиль «СБ-18» устройство однонаправленной передачи аудиоинформации

Изделие «Аудиовентиль СБ-18» обеспечивает однонаправленную передачу аудиоинформации из сегмента информационной системы более низкого уровня конфиденциальности в сегмент информационной системы до 2 категории включительно (рис. 5.8).



Рис. 5.8. Аудиовентиль «СБ-18»

Реализуемая при изготовлении аудиовентиля технология однонаправленной передачи данных позволяет осуществлять безопасную коммутацию устройств ввода/вывода и обработки без использования дополнительных устройств и средств активной защиты информации.

Однонаправленная передача аудиоинформации реализована за счёт применения схемы оптической развязки между передающим и приёмным модулями устройства.

Фильтр ФП-6МА (40А) сетевой помехоподавляющий

Фильтр ФП-6МА (40А) сетевой помехоподавляющий марки является пассивным средством защиты информации. Данная модель

предотвращает информационные утечки по трехфазным цепям электропитания с номинальным током до 40 А, также защищает оргтехнику от внешних помех.



Рис. 5.9. Фильтр ФП-6МА (40А)

Данное устройство обеспечивает ослабление любых сигналов в частотном диапазоне определённом в РД ФСТЭК России. Помехоподавляющий сетевой фильтр марки ФП-6МА 40А сертифицирован по новым требованиям ФСТЭК России (Сертификат соответствия ФСТЭК России № 3895) и может быть установлен в категорированных помещениях до 1 категории включительно.

Защитное устройство ФСПК-10

Защитное устройство ФСПК-10 применяется в средствах вычислительной техники для защиты информации от утечки по однофазным цепям электропитания с заземляющим проводом напряжением 220 В частотой 50 Гц, а также для подавления высокочастотных помех в питающей сети в диапазоне частот от 125 кГц до 1000 МГц.

В общем случае, защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети (рис. 5.10).



Рис. 5.10. Защитное устройство ФСПК-10

ФСПК-200 Защитное устройство

Защитные устройства ФСПК-200 (фильтр сетевой помехоподавляющий комбинированный) предназначены для подавления напряжений помех в трехфазных четырехпроводных электросетях напряжением 220/380В, частотой 50 Гц, с максимальным рабочим током 200 А в диапазоне частот от 20 кГц до 1000 МГц (рис. 5.11).



Рис. 5.11. Защитные устройства ФСПК-200

ЛГШ-719 Кейс

Блокиратор сотовой связи ЛГШ-719 Кейс применяется для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах:

IMT-MC-450,
GSM900,
DSC/GSM1800, (DECT1800),
IMT-2000/UMTS (3G),
4G (LTE, WiMAX),
Bluetooth,
WiFi.

Устройство ЛГШ-719 Кейс объединяет в себе все возможности изделий ЛГШ-701, ЛГШ-712, ЛГШ-713, ЛГШ-704 и ЛГШ-705. ЛГШ-719 Кейс предотвратит несанкционированный съем информации через стандарты сотовой связи и заблокирует работу устройств несанкционированного прослушивания, созданных на основе сотового телефона, цифровых каналов передачи данных Bluetooth и WiFi (рис. 5.12).



Рис. 5.12. ЛГШ-719 Кейс

Блокиратор ЛГШ-719 Кейс подавляет работу сотовой связи в помещениях, в которых необходима полная тишина и может использоваться в переговорных комнатах, конференц-залах, в музеях, галереях, театрах, учебных аудиториях и церквях.

ЛГШ-719 Кейс легко устанавливается, и его эксплуатация не требует специальных навыков. Особенностью ЛГШ-719 Кейс является наличие шести независимых каналов, регулирующих мощность по каждому диапазону частот, что дает возможность образовывать зоны блокирования, руководствуясь требованиями администратора.

Фильтр ЛФС-100-3Ф (100А) сетевой трехфазный

Сетевой помехоподавляющий фильтр ЛФС-100-3Ф применяется для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации за счет наводок по трехфазным цепям электропитания напряжением до 380 В, частотой 50+0,5 Гц с максимальным рабочим током до 100 А.



Фото 5.13. Фильтр сетевой помехоподавляющий ЛФС-100-3Ф

Фильтр ЛФС-100-3Ф обеспечивает электромагнитную развязки по цепям электропитания радиоэлектронных устройств, средств вычислительной техники и электросетей промышленных и других объектов.

ЛФС-100-3Ф устанавливается в трехфазную четырехпроводную сеть напряжением (380+10%) В частоты 50 Гц без соблюдения полярности.

Система постановки виброакустических помех ЛГШ-402

Система постановки виброакустических помех ЛГШ-402 предназначена для защиты акустической речевой информации, циркулирующей в помещениях, предназначенных для обсуждения или воспроизведения, а также проведения мероприятий с обсуждением информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки информации по виброакустическому и акустическому каналам (рис. 5.14).



Рис. 5.14. Система постановки виброакустических помех ЛГШ-402

ЛГШ-402 соответствует:

- типу «А» — средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными (не содержащими в своей конструкции индивидуальные задающие источники шума, требующие электропитания) преобразователями;
- требованиям к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) по 4 классу защиты.

Устройство представляет собой двухканальный генератор шума. Величина сопротивления электромагнитных вибропреобразователей составляет 8 Ом. Допускается параллельно-последовательное подключение к каждому каналу до 4-х электромагнитных вибропреобразователей и акустического излучателя таким образом, чтобы общее сопротивление нагрузки составляло 4 Ом. Общее количество вибропреобразователей, подключаемых к генератору — 8 шт.

ЛГШ-402 оснащен визуальной системой индикации нормального режима работы.

Конструкция генератор ЛГШ-402 обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.

Блокиратор сотовой связи ЛГШ-725

Блокиратор сотовой связи ЛГШ-725 применяется для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, которые работают в стандартах:

IMT-MC-450,
GSM900,
DSC/GSM1800, (DECT1800),
IMT-2000/UMTS (3G),
LTE 2600 (4G, WiMAX),
LTE 800 (4G),
Bluetooth,
WiFi 2.4 ГГц,
WiFi 5 ГГц.

Устройство является новой модификацией популярного генератора ЛГШ-719 с дополнительным подавлением сигналов WiFi на частоте 5 ГГц (рис. 5.15).

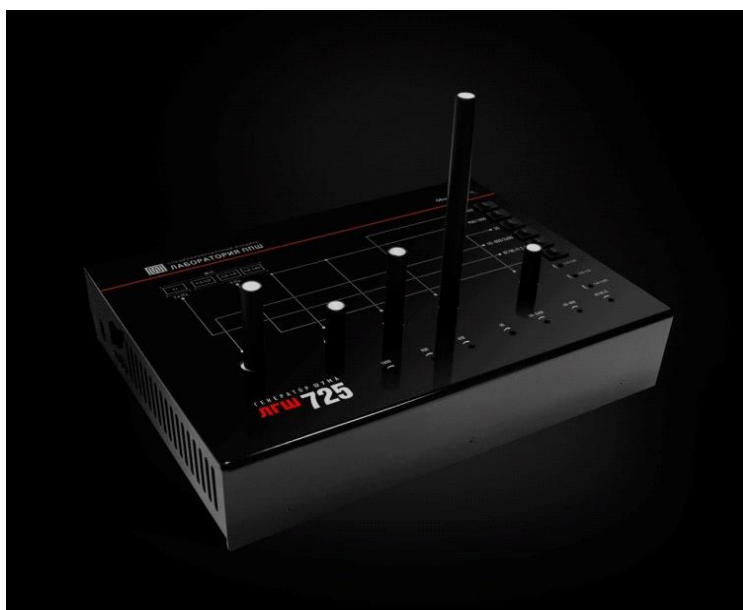


Рис. 5.15. Блокиратор сотовой связи ЛГШ-725

ЛГШ-725 предотвратит несанкционированный съем информации через стандарты сотовой связи и заблокирует работу устройств несанкционированного прослушивания, созданных на основе сотового телефона, цифровых каналов передачи данных Bluetooth и WiFi.

Видеодиод ВД-2 (заключение ФСБ)

Видеодиод ВД-2 предназначен для осуществления односторонней передачи видеосигналов стандарта DVI-D в системах обработки информации, имеющих в своем составе отдельные контуры, в которых может обрабатываться информация с различной степенью секретности (рис. 5.16).



Рис. 5.16. Видеодиод ВД-2

Видеодиод ВД-2 обеспечивает одностороннюю передачу видеoinформации, которая обрабатывается специальными техническими средствами, для ее защиты от непреднамеренной передачи из контура с высшей степени секретности обрабатываемой информации в контур с низшей степенью секретности обрабатываемой информации. Используемая в устройстве технология односторонней передачи данных позволяет осуществлять безопасную коммутацию устройств ввода/вывода и обработки без использования дополнительных устройств и средств активной защиты информации.

Видеодиод ВД-2 применяется для подключения комплекта устройств ввода/вывода и обработки видеoinформации в многоуровневых информационных системах, ситуационных и кризисных центрах, работающих с информационными ресурсами различных струк-

тур, ведомств или разной категорией защищаемой информации. Устройство может устанавливаться и эксплуатироваться в выделенных помещениях до 1 категории включительно, находящихся на территории Российской Федерации, в том числе в органах государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций, осуществляющих в соответствии с законодательством Российской Федерации о государственной тайне проведение работ, связанных с использованием сведений, составляющих государственную тайну, на территории Российской Федерации.

Видеодиод ВД-2 может использоваться в системах обработки информации, содержащей сведения, составляющие государственную тайну со степенью секретности до «совершенно секретно» включительно.

ПЭВМ Secret

ПЭВМ в защищенном исполнении семейства «Secret» является средством вычислительной техники в защищенном исполнении от утечки информации по каналу побочных электромагнитных излучений и наводок и может применяться на объектах вычислительной техники 2 и 3 категории, устанавливаться в выделенных помещениях до 1 категории включительно, а также использоваться для обработки информации, содержащей сведения, составляющие государственную тайну (рис. 5.17) [31].



Рис. 5.17. ПЭВМ Secret

КриптоПро CSP

КриптоПро CSP представляет собой криптопровайдер — программный модуль, позволяющий осуществлять криптографические операции в операционных системах, управление которым происходит с помощью функций CryptoAPI. КриптоПро CSP поддерживает российские криптографические алгоритмы (ГОСТ) и имеет сертификаты ФСБ России.

КриптоПро CSP применяется:

- для авторизации и обеспечения юридической значимости электронных документов при осуществлении обмена ими между пользователями, путем проведения процессов формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с государственными стандартами ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;
- контроля целостности информации и соблюдения конфиденциальности, используя ее шифрование и имитозащиты, в соответствии с ГОСТ 28147-89;
- гарантирования аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- управления основными элементами системы в соответствии с регламентом средств защиты [31].

Комплекс радиомониторинга Кассандра K21

Комплекс радиомониторинга Кассандра K21 предназначен для постоянного, периодического или оперативного мониторинга радиобстановки для возможного обнаружения несанкционированных радиоизлучений, имеющих сложные алгоритмы скрытия информации, анализа цифровых стандартов связи (рис. 5.18).



Рис. 5.18. «Кассандра K21»

Данный комплекс включает в себя новейшие технические решения и использует современное программное обеспечения «RadioInspector».

Расширенный диапазон частот — до 21000 МГц. Ведение радиомониторинга без применения сверхвысокочастотных конвертеров.

Максимальная скорость сканирования свыше 2000 МГц/св полосе анализа 20 кГц, динамический диапазон — более 113 дБ.

«Чистота» спектра внутренних тюнеров в ВЧ- и СВЧ-диапазоне, отсутствие пораженных частот и внутренних комбинационных помех.

Автоматическая классификация излучений и возможность анализа цифровых стандартов связи. Опция DTest дает возможность автоматически идентифицировать и проводить анализ цифровых стандартов связи DECT, TETRA, GSM, Bluetooth, DMR, APCO25, DRM, DVB, демодулировать APCO25, DMR(MOTOTRBO), DRM, отображать PAL/SECAM/NTSC ТВ, проводить цифровой анализ сигналов (векторная диаграмма, фильтрация, децимация и цифровой сдвиг сигналов в векторной форме (I/Q)). ПО «RINspectorWiFi» осуществляет поиск устройств и анализ сети Wi-Fi.

Удалённое управление комплексом по общей локальной или глобальной сети.

Программное обеспечение комплекса «RINspector» [31]:

- особенный по своему качеству и возможностям быстро модифицироваться и конфигурироваться в широких диапазонах пользовательский интерфейс;
- выстраивание комплекса заданий на сканирование в границах рабочего спектра с неограниченным числом по порядку обрабатываемых вопросов, каждый из которых имеет свои параметры;
- обзор текущих, минимальных, максимальных и средних величин принимаемых сигналов;
- спектрограмма — вид во времени в 2D или 3D представлении, с возможностью не ограничивать время записи;
- сохранение в полном объеме итогов работы и способность проводить отложенный анализ, приведение в действие сохраненного задания и дальнейшая запись в базу данных панорам;
- сохранение эталонной панорамы и возможность сравнения с ней;
- маркерные и курсорные измерения;
- метод разнесенного приема с использованием антенного коммутатора;
- управляемая линия порога, адаптивный и динамический порог;
- перечень сигналов, превысивших порог;
- создание базы данных частотных присвоений и средства их обработки, включая специализированный калькулятор;
- ВЧ-анализатор спектра для анализа отдельных сигналов в масштабе реального времени;
- НЧ-анализ — осциллограф, низкочастотный анализатор спектра, октавный анализатор спектра, запись фонограмм, включая пять секунд информации до начала записи, анализ и редактирование сохраненного;
- автоматические действия при обнаружении — запись звукового сигнала, анализ сигналов, в частности, на принадлежность к классу аналоговых телевизионных сигналов;
- дополнительный анализ перечня обнаруженных сигналов (числовой и графический), создание отчетов об изученных диапазонах частот и обнаруженных сигналах, способность переводить их в форматы Microsoft Word®, Microsoft Excel®, в текстовые и графические файлы;
- руководство дополнительным приемником для независимого низкочастотного анализа;
- свитч на 4 канала в ВЧ-диапазоне (до 6ГГц), дополнительный низкочастотный вход (до 30МГц), СВЧ антенна в комплекте;

- «пользовательский» интерфейс, свободные параметры окон, подсказки, помощь;
- масштабируемая одним «кликом» панорама спектра;
- масштабируемая спектрограмма (водопад) 2D и 3D с прокруткой;
- адаптивный порог;
- список обнаруженных сигналов со статистической компьютерной программой для просмотра файлов;
- анализатор спектра в диапазоне до 8 МГц, работающий в масштабе реального времени, с возможностью не ограничивать время анализа;
- задание на обработку обнаруженных сигналов в автоматическом режиме;
- блок управления дополнительным приемником;
- низкочастотный осциллограф, анализатор спектра, октавный анализатор;
- запись данных IQ и демодулированных АМ и FM сигналов;
- база данных частотных присвоений и специализированный калькулятор;
- увеличение функционального потенциала благодаря дополнительным возможностям.

Устройство защиты конфиденциальных переговоров TF-012N

Защита речевой информации при проведении конфиденциальных переговоров от ее перехвата при возможном использовании средств негласного контроля информации (рис. 5.19).



Рис. 5.19. Устройство защиты конфиденциальных переговоров TF-012N

Областью применения является защита конфиденциальных переговоров, проводимых в помещении или автомобиле, не оборудованных системами защиты речевой информации посредством постановки акустической маскирующей помехи [29].

Кабина переговорная КПЗИ-1

Кабина переговорная предназначена для проведения закрытых мероприятий и разговорам по телефонам спецсвязи (рис. 5.20).



Рис. 5.20. Кабина переговорная КПЗИ-1

Виброакустический шумогенератор СИ-3030

Предназначен для защиты помещений от прослушивания через строительные элементы конструкции. Принцип действия прибора основан на маскировании спектра речи шумовой помехой, излучаемой в стены, перекрытия, окна, воздуховы (рис. 5.21) [27].



Рис. 5.21. Виброакустический шумогенератор SI-3030

***Устройство блокирования утечки информации
по акустическому каналу SpyLockJack***

Предназначено для защиты речевой информации, имеющейся в местах нахождения владельца сотового телефона при его активировании для прослушивания через каналы сотовой связи, а также для защиты от возможной утечки речевой информации через активацию видеокамеры в мобильном телефоне (рис. 5.22) [27].



Рис. 5.22. SpyLockJack

Генератор акустической помехи «БУБЕН»

Изделие используется при проведении конфиденциальности переговоров для создания акустических помех в замкнутом помещении (рис. 5.23).



Рис. 5.23. Генератор акустической помехи «БУБЕН»

Изделие работает в одном из двух режимов на выбор:

- создание речеподобной помехи;
- создание помехи типа «белый шум».

Режим «речеподобная помеха»: генератор создает помеху, «разрушающую» смысл отдельных фраз и предложений при конвертировании речевого сигнала в электрический при помощи средств звукового контроля всех видов (диктофонов, проводных микрофонов, радиозакладок, стетоскопов и пр.). Принцип записи или передачи речевого сигнала в конкретном акустическом средстве контроля при этом значения не имеет.

Режим «белый шум»: генератор создает помеху, образующую шумовые помехи во время записывания или прослушивания звукового сигнала посредством негласного съема информации. Принцип записи или передачи речевого сигнала в конкретном акустическом средстве контроля при этом значения не имеет.

Преимущество генератора речеподобной помехи заключается в энергетическом выигрыше в несколько дБ. То есть заданное снижение разборчивости защищаемых переговоров обеспечивается при

меньшем уровне маскирующего шума. Если регламент проведения переговоров требует применения генератора «белого шума», рекомендуется использовать именно этот режим [27].

Портативный генератор акустического шума ЛГШ-303

Изделие применяется для защиты речевой информации от перехвата по прямому акустическому каналу. Изделие мобильно и предназначено для работы в помещениях, (автомобилях) и других местах, не требующих стационарных средств защиты информации по прямому акустическому каналу и не оборудованных стационарными источниками питания (рис. 5.24) [27].



Фото 5.24. Портативный генератор акустического шума ЛГШ-30

Устройство защиты оптоволоконной линии от утечки акустической информации «Фотон-М»

«Фотон-М» предназначено для защиты акустической речевой информации от ее утечки вследствие возможных акустооптических преобразований в элементах оптического сетевого интерфейса технического средства, оптической среде ВОЛС (рис. 5.25) [27].



Рис. 5.25. Фотон-М

Акустический сейф «Ладья-2Л»

Акустический сейф Ладья-2Л — новинка на рынке отечественного оборудования для защиты ценных сведений. Изделие предназначено для предотвращения утечки конфиденциальной речевой информации через микрофон сотового телефона. Оно выполнено в виде изящной каменной подставки с отсеком для размещения одного смартфона. Благодаря наличию микролифта, помещать телефон в сейф и доставать девайс очень удобно (рис. 5.26) [30].

Модель Ладья-2Л предназначена для зашумления микрофона смартфона путем постановки помехи в звуковом диапазоне. Устройство способно создавать как бесшумную ультразвуковую, так и слышимую акустическую помеху.

Дополнительно акустический сейф оснащен встроенным излучателем радиопомехи, которая блокирует стандарты связи bluetooth и wi-fi. Благодаря этому, к помещенному в устройство гаджету злоумышленники не смогут подключиться через беспроводные локальные сети.

На корпусе устройства находится кнопка микролифта, кнопка включения/выключения прибора, световые индикаторы уровня заряда батареи и энергетической активности процессора. Работает оборудование от встроенного аккумулятора и от сети.



Фото 5.26. «Ладья-2Л»

Подавитель «Тайфун-3ДК»

«Тайфун-3ДК» предназначен для предотвращения несанкционированной записи разговора, записываемого на цифровые и кинематические диктофоны, а также для блокирования средств несанкционированного прослушивания и передачи данных, использующих каналы систем мобильной связи.

Можно также применять устройства для предотвращения утечки данных с использованием проводных микрофонов и малогабаритных передатчиков, в случае их попадания в сектор действия устройства.

Камуфлирован в атташе-кейс и имеет возможность эксплуатации как в стационарных, так и полевых условиях (рис. 5.27) [30].



Рис. 5.27. «Тайфун-3ДК»

Мультичастотный подавитель «Терминатор 130-5G»

Широкий радиус воздействия: 130 м — расстояние, на котором блокиратор может заглушить сигнал компьютерного/сотового соединения или беспроводной сети (рис. 5.28).

Гибкое регулирование параметров подавления. Дальность блокирования частот можно откорректировать с помощью специального регулятора. Это поможет настроить работу аппарата под определенную задачу и размеры помещения.

Дальность действия прибора пропорциональна изменению мощности ретранслятора.

Мультичастотный подавитель «Терминатор 130–5G» полностью отключает работу любого роутера, следовательно, использовать даже самые новые гаджеты, которые подключаются к сети wi-fi для входа в интернет, бесполезно.



Рис. 5.28. «Терминатор 130-5G»

Следует отметить, что поле воздействия может находиться в прямой зависимости от места дислокации базовых станций оператора. Радиус работы указан, опираясь на расчеты уровня сигнала мобильной связи в пределах 60–80 %. Для лучшей работы прибора необходимо установить его на расстоянии ≈ 200 м от ближайшей радиовышки или других источников беспроводного соединения [30].

Акустический сейф «ЛАРЕЦ-5У3»

Ларец-5У — акустический сейф для размещения до 5 мобильных телефонов. Этот сейф предназначен для подавления опции «диктофон» на смартфонах и для защиты микрофонов коммуникационных устройств от дистанционной активации. Использование данного акустического контейнера гарантирует, что злоумышленники не смогут с помощью хакерского ПО подключиться к смартфону кого-либо из участников переговоров, активировать микрофон и прослушать разговор. Также ни один из переговорщиков не сможет скрытно записать беседу на диктофон сотового телефона (рис. 5.29).



Рис. 5.29. «Ларец-5У3»

Акустический сейф «СКАТ 22»

«СКАТ 22» предназначен для защиты речевой информации от утечки как через каналы сотовой связи группы мобильных телефонов при их несанкционированной дистанционной активации, так и от утечки по речевому каналу при несанкционированной активации функции «диктофон» мобильных устройств. Изделие конструктивно исполнено в носимом варианте и размещается в ударопрочном кейсе (рис. 5.30) [27].



Рис. 5.30. «СКАТ 22»

Акустический сейф «КОКОН-DS»

Изделие «КОКОН-DS» применяется для защиты речевой информации, вращающейся в местах нахождения владельца сотового телефона, при его негласном дистанционном активировании с целью прослушивания через каналы сотовой связи (рис. 5.31).



Фото 5.31. Акустический сейф «КОКОН-DS»

Принцип действия устройства основан на дистанционном контроле энергетической активности телефона. В состоянии «сна» она

минимальна. Если в телефоне начинает работать любое приложение, то это приводит к изменению энергетического состояния, что фиксируется соответствующими датчиками и запускает механизм акустической защиты телефона. Этот принцип позволяет реализовать защиту любого сотового телефона от удаленной дистанционной активации (в том числе и от активной функции «диктофон»).

При включении переключателя раздается короткий звуковой сигнал, свидетельствующий о готовности устройства к работе. Включение акустического шумогенератора свидетельствует о несанкционированном подключении к телефону и начале информационного обмена. Интеллектуальный режим реализуется следующим образом: после начала сеанса связи шумогенератор включается с определенной задержкой (примерно в 5–10 секунд), достаточной для того, чтобы услышать штатные звуковые сигналы (гудки) телефона и принять вызов. При нажатии нижней круглой кнопки, отключается акустическая помеха и устройство переходит в режим индикации, сигнализируя об активности встроенным светодиодом [27].

***Программно-аппаратный комплекс защиты
телефонных переговоров по каналам сотовой связи
«Референт-PDA»***

Программно-аппаратный продукт «Референт-ПДА» (рис. 5.32) создан для устройств как смартфон (коммуникатор), управляемый операционной системой WindowsMobile 2003/2005. Референт ПДА предотвращает прослушивание переговоров, происходящих между двумя коммуникаторами. Комплект состоит из SD/miniSD/microSD — модуля, программного обеспечения и смартфона qtek-8500 [27].



Рис. 5.32. Референт-PDA

Старт программы происходит автоматически при подключении SD/miNoiSD/microSD - модуля «Референт ПДА», на экране коммуникатора при этом в правом нижнем углу появляется значок индикации запуска программы в фоновый режим. Чтобы вызвать в защищенном режиме другого абонента, следует нажать на значок индикации и в открывшейся программе «Референт ПДА» произвести те же самые действия, что и при обычном вызове. Когда поступает звонок от другого комплекта Референт ПДА, вместо программы «телефон» автоматически открывается интерфейс программы «Референт ПДА», затем все действия как при обычном звонке.

В интерфейс программы входит: кнопки управления вызовом, наборное поле, кнопку отмены ввода последней цифры и индикатор, который отображает набираемый номер, номер вызывающего абонента при входящем вызове, состояния при установлении соединения и т. п.

П р и м е ч а н и е : Возможна индивидуальная разработка под аппараты (телефоны/смартфоны) разных производителей марок и операционной системы на базе данного программно-аппаратного комплекса. Ориентировочная стоимость (по согласованию с Заказчиком) предлагаемой разработки составляет 1 500 000 рублей и срок исполнения работ 3–4 месяца.

Маскиратор речи/изменитель голоса «i-Stranger» (гарнитура)

«i-Stranger» предназначен для работы со смартфонами и диктофонами, такими как Apple, Samsung, HTC и других производителей (рис. 5.33).



Рис. 5.33. «i-Stranger»

Для совместимости телефон должен иметь 4-х контактный разъем 3,5 мм. (Если в телефоне три контакта, то изменения голоса происходить не будет!)

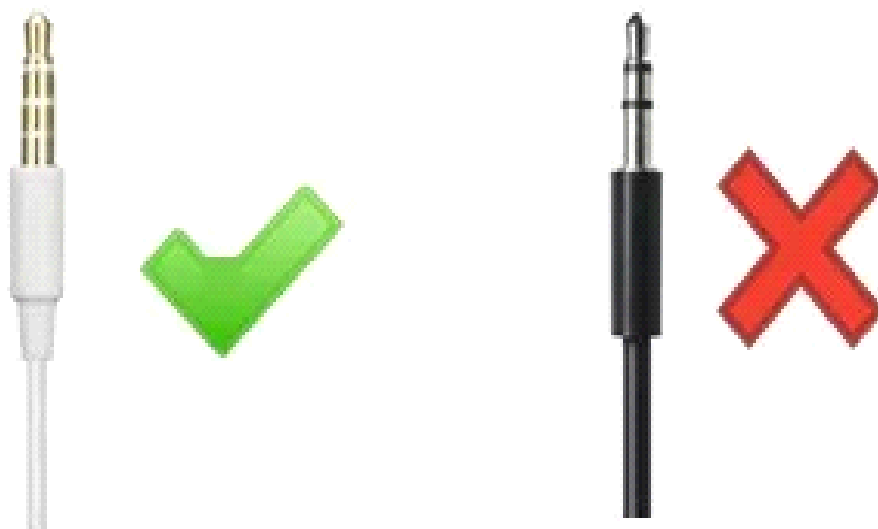


Рис. 5.34. Разъёмы к мобильным устройствам

Изменитель голоса имеет два режима работы: «low» (низкий тон) (красный светодиод) и «high» (высокий тон) (синий светодиод). Для изменения режима работы следует нажать на кнопку «mode». Изменить режим можно как до начала, так и в процессе работы [27].

Индикатор активации мобильных средств связи «GSM-box II»

Новейшие технические средства мобильной связи, применяющие цифровые протоколы для передачи речевой информации и данных, могут стать опасным инструментом для несанкционированного доступа к информации. Подмена или подарок модифицированного устройства, перепрограммирование мобильного телефона, внедрение вируса в коммуникатор предоставят злоумышленникам возможность получить доступ к имеющейся информации и возможность слушать все разговоры, которые ведутся рядом с мобильным телефоном. Специальные программы, прошивки, дополнительные электронные приспособления, применяемые для такого рода шпионажа, дают возможность получать информацию без согласия правообладателя и при отсутствии внешних признаков несанкционированного запуска устройства (отсутствие вызова и индикации на экране и т. п.). Интеллектуальные детекторы радиоизлучения дают возможность оставлять мо-

бильный телефон включенным, оставаться на связи и, одновременно, держать под контролем режимы передачи данных и выявлять нештатные подключения, в отличие от обесточивания мобильных телефонов, использования радиоподавителей.

GSM-box II — устройство применяется для определения и индикации активного состояния мобильных средств связи (GSM 900/1800, CDMA850, WCDMA2100 (3G, UMTS) и Wi-Fi/Bluetooth). Специальная, создаваемая автоматически, акустическая помеха создает препятствие для доступа к речевой информации несанкционированно через мобильный телефон без ведома владельца (рис. 5.35).



Рис. 5.35. GSM-box II

Акустический сейф «Скат 20-10»

Сейф акустический «Скат 20-10» предназначен для защиты речевой информации от утечки как через каналы сотовой связи группы мобильных телефонов и планшетов при их несанкционированной дистанционной активации, так и от утечки по речевому каналу при несанкционированной активации функции «диктофон» мобильных устройств. Кроме того, в акустическом сейфе «Скат 20-10» применяется экранированный контейнер для хранения 20 сотовых телефонов и 10 планшетов, что обеспечивает более надёжную защиту информации от возможных утечек (рис. 5.36) [31].



Рис. 5.36. Скат 20-10

***Автоматизированный комплекс выявления
акустопараметрических каналов утечки информации «КРОНА А1»***

Комплекс «КРОНА А1» предназначен для обнаружения и локализации электронных устройств негласного получения информации (ЭУНПИ), передающих данные по радиоканалу, использующих все известные средства маскирования, выявления каналов утечки информации, созданных за счет акустопараметрических преобразований, а также для решения широкого круга задач радиомониторинга. Позволяет обнаруживать пассивные и полупассивные акустопараметрические электромагнитные отражатели (эндовибраторы) в диапазоне частот от 30 МГц до 12 ГГц.

Разработан на основе многолетнего опыта создания подобных систем и включает в себя самые инновационные алгоритмы обнаружения ЭУНПИ. Применение сразу нескольких алгоритмов обнаруже-

ния, основанных на индивидуальных принципах демаскирования ЭУНПИ, дает возможность с большим процентом достоверности устанавливать наличие ЭУНПИ, замаскированных по алгоритмам модуляции и по способам передачи (ЭУНПИ с цифровыми каналами передачи данных, с накоплением информации, с перестраиваемой частотой и т. д.).

Данный комплекс можно применять как для экспресс-анализа присутствия радиопередающих ЭУНПИ в контролируемом помещении, так и для круглосуточного наблюдения за электромагнитной обстановкой в одном или нескольких контролируемых помещениях.

Комплекс «КРОНА А1» имеет эффективный алгоритм выделения полезного информативного сигнала в сложной помеховой обстановке, высокую точность измерений, что обеспечивает достоверные результаты поиска каналов утечки речевой информации, образованных за счет акустопараметрических преобразований (рис. 5.37) [31].



Рис. 5.37. КРОНА А1

**Автоматизированный комплекс выявления
акустопараметрических каналов утечки информации
«БАСТИОН-М2»**

Комплекс выявления акустопараметрических каналов утечки информации «БАСТИОН-М2» (рис. 5.38) обеспечивает [31]:

- обнаружение и локализацию электронных устройств негласного получения информации (ЭУНПИ), передающих данные по радиоканалу с различными видами модуляции, в том числе использующих цифровые стандарты связи;
- выявление широкополосных сигналов (ШПС) с полосой выше 200 МГц, сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ), сигналов сверхкороткой передачи (СКП);
- выявление новых радиоизлучений;
- прием сигналов с нескольких антенн (метод разнесенного приема);
- локализацию местоположения источника постоянно присутствующего опасного сигнала в контролируемой зоне методом пространственной локализации;
- возможность круглосуточного ведения сеанса радиоконтроля;
- контроль диапазона частот;
- контроль фиксированных частот;
- контроль сетки частот;
- выявление корреляционным методом радиоизлучений с признаками модуляции тестовым акустическим сигналом;
- обнаружение пассивных и полуактивных акустопараметрических электромагнитных отражателей (эндовибраторов);
- исследование каналов утечки информации, образованных за счет эффекта ВЧ-навязывания в отходящих коаксиальных кабелях;
- оценку сигналов в силовых сетях, слаботочных и коаксиальных линиях;
- обнаружение ИК-излучателей;
- выполнение комплексных заданий.



Рис. 5.38. БАСТИОН-М2

***Программно-аппаратный комплекс выявления
технических каналов утечки акустической информации
за счет высокочастотного облучения
«Гранат»***

Программно-аппаратный комплекс выявления технических каналов утечки акустической информации за счет высокочастотного облучения «Гранат» предназначен для выполнения работ по оценке эффективности защиты акустической речевой информации от утечки за счет высокочастотного облучения (рис. 5.39) [27].



Рис. 5.39. «Гранат»

Система защиты «Security Studio Endpoint Protection»

Данная система обеспечивает защиту компьютера с применением межсетевого экрана, антивируса и средства обнаружения вторжений. Обеспечивает безопасную и комфортную работу с сетью Интернет, предотвращая любые попытки проникновения на компьютер вредоносного программного оборудования, блокируя нежелательный трафик.

Сертификаты SecurityStudio Endpoint Protection дает возможность выполнить требования ФСТЭК по защите персональных данных. Систему можно использовать совместно с СЗИ от НСД Secretnet для гарантии комплексной защиты автоматизированного рабочего места.

Сканер безопасности «X-Spider»

Анализатор уязвимостей, ошибок в отладке, с гибкой системой сканирования и проверки системы на безопасность.

Сканер используется для решения следующих задач:

- инвентаризация сети;
- идентификация уязвимостей и проблем в безопасности;
- планирование процесса устранения;
- контроль устранения;
- анализ тенденций защищенности;
- обеспечение соответствия требований стандартов PCI DSS и федерального закона «О персональных данных».

Распределенный межсетевой экран «TrustAcces»

«TrustAccess» — распределенный межсетевой экран высокого класса защиты с централизованным управлением и аудитом событий информационной безопасности, применяется для защиты серверов и рабочих станций локальной сети от несанкционированного доступа, разграничения сетевого доступа к информационным системам организации.

Блок электропитания и управления «Соната-ИП4.1»

Блок электропитания и управления «Соната-ИП4.1» (рис. 5.40) предназначен:

- для электропитания и управления подключаемыми к выходу «нагрузка» элементами системы активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ», модель 4Б, в ходе ее эксплуатации;
- управления подключаемыми к выходу «нагрузка» средств активной защиты информации от утечки за счёт побочных электромагнитных излучений и наводок («Соната-РЗ», «Соната-РЗ.1», «Соната-РСЗ»);
- автоматический контроль исправности и режимов работы подключенных к нему устройств;
- настройки (установки интегрального уровня, корректировки спектра и т. п.) и считывания из них служебной информации (состояние счетчика наработки, код ошибки при отказе, индивидуальный ад-

рес и т. п.), при инсталляции (проверке) комплекса технических средств защиты информации [27].



Рис. 5.40. «Соната-ИП4.1»

Акустический сейф «Ладья-Л»

Акустический сейф выполнен в виде лаконичной прямоугольной подставки (рис. 5.41). Корпус изготовлен из натурального камня в цвете серый мрамор. Данное изделие предназначено для предотвращения утечки конфиденциальной информации через микрофон смартфона. Чтобы не допустить прослушивания разговоров, ведущихся в непосредственной близости от телефона, достаточно поместить девайс в отсек сейфа и включить прибор [27].



Фото 5.41. Ладья-Л

В акустический сейф встроен генератор низкочастотных помех, которые зашумляют звуковой диапазон. Генератор расположен таким образом, чтобы обеспечить максимальную мощность помехи в той части отсека, где находится микрофон смартфона. Изделие может работать в двух режимах:

- бесшумный режим, в котором осуществляется излучение только ультразвуковой помехи;
- режим генерации слышимого акустического шума.

Акустическая шумовая помеха обеспечивает стопроцентную защиту конфиденциальных сведений от утечки через микрофон сотового телефона. Даже если злоумышленники смогут удаленно подключиться к микрофону девайса, при попытке прослушать информацию они услышат только помеховый шум.

Для удобства эксплуатации «Ладья-Л» оснащен индикаторами энергетической активности процессора и уровня заряда батареи. Работает устройство от аккумулятора и от сети 220 Вольт.

SEL-151 «Шкатулка-люкс»

Изделие предназначено для защиты речевой информации от дистанционного прослушивания через негласно активированный сотовый телефон путём акустического зашумления его микрофона (рис. 5.42). Контролируемые сигналы: GSM, 3G, 4G, Wi-Fi, Bluetooth[27].



Рис. 5.42. SEL-151 «Шкатулка-люкс»

При попытке несанкционированной активации телефонного аппарата в режиме удалённого информационного доступа с целью прослушивания окружающей обстановки уровень напряжённости электромагнитного поля вблизи телефона незначительно повышается. Именно это повышение фиксируется детектором электромагнитного поля, входящим в состав устройства «шкатулка».

После фиксации факта повышения уровня электромагнитного поля автоматически включается генератор акустических шумовых помех, излучатель которого расположен в непосредственной близости от микрофона сотового телефона. Уровень акустического шума на входе микрофона телефонной трубки таков, что он гарантированно обеспечивает зашумление микрофона сотового телефона. Этот же шум служит владельцу сотового телефона сигналом того, что его телефонный аппарат активирован.

Отличительные особенности:

- детектор устройства определяет включение не только голосовых каналов передачи мобильных телефонов, но и их работу в режимах широкополосной передачи данных;
- генератор акустической помехи устройства излучает сигналы двух типов: «белый акустический шум» и псевдослучайный сигнал типа «речевой хор»;
- устройство имеет встроенный счетчик учёта времени работы с выводом информации на ЖК-экране и индикацию режимов работы и зарядки батареи.

Изделие выполнено из натурального природного камня.

Акустический сейф с ультразвуковой помехой «ASU-20»

Изделие (рис. 5.43) предназначено для защиты речевой и любой другой акустической информации от утечки через смартфоны, планшеты и гарнитуры за счет навязывания ультразвуковой помехи [27].

Материал: натуральное дерево.



Рис. 5.43. ASU-20

***Акустический сейф ультразвуковой
с автоматическим выключателем «ASU-20А»***

Акустический сейф ультразвуковой с автоматическим выключателем ASU-20А с автоматическим выключателем (рис. 5.44) предназначен для защиты речевой и любой другой акустической информации от утечки через смартфоны, планшеты и гарнитуры за счет навязывания ультразвуковой помехи [27].

Материал: натуральное дерево.



Рис. 5.44. ASU-20A»

В отличие от пассивных шкатулок и блокираторов, включающих подавление только в момент активности телефона, постоянно работающий подавитель в ASU-20A гарантирует стопроцентную блокировку микрофонов смартфонов и гарнитур.

Благодаря применению мощных ультразвуковых излучателей в непосредственной близости от микрофона сотового телефона обеспечивается подавление любой акустической информации. При закрытой крышке шкатулка работает бесшумно. Прием входящих звонков и сообщений не блокируется. Когда телефоны находятся в шкатулке, звуки звонков и сообщений слышны снаружи, а все внешние звуки внутри шкатулки заглушаются. Время работы акустического сейфа не ограничено.

Почему так важно подавить именно микрофон, при этом подавление радиоканала не так важно или даже не нужно вообще? Даже в отсутствие сети, когда включен обычный GSM-подавитель, любая шпионская программа запишет разговоры в память и передаст их, как только сеть будет снова доступна. Поэтому важно, чтобы в любом случае микрофон был полностью и постоянно заблокирован.

Акустический сейф «СКАТ 5»

«СКАТ 5» предназначен для защиты речевой информации от утечки как через каналы сотовой связи группы мобильных телефонов при их несанкционированной дистанционной активации, так и от утечки по речевому каналу при несанкционированной активации функции «диктофон» мобильных устройств (фото. 5.45).



Фото. 5.45. Акустический сейф СКАТ 5

Особенности:

- ультразвуковая защита по НЧ-тракту;
- розовый шум(постоянный фоновый звук);
- одновременная защита 5 телефонов;
- пассивная электромагнитная защита предотвращает любой радиообмен по каналам сотовой связи.

Акустический сейф «Ларец-1»

Изделие «Ларец-1» предназначено для защиты речевой информации, циркулирующей в местах пребывания владельца сотового те-

лефона, в случае его негласной дистанционной активизации с целью прослушивания через каналы сотовой связи или при дистанционном включении диктофона, а также для защиты от возможной утечки информации по каналу Bluetooth или Wi-Fi (рис. 5.46).



Рис. 4.46. Акустический сейф «Ларец-1»

Для защиты речевой информации владельца сотового телефона в изделие встроен генератор ультразвукового шумоподобного сигнала (УЗ), который предотвращает запись акустической информации через микрофон телефона, при этом все функции телефона работают в штатном режиме. Таким образом, изделие обеспечивает защиту акустической информации даже при удаленной дистанционной активации сотового телефона — «полицейский» режим (в т. ч. и от активной функции «диктофон»). При попытке установления связи с сотовым телефоном через канал Bluetooth или Wi-Fi автоматически включается генератор радиопомехи в диапазоне 2,4–2,5 ГГц (3дБм), блокирующий обмен данными между телефоном и другим устройством [27].

Акустический сейф «Ларец-УЗ»

Изделие предназначено для защиты от неправомерной записи или передачи речевой и цифровой информации, циркулирующей в помещении, через сотовый телефон, смартфон или планшет (рис. 5.47) [27].



Рис. 5.47. Акустический сейф «Ларец-УЗ»

Актуальность защиты речевой информации необходимостью защиты от утечки конфиденциальных сведений третьим лицам, могущей привести к катастрофическим последствиям.

Изделие обеспечивает подавление речевого сигнала с использованием ультразвукового шумогенератора, то есть обеспечивает защиту от утечки акустической информации через каналы сотовой связи 2G, 3G, 4G и одновременно блокирует передачу акустической информации по беспроводным каналам W-Fi и Bluetooth.

При работе изделия сам телефон находится «на связи», то есть поступают все входящие звонки и sms, а блокируется только микрофон сотового телефона.

Примечание 1. Изделие предназначено для защиты современных флагманских абонентских устройств сотовой связи (телефонов). Критерием работоспособности изделия является проверка записи речи в приложении «дик-

тофон» на телефоне. При этом на фонограмме должен присутствовать только белый шум, без признаков речи.

Конструкция изделия

Акустический сейф «Ларец-УЗ» выполнен в виде шкатулки из ценных пород дерева. Крышка шкатулки фиксируется замком. Для работы с изделием замок можно не закрывать, достаточно просто закрыть крышку.

Внутри шкатулки установлен деревянный ложемент с отсеком для размещения сотовых телефонов. В ложементе изделия можно разместить 2–3 телефона или 2 смартфона или 1 планшет (рис. 4.57). На правой планке ложемента установлена красная кнопка для включения изделия, а на левой — синяя кнопка для включения генератора радиопомехи и УФ-излучателя расположены на боковой поверхности (левой и правой) планки ложемента. На тыловой части шкатулки расположен внешний разъем для подключения зарядного устройства [27].

Чехол-сейф для мобильного телефона – подавитель GSM, CDMA, GPS сигналов «Фарадей»

«Фарадей» (рис. 4.58) предназначен для защиты от утечки информации по каналам радиосвязи путем блокирования самого сигнала. Блокирует каналы передачи данных местонахождения телефона. При нахождении телефона в чехле происходит постоянная блокировка GSM, CDMA, GPS сигналов [27].



Рис. 4.58. «Фарадей»

При размещении мобильного телефона в чехле и закрытой крышке происходит полная потеря сигнала сотовой и спутниковой связи. Соответственно, лица, заинтересованные в негласном съеме информации на телефоне и слежении, не смогут получить данные с мобильного устройства или удаленно к нему подключиться, так как канал радиосвязи, по которому может быть утечка информации, будет недоступен.

После того извлечения как мобильного устройства из чехла оно автоматически возвращается в исходный режим передачи данных с оператором сотовой связи.

Вопросы и задания для самоконтроля

1. Пассивные средства защиты информации от утечки по акустическому каналу.
2. Активные средства защиты информации от утечки по акустическому каналу.
3. Организационные меры защиты информации от утечки по акустическому каналу.
4. Организационно-технические меры защиты информации от утечки по акустическому каналу.
5. Защита информации от утечки по акустическому каналу.
6. Средства защиты информации от несанкционированного доступа.
7. Средства защиты от утечек по акустическим каналам информации.

Глава 6

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

6.1. Методика оценки угроз безопасности информации¹

1. Общие положения

1.1. Настоящая Методика оценки угроз безопасности информации (далее — Методика) разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее — системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

1.3. Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

В иных случаях решение о применении настоящей Методики принимается обладателями информации или операторами систем и сетей.

1.4. В документе не рассматриваются методические подходы по оценке угроз безопасности информации, связанных с нарушением

¹ Сайт информационно-правового портала «Гарант.ру». URL: <https://www.garant.ru/products/ipo/prime/doc/400325044/> (датаобращения: 12.02.2024).

безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

1.5. Методика ориентирована на оценку антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей.

1.6. На основе настоящей Методики могут разрабатываться отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации, которые учитывают особенности функционирования систем и сетей в соответствующей области деятельности. Разрабатываемые отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации не должны противоречить положениям настоящей Методики.

1.7. В Методике используются термины и определения, приведенные в приложении 1 к настоящей Методике, а также термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области защиты информации и обеспечения информационной безопасности.

1.8. Положения настоящей Методики применяются для оценки угроз безопасности информации в системах и сетях, решение о создании или модернизации (развитии) которых принято после даты ее утверждения, а также в эксплуатируемых системах и сетях.

Модели угроз безопасности информации систем и сетей, разработанные и утвержденные до утверждения настоящей Методики, продолжают действовать и подлежат изменению в соответствии с настоящей Методикой при развитии (модернизации) соответствующих систем и сетей.

В связи с утверждением настоящего методического документа не применяются для оценки угроз безопасности информации Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.) и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007 г.).

2. Порядок оценки угроз безопасности информации

2.1. Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях функционирования — актуальных угроз безопасности информации.

2.2. Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

г) оценка способов реализации (возникновения) угроз безопасности информации;

д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

е) оценка сценариев реализации угроз безопасности информации в системах и сетях.

2.3. Исходными данными для оценки угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного указом Президента Российской Федерации от 16 августа 2004 г. №1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) документация на системы и сети (а именно: техническое задание на создание систем и сетей, частное техническое задание на создание системы защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на системы и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

д) нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

е) технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее — основные (критические) процессы);

ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют системы и сети.

2.4. Оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) систем и сетей. Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем и сетей. Учет изменений угроз безопасности информации обеспечит своевременную выработку адекватных и эффективных мер по защите информации (обеспечению безопасности) в системах и сетях.

2.5. На этапе создания систем и сетей оценка угроз безопасности информации проводится на основе их предполагаемых архитектуры и условий функционирования, определенных по результатам изучения и анализа исходных данных на них. В ходе эксплуатации систем и сетей, в том числе при развитии (модернизации) систем и сетей, оценка угроз безопасности информации проводится для реальной архитектуры систем и сетей и условий их функционирования, полученных по результатам анализа исходных данных, инвентаризации информацион-

ных ресурсов, анализа уязвимостей и (или) тестирования на проникновение систем и сетей, а также иных методов исследований уровня защищенности систем и сетей и содержащейся в них информации.

2.6. По результатам оценки, проведенной в соответствии с настоящей Методикой, должны быть выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей.

На этапе создания систем и сетей результаты оценки угроз безопасности информации должны быть направлены на обоснование выбора организационных и технических мер по защите информации (обеспечению безопасности), а также на выбор средств защиты информации и их функциональных возможностей.

На этапе эксплуатации систем и сетей результаты оценки угроз безопасности информации должны быть направлены на оценку эффективности принятых технических мер, в том числе используемых средств защиты информации.

2.7. Оценка угроз безопасности информации проводится подразделением по защите информации (отдельными специалистами, назначенными ответственными за обеспечение защиты информации (обеспечение безопасности)) обладателя информации или оператора с участием подразделений или специалистов, ответственных за эксплуатацию систем и сетей (IT-специалистов, специалистов автоматизированных систем управления, специалистов связи и др.), основных (профильных) подразделений обладателя информации или оператора. Для оценки угроз безопасности информации по решению обладателя информации или оператора в соответствии с законодательством Российской Федерации могут привлекаться специалисты сторонних организаций.

Для оценки угроз безопасности информации рекомендуется привлекать специалистов, обладающих следующими знаниями и умениями:

а) основ оценки рисков, а также основных рисков от нарушения функционирования систем и сетей и нарушения безопасности обрабатываемой информации (далее — информационные риски);

б) угроз безопасности информации и способов их реализации (возникновения);

в) тактик и техник проведения компьютерных атак (реализации угроз безопасности информации);

г) основных типов компьютерных инцидентов и причин их возникновения;

д) основных уязвимостей систем и сетей;

е) нормативных правовых актов по созданию и функционированию систем и сетей, защите информации (обеспечению безопасности) в них, основных (критических) процессов (бизнес-процессов) обладателя информации и (или) оператора;

ж) оценивать информационные риски;

з) классифицировать и оценивать угрозы безопасности информации;

и) определять сценарии (тактики, техники) реализации угроз безопасности информации;

к) определять источники и причины возникновения компьютерных инцидентов;

л) проводить инвентаризацию систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств;

м) оценку уровня защищенности (аудит) систем и сетей и содержащейся в них информации.

2.8. Оценка угроз безопасности информации проводится с использованием экспертного метода. В интересах снижения субъективных факторов при оценке угроз безопасности информации рекомендуется создавать экспертную группу. Рекомендации по формированию экспертной группы и проведению экспертной оценки угроз безопасности информации приведены в приложении 2 к настоящей Методике.

2.9. При оценке угроз безопасности информации могут использоваться программные средства, позволяющие автоматизировать данную деятельность.

Для получения (уточнения) отдельных исходных данных (например, объектов воздействия и их интерфейсов, уязвимостей) в интересах оценки угроз безопасности информации на этапе эксплуатации систем и сетей применяются автоматизированные средства инвентаризации систем и сетей, анализа уязвимостей, тестирования на проникновение систем и сетей, а также иные средства, используемые для исследований уровня защищенности систем и сетей и содержащейся в них информации.

2.10. В случае оценки угроз безопасности информации для систем и сетей, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, угрозы безопасности информации определяются как для са-

мих систем и сетей, так и для информационно-телекоммуникационной инфраструктуры, на которой они функционируют (рис. 6.1).

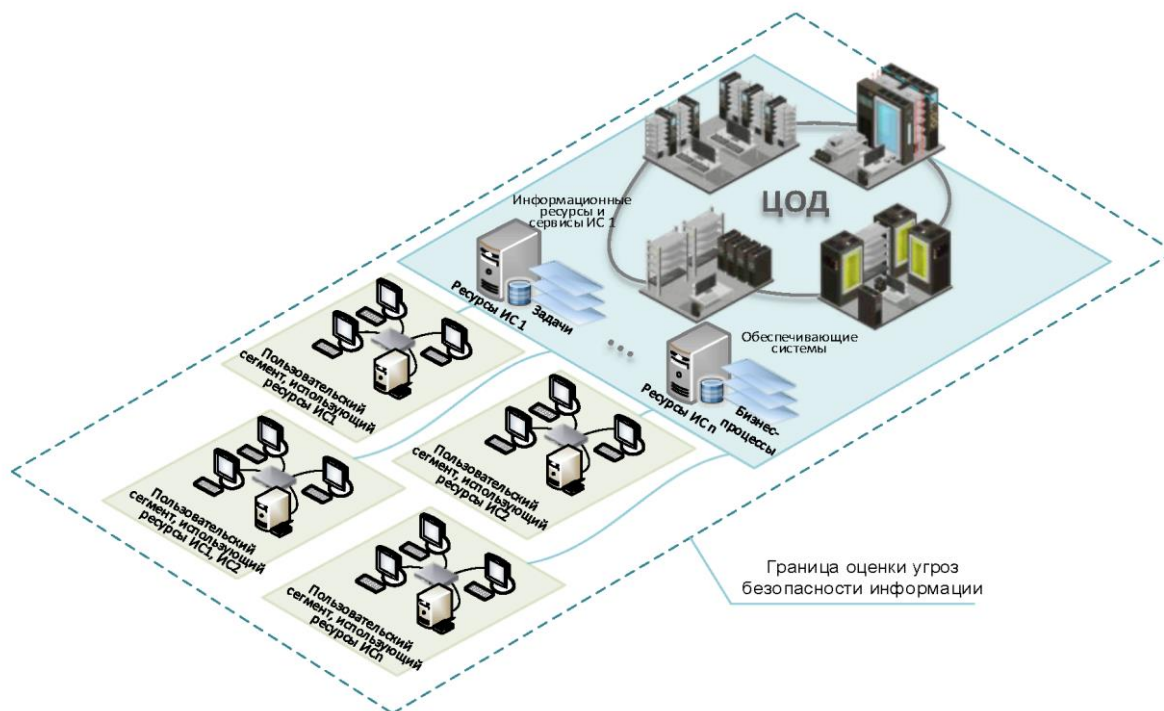


Рис. 6.1. Оценка угроз безопасности информации в информационной инфраструктуре на базе центра обработки данных

2.11. При размещении систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, принадлежащей поставщику услуг, оценка угроз безопасности информации проводится оператором во взаимодействии с поставщиком услуг.

В случае размещения систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, для которой поставщик услуг не оценил угрозы безопасности информации или не представил результаты такой оценки, оператор при оценке угроз безопасности информации исходит из предположения, что информационно-телекоммуникационная инфраструктура центра обработки данных или облачная инфраструктура, являющаяся средой функционирования для его систем и сетей, подвержена угрозам безопасности информации (скомпрометирована нарушителем с максимальным уровнем возможностей).

2.12. Результаты оценки угроз безопасности информации отражаются в модели угроз, которая представляет собой описание систем и сетей и актуальных угроз безопасности информации. Рекомендуемая

структура модели угроз безопасности информации приведена в приложении 3 к настоящей Методике.

2.13. По решению обладателя информации или оператора модель угроз безопасности информации разрабатывается как для отдельной системы или сети, так и для совокупности взаимодействующих систем и сетей оператора. При разработке модели угроз безопасности информации для отдельной системы и сети, она должна содержать описание угроз безопасности информации, актуальных для информационно-телекоммуникационной инфраструктуры, на базе которой эта система или сеть функционирует, а также угроз безопасности информации, связанных с интерфейсами взаимодействия со смежными (взаимодействующими) системами и сетями.

Допускается разработка одной модели угроз безопасности информации для нескольких однотипных создаваемых систем и сетей обладателя информации или оператора.

2.14. Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.

Ведение модели угроз безопасности информации и поддержание ее в актуальном состоянии может осуществляться в электронном виде с учетом приложения 3 к настоящей Методике.

Изменение модели угроз безопасности информации осуществляется в случаях:

а) изменения требований нормативных правовых актов Российской Федерации, методических документов ФСТЭК России, регламентирующих вопросы оценки угроз безопасности информации;

б) изменений архитектуры и условий функционирования систем и сетей, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;

в) выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;

г) включения в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

2.15. Оценка угроз безопасности информации включает следующие этапы:

- 1) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- 2) определение возможных объектов воздействия угроз безопасности информации;
- 3) оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

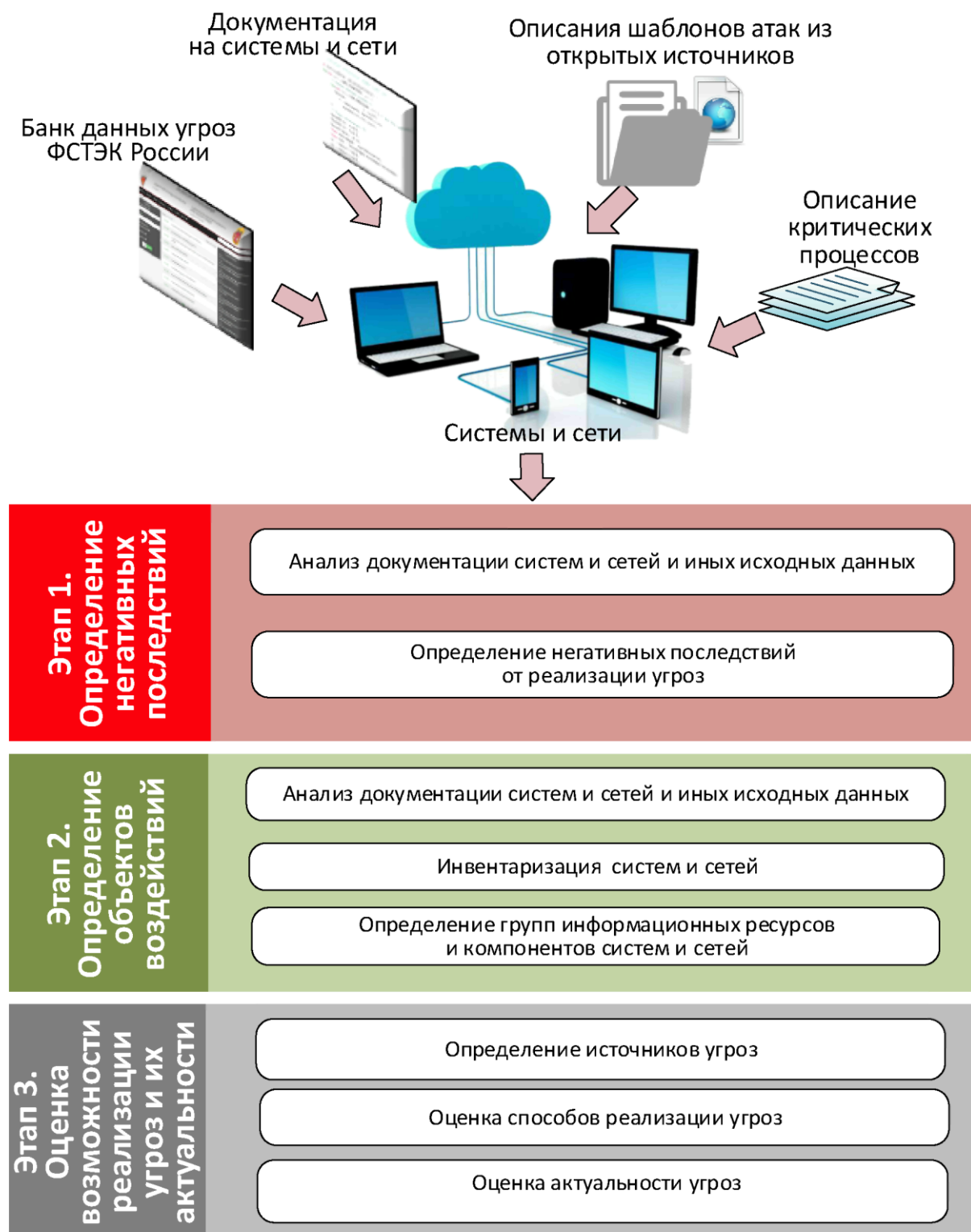


Рис. 6.2. Общая схема проведения оценки угроз безопасности информации

3. Определение негативных последствий от реализации (возникновения) угроз безопасности информации

3.1. В ходе оценки угроз безопасности информации должны быть определены негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

3.2. Исходными данными для определения негативных последствий от реализации угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

в) документация на сети и системы (в части сведений о назначении и функциях систем и сетей, о составе и архитектуре систем и сетей);

г) технологические, производственные карты или иные документы, содержащие описание основных (критических) процессов (бизнес-процессов) обладателя информации, оператора;

д) результаты оценки рисков (ущерба), проведенной обладателем информации или оператором.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

3.3. На основе анализа исходных данных определяются событие или группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести:

а) к нарушению прав граждан;

б) возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства;

в) возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора.

Событие или группа событий определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивают системы и сети, и применительно к нарушению безопасности информации, содержащейся в системах исетях.

3.4. В случае отсутствия у обладателя информации или оператора результатов оценки рисков (ущерба), возможные негативные последствия от реализации угроз безопасности информации могут определяться как на основе экспертной оценки специалистов, проводящих оценку угроз безопасности информации, так и на основе информации, представляемой профильными подразделениями или специалистами обладателя информации или оператора.

3.5. Определяемые в ходе оценки угроз безопасности информации негативные последствия должны быть конкретизированы применительно к областям и особенностям деятельности обладателя информации или оператора. Для систем и сетей обладателя информации или оператора может быть определено одно или несколько негативных последствий.

Пример 1: 1) если оператор обрабатывает персональные данные граждан, которые в соответствии с Федеральным законом «О персональных данных» подлежат обязательной защите, одним из возможных негативных последствий от реализации угроз безопасности информации является нарушение конфиденциальности персональных данных, в результате которого будут нарушены права субъектов персональных данных и соответствующие законодательные акты; 2) если оператор обеспечивает транспортировку нефти, одним из возможных негативных последствий от реализации угроз безопасности информации является разлив нефти из нефтепровода, повлекший наступление экологического ущерба; 3) если оператор предоставляет услуги связи, одним из возможных негативных последствий от реализации угроз безопасности информации является непредоставление услуг связи абонентам, повлекшее наступление ущерба в социальной сфере; 4) для оператора по переводу денежных средств одним из возможных негативных последствий от реализации угроз безопасности информации является хищение денежных средств, в результате которого возможны финансовые и репутационные риски.

Виды рисков (ущербов) и типовые негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации, приведены в приложении 4 к настоящей Методике.

4. Определение возможных объектов воздействия угроз безопасности информации

4.1. В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям — объекты воздействия.

Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации

4.2. Исходными данными для определения возможных объектов воздействия являются:

а) общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

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

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

д) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

4.3. На основе анализа исходных данных и результатов инвентаризации систем и сетей определяются следующие группы информацион-

ных ресурсов и компонентов систем и сетей, которые могут являться объектами воздействия:

а) информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.);

б) программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства));

в) программные средства (в том числе системное и прикладное программное обеспечение, включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации);

г) машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;

д) телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);

е) средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);

ж) привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;

з) обеспечивающие системы.

Пример 2 : К основным информационным ресурсам и компонентам систем и сетей могут относиться системы хранения данных (базы данных), системы управления базами данных, веб-сайт, почтовый сервер, почтовый клиент, автоматизированное рабочее место пользователя, система управления и администрирования, контроллер домена, сетевые службы, проводные и беспроводные каналы передачи данных, телекоммуникационное оборудование и т. д.

4.4. На этапе создания систем и сетей объекты воздействия определяются на основе предполагаемых архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных. В ходе эксплуатации систем и сетей, в том числе при развитии (модернизации) систем и сетей, объекты воздействия определяются для реальных архитектуры и условий функционирования систем и сетей, полученных по результатам анализа исходных данных и инвентаризации систем и сетей.

Инвентаризация систем и сетей проводится с использованием автоматизированных средств, которые позволяют определить компоненты систем и сетей, а также внешние и внутренние интерфейсы.

4.5. Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям. Основными видами таких воздействий являются:

- а) утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
- б) несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
- в) отказ в обслуживании компонентов (нарушение доступности);
- г) несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
- д) несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
- е) нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

4.6. Объекты воздействия определяются на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей (рис. 6.3).

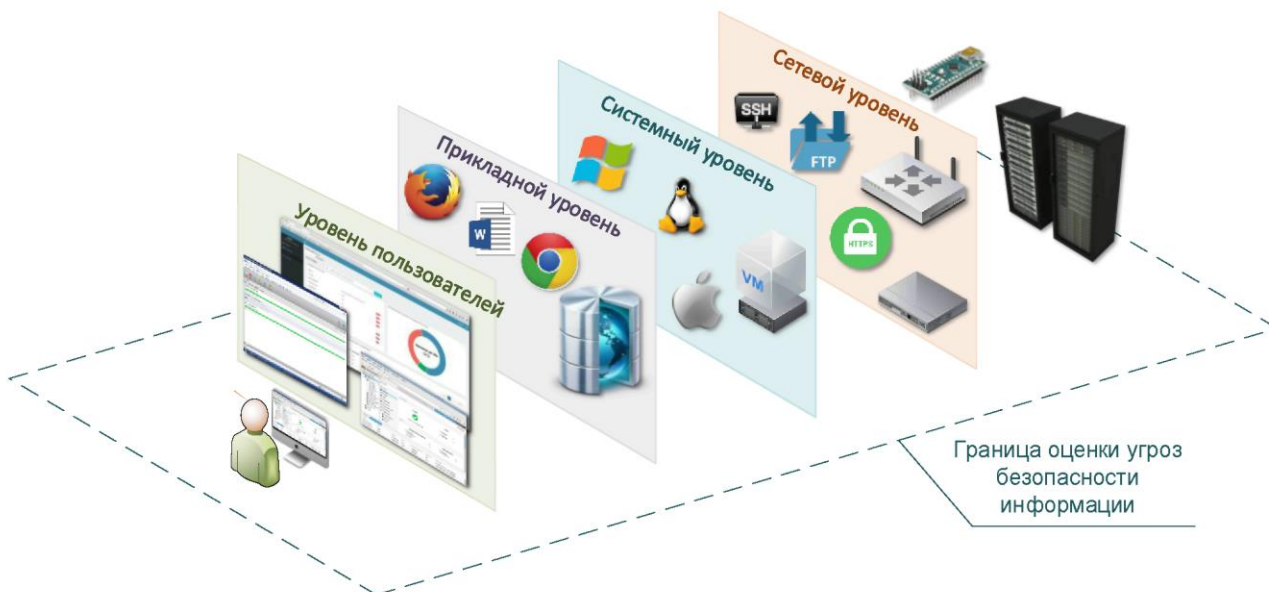


Рис. 6.3. Уровни архитектуры систем и сетей, на которых определяются объекты взаимодействия

4.7. В процессе эксплуатации систем и сетей объекты воздействия и виды воздействия на них могут дополняться и изменяться относительно их состава и видов воздействия, определенных на этапе создания данных систем и сетей. В этом случае учет изменений должен проводиться в рам-

ках реализации мероприятий по управлению конфигурацией систем и сетей и анализу угроз безопасности информации в ходе их эксплуатации.

4.8. При оценке угроз безопасности информации в системах и сетях, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, объекты воздействия определяются с учетом состава и содержания услуг, предоставляемых поставщиком услуг (например, инфраструктура как услуга, платформа как сервис, программное обеспечение как сервис).

Арендуемые или используемые на ином законном основании программно-аппаратные средства и их интерфейсы, каналы связи, программное обеспечение (в том числе программное обеспечение виртуализации и построенных на его базе виртуальных машин, виртуальных серверов, систем управления виртуализацией, виртуальных каналов связи и т. д.) относятся к объектам воздействия, находящимся в границе оценки угроз безопасности информации оператора. В отношении остальной информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры угрозы безопасности информации оцениваются поставщиком услуг.

Пример распределения границ при оценке угроз безопасности информации между оператором и поставщиком услуг представлен на рис. 6.4.



Рис. 6.4. Пример распределения границ при оценке угроз безопасности информации между оператором и поставщиком услуг

4.9. Объекты воздействия и виды воздействия на них должны быть конкретизированы применительно к архитектуре и условиям функционирования систем и сетей, а также областям и особенностям деятельности обладателя информации и оператора.

Пр и м е р 3 : 1) разглашение персональных данных и (или) их модификация возможны в результате несанкционированного доступа к базе данных, в которой эта информация хранится; 2) разлив нефти из нефтепровода возможен в результате несанкционированного доступа к программируемому логическому контроллеру, обеспечивающему управление задвижками нефтепровода, и подмены хранящихся в нем значений уставок; 3) непредоставление услуг связи абонентам возможно в результате отказа в обслуживании маршрутизатора уровня ядра сети; 4) нарушение электроснабжения потребителей возможно в результате несанкционированного доступа к программируемому логическому контроллеру, управляющему выключателем, с целью подачи ложных команд на его отключение; 5) хищение денежных средств у оператора по переводу денежных средств возможно в результате подмены (модификации) информации, содержащейся в электронных сообщениях.

Примеры определения объектов воздействия и видов воздействия на них приведены в приложении 5 к настоящей Методике.

5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

5.1 Определение источников угроз безопасности информации

5.1.1. В ходе оценки угроз безопасности информации должны быть определены возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей, — актуальные нарушители.

5.1.2. Исходными данными для определения возможных актуальных нарушителей являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) нормативные правовые акты Российской Федерации, в соответствии с которыми создается и функционирует система или сеть, содержащие описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

г) документация на сети и системы (в части сведений о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах);

д) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в части персонала поставщика услуг, имеющего доступ к этой инфраструктуре, его прав и обязанностей, уровня полномочий и типов доступа);

е) результаты оценки ущерба (рисков), проведенной обладателем информации или оператором;

ж) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

з) объекты воздействия угроз безопасности информации и виды воздействия на них, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

5.1.3. На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей.

Основными видами нарушителей, подлежащих оценке, являются:

- специальные службы иностранных государств;
- террористические, экстремистские группировки;
- преступные группы (криминальные структуры);
- отдельные физические лица (хакеры);
- конкурирующие организации;
- разработчики программных, программно-аппаратных средств;

лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;

поставщики услуг связи, вычислительных услуг;

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

лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);

авторизованные пользователи систем и сетей;

системные администраторы и администраторы безопасности;

бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционируют системы и сети. Для одной системы и сети актуальными могут являться нарушители нескольких видов.

5.1.4. Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба). Возможные цели реализации угроз безопасности информации нарушителями приведены в приложении 6 к настоящей Методике.

Пример соответствия нарушителей, возможных целей реализации ими угроз безопасности информации и возможных негативных последствий и видов рисков (ущерба) от их реализации (возникновения) приведен в приложении 7 к настоящей Методике.

5.1.5. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

базовыми возможностями по реализации угроз безопасности информации (Н1);

базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);

средними возможностями по реализации угроз безопасности информации (Н3);

высокими возможностями по реализации угроз безопасности информации (Н4).

Для одной системы или сети актуальными могут являться нарушители, имеющие разные уровни возможностей.

Уровни возможностей нарушителей по реализации угроз безопасности информации приведены в приложении 8 к настоящей Методике.

5.1.6. Для актуальных нарушителей должны быть определены их категории в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования этих систем и сетей, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории (рис. 6.5):

внешние нарушители — нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;

внутренние нарушители — нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

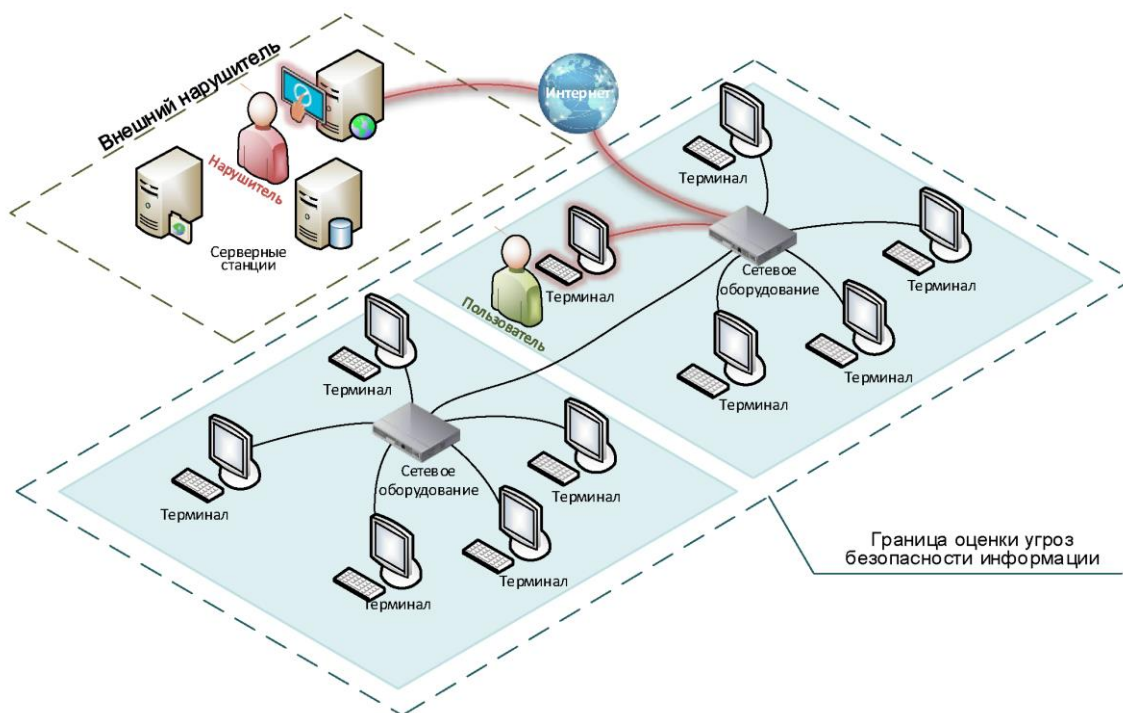


Рис. 6.5. Внешний нарушитель при реализации угроз безопасности информации

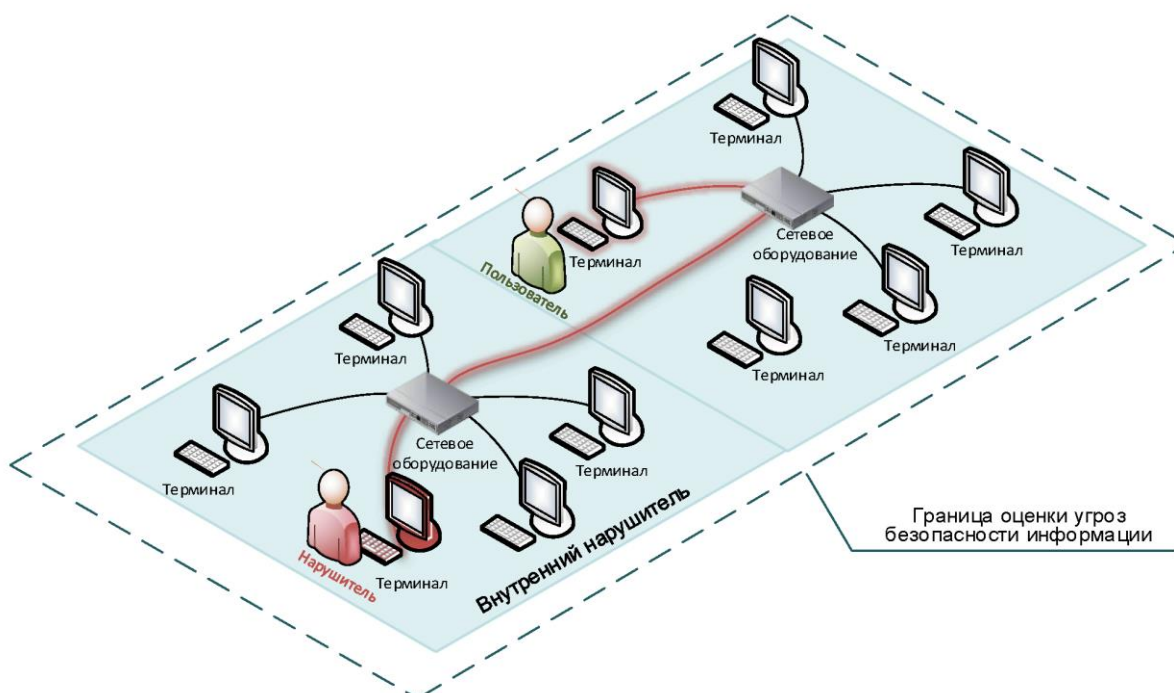


Рис. 6.6. Внутренний нарушитель при реализации угроз безопасности информации

Внутренние нарушители первоначально могут иметь разный уровень прав доступа к информационным ресурсам и компонентам систем и сетей (например, доступ в личный кабинет на сайте, исполнение обязанностей на автоматизированном рабочем месте, администрирование систем и сетей). К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам систем и сетей.

5.1.7. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

Пример 4: к непреднамеренным угрозам безопасности информации могут относиться: 1) нарушение функционирования системы управления базы данных за счет ввода в поля данных информации, превышающей допустимый объем; 2) нарушение функционирования веб-ресурса за счет того, что системный администратор допустил ошибку при выборе конфигурационного файла веб-сервера.

5.1.8. В случае если к системам и сетям предъявлены требования к устойчивости и надежности функционирования (в части целостности и доступности информационных ресурсов и компонентов систем и сетей), дополнительно к антропогенным источникам угроз безопасности информации в качестве актуальных могут быть определены техногенные источники (физические явления, материальные объекты). Угрозы безопасности информации, связанные с техногенными источниками, включаются в модель угроз безопасности информации по решению обладателя информации или оператора систем и сетей.

Основными факторами возникновения угроз безопасности информации, связанными с техногенными источниками, могут являться:

а) недостатки качества, надежности программного обеспечения, программно-аппаратных средств, обеспечивающих обработку и хранение информации, их линий связи;

б) недостатки в работе обеспечивающих систем;

в) недоступность сервисов (услуг), предоставляемых сторонними организациями.

Возможность возникновения таких угроз определяется на основе статистики их возникновения за прошлые годы. В случае отсутствия указанной статистики возможно использование экспертной оценки.

Выявление техногенных источников должно осуществляться с учетом требований и правил, установленных уполномоченными федеральными органами исполнительной власти, национальными стандартами.

5.1.9. По результатам определения источников угроз безопасности информации должны быть определены:

а) виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;

б) категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

При определении источников угроз безопасности информации необходимо исходить из предположения о наличии повышенной мотивации внешних и внутренних нарушителей, преднамеренно реализующих угрозы безопасности информации. Кроме того, необходимо учитывать, что такие виды нарушителей как специальные службы иностранных государств и террористические, экстремистские группировки могут привлекать (входить в сговор) внутренних нарушите-

лей, в том числе обладающих привилегированными правами доступа. В этом случае уровень возможностей актуальных нарушителей будет определяться совокупностью возможностей нарушителей, входящих в сговор.

Примеры определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведены в приложении 9 к настоящей Методике.

5.2 Оценка способов реализации (возникновения) угроз безопасности информации

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

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

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

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

г) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

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

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

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

5.2.3. На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для систем и сетей.

Основными способами реализации (возникновения) угроз безопасности информации являются:

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

2) внедрение вредоносного программного обеспечения;

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

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

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

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

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

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

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

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

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия, определенным в соответствии с настоящей Методикой. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

5.2.4. Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

- внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

- внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);

- интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

- интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;

- интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;

- возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования систем и сетей, группами пользователей, их типами доступа и уровнями полномочий. В ходе анализа должны быть определены как логические, так и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

Интерфейсы определяются на аппаратном, системном и прикладном уровнях систем и сетей, а также для телекоммуникационно-

го оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

5.2.5. На этапе создания систем и сетей определение интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, проводится на основе предполагаемой архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных о них.

На этапе эксплуатации систем и сетей для определения интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, дополнительно к документации на сети и системы используются результаты инвентаризации систем и сетей, проведенной с использованием автоматизированных средств.

5.2.6. По результатам оценки возможных способов реализации угроз безопасности информации должны быть определены:

а) виды и категории нарушителей, которые имеют возможность использования актуальных способов;

б) актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

Примеры определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведены в приложении 10 к настоящей Методике.

5.3 Оценка актуальности угроз безопасности информации

5.3.1. В ходе оценки угроз безопасности информации должны быть определены возможные угрозы безопасности информации и оценена их актуальность для систем и сетей — актуальные угрозы безопасности информации.

5.3.2. Исходными данными для оценки актуальности угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей Методикой;

д) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей Методикой;

е) актуальные способы реализации (возникновения) угроз безопасности информации.

5.3.3. На основе анализа исходных данных определяются возможные для систем и сетей угрозы безопасности информации, к которым относятся осуществляемые нарушителем воздействия на информационные ресурсы и компоненты систем и сетей (объекты воздействия), в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям:

$УБИ_i = [\text{нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия}]$.

5.3.4. Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

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

терфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик (тактических задач) и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, приведен в приложении 11 к настоящей Методике.

5.3.5. На этапе создания систем и сетей должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации (рис. 6.7).

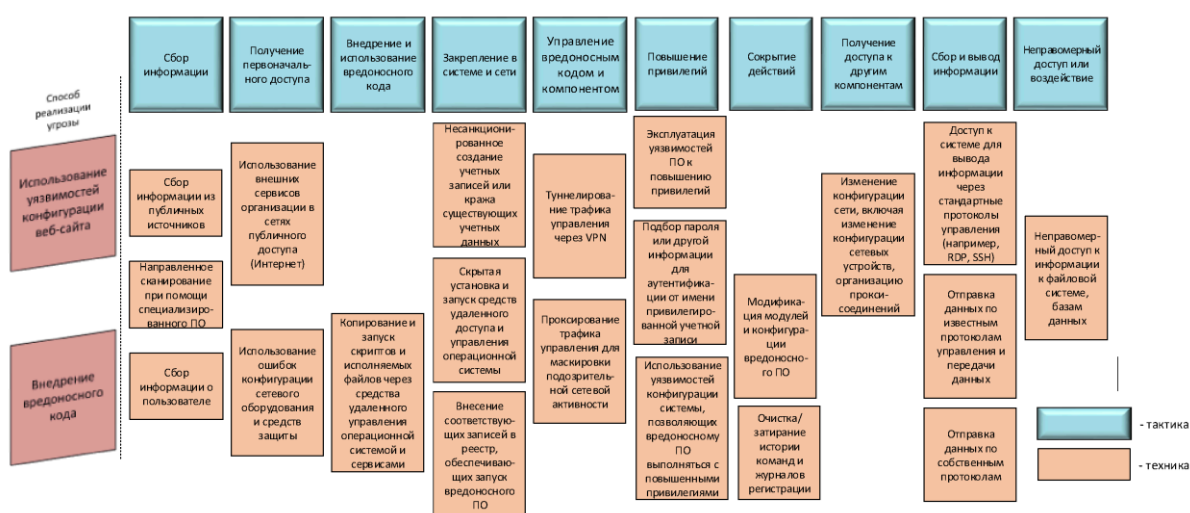


Рис. 6.7. Пример сценария реализации угрозы безопасности информации

На этапе эксплуатации систем и сетей для каждой возможной угрозы безопасности информации определяется множество возможных сценариев ее реализации в интересах оценки эффективности принятых технических мер по защите информации (обеспечению безопасности), в том числе средств защиты информации. При этом множество сценариев определяется для каждого актуального нарушителя и уровней его возможностей в соответствии с полученными результатами инвентаризации систем и сетей, анализа уязвимостей и (или) тестирования на проникновение, проведенных с использованием автоматизированных средств (рис. 6.8).

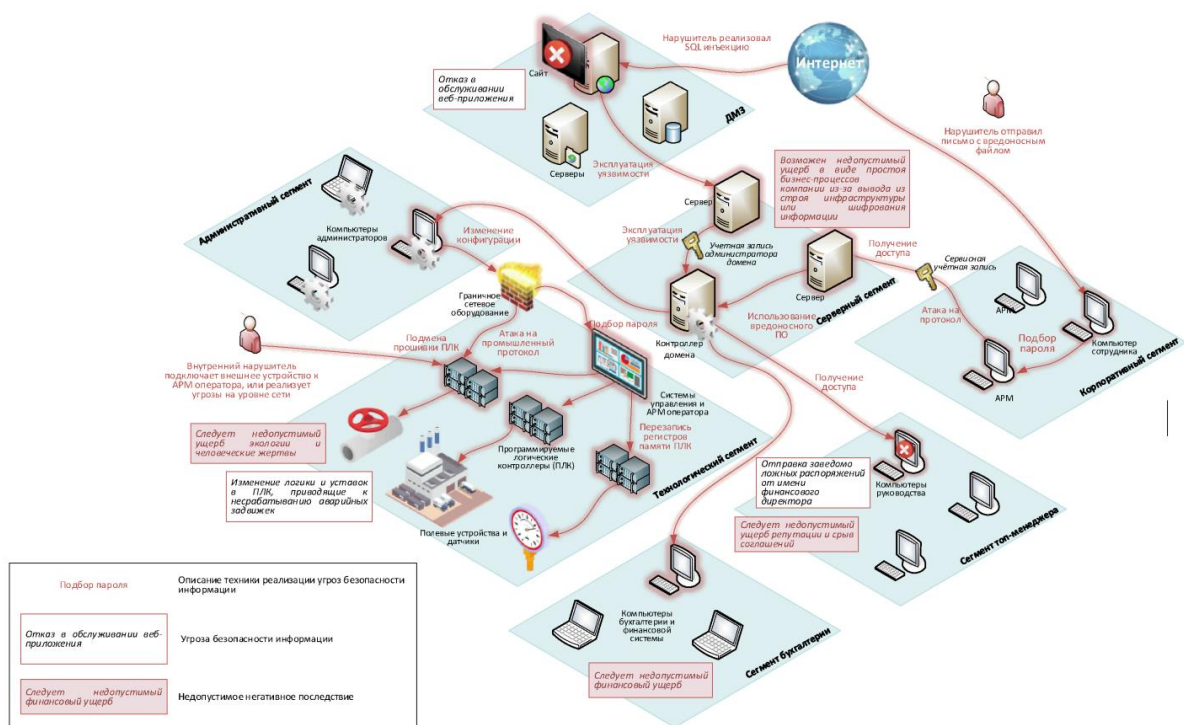


Рис. 6.8. Пример сценария реализации угроз безопасности информации

5.3.6. На этапе эксплуатации определение сценариев реализации угрозы включает:

- а) анализ исходных данных на систему или сеть, предусматривающий в том числе анализ документации, модели угроз безопасности информации, применяемых средств защиты информации, и определение планируемых к применению автоматизированных средств;
- б) проведение инвентаризации информационных систем и сетей и определение объектов воздействия и их интерфейсов;
- в) определение внешних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;
- г) определение внутренних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;
- д) выявление уязвимостей объектов воздействия, а также компонентов систем и сетей, имеющих внешние интерфейсы, с которыми посредством внутренних интерфейсов взаимодействуют объекты воздействия;
- е) проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности информации;
- ж) поиск последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации, исходя из уровня возможностей актуальных нарушителей, а также ре-

зультатов инвентаризации, анализа уязвимостей и тестирования на проникновение;

з) составление сценариев реализации угрозы безопасности информации применительно к объектам и видам воздействия, а также способам реализации угроз безопасности информации.

6.2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

1. Термины и определения¹

В настоящем документе используются следующие термины и их определения:

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных — подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных — состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия

¹ Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (*Выпуска*) (утв. ФСТЭК России 15.02.2008).

на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы — технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) — получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т. п.), исполняемых файлов прикладных программ.

Доступ к информации — возможность получения информации и ее использования.

Закладочное устройство — элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал — электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации — субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона — пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных — физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности — функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических ре-

шений и процессов, количественных характеристик физических величин.

Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки — электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка — скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие — несанкционированное воздействие на ресурсы автоматизированной

информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы — именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации.

Технический канал утечки информации — совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость — некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения

Настоящая «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (далее — модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн), связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для государственных и муниципальных органов, юридических и(или) физических лиц (далее — операторов), организующих и (или) осуществляющих обработку ПДн, а также определяющих цели и содержание обработки ПДн, заказчиков и разработчиков ИСПДн и их подсистем. С применением модели угроз решаются следующие задачи:

- разработка частных моделей угроз безопасности ПДн конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

контроль обеспечения уровня защищенности персональных данных.

В Модели угроз дано обобщенное описание ИСПДн как объектов защиты, возможных источников угрозы безопасности персональных данных (УБПДн), основных классов уязвимостей ИСПДн, возможных видов деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов иссредств реализации УБПДн в ИСПДн. Внесение изменений в модель угроз осуществляется ФСТЭК России в устанавливаемом порядке.

3. Классификация угроз безопасности персональных данных

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее – технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т. п.);

средства защиты информации;

вспомогательные технические средства и системы (ВТСС) — технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее — служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

источник УБПДн — субъект, материальный объект или физическое явление, создающие УБПДн;

среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

носитель ПДн — физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носители ПДн могут содержать информацию, представленную в следующих видах:

акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками:

по виду защищаемой от УБПДн информации, содержащей ПДн;
по видам возможных источников УБПДн;

по типу ИСПДн, на которые направлена реализация УБПДн;
по способу реализации УБПДн;
по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
по используемой уязвимости;
по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПДн по техническим каналам утечки информации;

- угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного ПО;

- угрозы, реализуемые с использованием уязвимости прикладного ПО;

- угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;

- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

- угрозы, реализуемые с использованием уязвимостей, обуславливающих наличие технических каналов утечки информации;

- угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;

- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, выне-

сенных мониторах, видеопроекторах, средствах звуковоспроизведения и т. п.);

угрозы безопасности ПДн, передаваемых по сетям связи;

угрозы прикладным программам, с помощью которых обрабатываются ПДн;

угрозы системному ПО, обеспечивающему функционирование ИСПДн.

Классификация угроз безопасности персональных данных по виду защищаемой от УБПДн информации, содержащей ПДн

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПДн:

значительным негативным последствиям для субъектов ПДн;

негативным последствиям для субъектов ПДн;

незначительным негативным последствиям для субъектов ПДн.

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД) (далее — угрозы НСД в ИСПДн), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

угроза НСД: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

4. Угрозы утечки информации по техническим каналам

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществ-

ляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

Среда распространения информативного сигнала — это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн:

- угроз утечки акустической (речевой) информации;
- угроз утечки видовой информации;
- угроз утечки информации по каналам побочных электромагнитных излучений и наводок.

4.1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Перехват акустической (речевой) информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки ПДн, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема

речевой информации, внедренных в технические средства обработки ПДн, ВТСС и помещения или подключенных к каналам связи.

Угрозы безопасности ПДн, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации («закладочных устройств»), определяются в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Перехват акустической (речевой) информации может вестись: стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц; портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

портативной носимой аппаратурой — физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;

автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

4.2. Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Угрозы безопасности ПДн, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видеозаказов), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Перехват ПДн может вестись:

стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

портативной носимой аппаратурой — физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

Перехват (просмотр) ПДн может осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов ИСПДн с использованием оптических (оптикоэлектронных) средств.

4.3. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Возникновение угрозы ПДн по каналам побочных электромагнитных излучений и наводок возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Регистрация побочных электромагнитных излучений и наводок осуществляется с целью перехвата информации, циркулирующей в технических средствах, обрабатывающих ПДн (в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, в том числе в средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео- и буквенно-цифровой информации).

Для регистрации побочных электромагнитных излучений и наводок используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Кроме этого, перехват побочных электромагнитных излучений и наводок возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн.

Регистрация побочных электромагнитных излучений и наводок может вестись с использованием аппаратуры следующих видов:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

- портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

- портативной носимой аппаратурой — физическими лицами в непосредственной близости от ИСПДн;

- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПДн.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений технических средств ИСПДн возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информативный сигнал.

Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств ИСПДн и цепей питания.

Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе аппаратуры ТСПи и цепей заземления.

Для съема информации с проводных линий могут использоваться:

средства съема сигналов, содержащих защищаемую информацию, с цепей технических средств ИСПДн и ВТСС, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты сети, токовые трансформаторы, пробники);

средства съема наведенных информативных сигналов с цепей электропитания;

средства съема наведенных информативных сигналов с шин заземления;

средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций.

Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна.

Появление новых каналов связи — сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных - привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:

перехвата пейджинговых сообщений и сотовой связи;

перехвата информации в каналах передачи данных вычислительных сетей.

5. Угрозы несанкционированного доступа к информации в информационной системе персональных данных

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т. п.;

угрозы внедрения вредоносных программ (программно-математического воздействия).

Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Эти угрозы реализуются относительно ИСПДн как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПДн, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств - это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к ИСПДн на базе локальных и распределенных информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

содержания служебной информации в пакетах сообщений, передаваемых по сети;

условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);

форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);

программного обеспечения обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др. Описание таких угроз формально может быть представлено следующим образом:

угроза «Отказа в обслуживании»: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (носитель ПДн)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т. п.)>.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что, во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации защиты информации на практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования). В связи с этим угрозы программно-математического воздействия (ПМВ) формально могут быть представлены следующим образом:

угроза ПМВ в ИСПДн: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т. п.)>, <описание возможных деструктивных действий>, <дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

Ниже дается общая характеристика источников угроз безопасности информации, уязвимостей, которые могут быть использованы при реализации угроз НСД, и характеристика результатов несанкционированного или случайного доступа. Характеристика способов реализации угроз дается при описании угроз доступа (проникновения) в операционную среду компьютера, угроз отказа в обслуживании и угроз ПМВ.

6. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных

В зависимости от целей и содержания обработки ПДн оператор может осуществлять обработку ПДн в ИСПДн различных типов.

По структуре информационные системы подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации УБПДн и наступления последствий в результате несанкционированного или случайного доступа можно выделить следующие типы ИСПДн:

автоматизированные рабочие места, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

локальные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

локальные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

распределенные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Применительно к основным типам ИСПДн составляются типовые модели угроз безопасности ПДн, характеризующие наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации УБПДн.

Частные модели угроз безопасности ПДн применительно к конкретным ИСПДн составляются операторами, заказчиками и разработчиками ИСПДн на этапах их создания и (или) эксплуатации.

6.3. Типы изделий электромагнитного зашумления

Существует два типа изделий электромагнитного зашумления:

1. *Генераторы объемного электромагнитного зашумления.*

В качестве генератора объемного электромагнитного зашумления выступает генератор электромагнитного шума «Пульсар» (рис. 6.9).



Рис. 6.9. Генератор электромагнитного шума «Пульсар»

Генератор электромагнитного шума «Пульсар» предназначен для маскировки информативных побочных электромагнитных излучений и наводок средств вычислительной техники и используется для защиты информации ограниченного доступа, в том числе сведений, составляющих государственную тайну любой категории до грифа «Совершенно секретно» включительно [27].

Сигналы побочных электромагнитных излучений и наводок могут возникать при работе таких устройств вычислительной техники как монитор, клавиатура, системный блок (интерфейсы) и т. п. Данные сигналы могут содержать обрабатываемую информацию и их можно перехватить с помощью специальных технических средств.

Генераторы электромагнитного шума создают широкополосную шумовую электромагнитную помеху, которая не позволяет злоумышленникам выделить полезный сигнал.

Изделие относится к следующим типам средств активной защиты:

- к типу «А» — средства активной защиты информации от утечки за счет побочных электромагнитных излучений;
- типу «Б» — средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.

Тактико-технические характеристики генератора электромагнитного шума «Пульсар»:

- диапазон рабочих частот от 10 кГц до 3 ГГц;
- две съемные антенны;
- визуальная система индикации нормального режима работы и визуально-звуковой система индикации аварийного режима;
- защита регулятора уровня выходного шумового сигнала от несанкционированного изменения и возможность обнаружения несанкционированного доступа к нему;
- счетчик учета времени функционирования устройства;
- соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России) – по 2 классу защиты;
- возможность применения в выделенных помещениях до 2 категории включительно.

Генератор шума SEL SP-21 «Баррикада»

Генератор с регулируемым уровнем излучения SEL SP-21 «Баррикада» предназначен для маскировки и предупреждения перехвата информативных побочных электромагнитных излучений и наводок от средств вычислительной техники путём создания в широкой полосе частот активных маскирующих помех (типа «белый шум») (рис. 6.10).

Область использования — помещения, в которых расположены средства вычислительной техники с информацией от конфиденциальной до содержащей сведения, составляющие государственную тайну.



Рис.6.10. Генератор шума SEL SP-21 «Баррикада»

Установка и настройка генератора должны производиться при аттестации объектов информатизации по требованиям безопасности информации организацией, аккредитованной в Государственном реестре системы сертификации средств защиты информации ФСТЭК России.

Антенна дисконусная «SI-5002.1»

Антенна дисконусная «SI-5002.1» предназначена для преобразования энергии генератора шумовой помехи в электрические волны путем излучения (рис. 6.11).



Рис.6.11. Антенна дисконусная «SI-5002.1»

Антенна представляет собой излучатель с вертикальной поляризацией и горизонтальной круговой диаграммой направленности. Главное преимущество антенны заключается в большой ширине полосы рабочих частот.

Дисконусная антенна относится к антеннам с верхним питанием, снабжена концевой емкостью в виде диска и конусообразным внешним проводником. Антенна может использоваться и в качестве приемной антенны в составе комплекса радиоконтроля.

Передачу высокочастотной энергии от генератора шумовой помехи к антенне выполняет коаксиальный кабель.

Антенна предназначена для эксплуатации внутри помещения.

Передачу высокочастотной энергии от генератора шумовой помехи к антенне выполняет коаксиальный кабель.

Антенна предназначена для эксплуатации внутри помещения.

Ответвитель для ГШ-1000У «Дух-01»

Ответвитель предназначен для съема высокочастотного электрического сигнала с различных токопроводящих проводных коммуникаций, токопроводящих инженерных сооружений и ввод высокочастотного электрического сигнала в эти коммуникации и сооружения, далее объекты, в диапазоне частот 0,1–1800 МГц. [44]. Ответвитель накладывается на объект и закрепляется на нем накладкой. Его выход подключается через СР 50-73 ФВ к измерительному устройству или источнику сигнала в зависимости от того, используется он в качестве датчика или устройства ввода. При использовании ответвителя совместно с генератором шума ГШ-1000У, его можно располагать в удаленных точках защищаемого помещения. Спектральная плотность напряжения шума, формируемого ГШ-1000У, достаточно высока, чтобы потери около 10 дБ на частоте 1000 МГц в соединительном радиочастотном кабеле повлияли на качество зашумления.

Маскиратор электромагнитных излучений «Маис-М»

Маскиратор предназначен для комплексной защиты информации, обрабатываемой основными техническими средствами и системами, от утечки за счет побочных электромагнитных излучений, а также наводок на цепи электропитания, заземления и коммуникаций, посредством постановки маскирующих помех со сплошным спектром в диапазоне частот 10Гц-10ГГц и нормализованным коэффициентом качества не хуже 0.8. Маскиратор соответствует требованиям технических условий, может устанавливаться в выделенных помещениях до 1 категории включительно (рис. 6.12).

Предусматривается 2 варианта поставки изделия:

– для защиты информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на цепи электропитания, заземления и коммуникаций (устройство изготавливается в отдельном корпусе);

– для комбинированной защиты информации (по эфиру и наводкам) (устройство изготавливается в корпусе сетевого фильтра-разветвителя «Пилот») [4, с. 5].

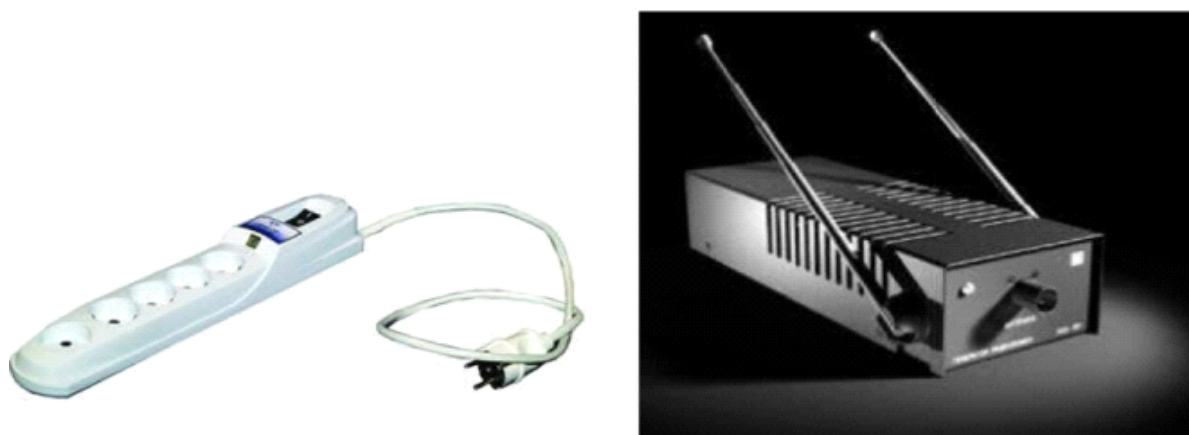


Рис.6.12. Маскиратор «Мaus-M»

Управление маскиратором сводится к подключению его к источнику питания перед включением основных технических средств и систем и отключению его после их выключения.

Генератор шума «Покров»

Генератор шума «Покров» предназначен для защиты информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок (ПЭМИН) путем излучения в окружающее пространство электромагнитного поля шумового сигнала и наводок на линии электропитания и заземления (рис. 6.13).



Рис. 6.13. Генератор шума «Покров»

Генератор шума «SEL SP-44»

Устройство защиты цепей электросети и заземления (генератор регулируемого шума по электросети) SEL SP-44.

Генератор шума «SEL SP-44» является техническим средством активной защиты от утечки информации по сети электропитания и подавления устройств несанкционированного съема информации, использующих электросеть в качестве канала передачи (рис. 6.14).



Рис. 6.14. SEL SP-44

Устройство предназначено для защиты информации обрабатываемой различными средствами вычислительной техники, средствами связи, передачи информации, от утечки за счет наводок на линии электропитания и заземления.

Данный генератор может применяться для защиты объектов обрабатывающих сведения, составляющие государственную тайну, а также для объектов обрабатывающих конфиденциальную информацию.

Основные узлы прибора (формирователи шума, регуляторы уровня и выходные усилители) представляют собой полностью цифровые устройства. Это позволяет при сохранении высокого коэффициента качества шумового сигнала полностью исключить утечку информации за счет самовозбуждения, паразитной генерации и модуляции опасным речевым сигналом, а также за счет электрических сигналов, вызванных электроакустическими преобразованиями в элементах схемы, и их утечки по цепям питания.

Некоррелируемые формирователи шума для цепей «фаза-земля» и «ноль-земля» позволяют исключить возможность съема информа-

ционного сигнала как для противофазной, так и синфазной схем подключения.

Наличие независимых регуляторов уровня для низкочастотного и высокочастотного диапазонов позволяет оптимизировать спектр помехи по электромагнитной совместимости и при сохранении достаточной эффективности маскировки.

Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания. Применение ключевых выходных усилителей существенно повышает экономичность, надежность и стабильность параметров изделия, позволяет эксплуатировать его в более жестких климатических условиях.

Во время работы прибор постоянно осуществляет самотестирование, и в случае неисправности выдает звуковой и световой сигнал.

Управление включением помехи может осуществляться с панели управления или дистанционно. Наличие интерфейса RS-485 (опция) позволяет включать его в интегрированные комплексные системы защиты информации, где удаленное управление прибором и контроль его состояния осуществляется с ПК или автономного контроллера.

С соответствии с сертификатом ФСТЭК России № 3771 от 11.07.2017, устройство «SEL SP-44» является техническим средством активной защиты информации от утечки за счет электромагнитных наводок на цепи электропитания и заземления типа «Б», соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) — по 2 классу защиты, может применяться в выделенных помещениях до 2 категории включительно.

2. Генераторы локального электромагнитного зашумления

Средство активной защиты информации «Соната-РЗ.1»

Средство активной защиты информации «Соната-РЗ.1» предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации (рис. 6.15).



¹ Рис. 6.15. Средство активной защиты информации «Соната-РЗ.1»

«Соната-РЗ.1» обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуктирования в них маскирующих шумовых напряжений.

«Стикс-4»

Устройство предназначено для активной защиты объектов вычислительной техники от утечки информации за счет побочных электромагнитных излучений и наводок на объектах до 2-ой категории включительно (рис. 6.16).



Рис. 6.16. «Стикс-4»

Имеет сертификат соответствия №3590 по требованиям безопасности информации ФСТЭК России.

За счет побочных электромагнитных излучений путем создания в диапазоне частот 0,01 – 1800 МГц электромагнитного поля маскирующего шума вокруг технических средств и подключенных к ним периферийных устройств, цепей электропитания и кабелей передачи данных.

За счет наведения шумового маскирующего электрического сигнала в отходящие от «Стикс-4» линии электропитания и заземления, а также в токопроводящие линии и инженерно-технические коммуникации в диапазоне частот 0,01 – 400 МГц.

Селективный вольтметр ВК6-18

Устройство предназначено для селективного высокоточного измерения напряжения, частоты, амплитуды и спектров радиосигналов в диапазоне частот от 20 Гц до 2 ГГц в жестких условиях эксплуатации. Имеет два измерительных входа 20 Гц – 30 МГц и 30 МГц – 2 ГГц, два преселектора калибраторы НЧ и ВЧ, вход внешнего опорного сигнала (рис. 6.17).



Рис. 6.17. Селективный вольтметр ВК6-18

Прибор позволяет осуществлять слуховой контроль амплитудной и частотной модуляций — сигналов в эфире, а в комплекте с антеннами пеленговать источник радиоизлучения в эфире. Возможен так же суточный мониторинг электромагнитной обстановки по заданной программе с помощью внешней персональной электронно-вычислительной машины (ПЭВМ) [50].

ВК6-18 позволяет:

— вводить предварительную селекцию сигналов;

- ослабить сигналы на величину до 50 дБ;
- усилить сигналы с помощью МШУ;
- выполнить измерения сигналов в радиотрактах с помощью высокоомного пробника;
- автоматически калибровать сигнальные тракты;
- осуществить цифровую фильтрацию и демодуляцию амплитудных и частотных сигналов;
- измерить пиковое, среднее, среднеквадратическое, квазипиковое значения сигналов (в соответствии с ГОСТ Р 51319-99);
- осуществлять обзор частотного диапазона, курсорные измерения, построение графиков в координатах время, амплитуда, частота с помощью ПЭВМ через USB-порт.

Широкополосный генератор радишума ПРП-1500

Формирует широкополосное шумоподобное радиоизлучение для создания помеховой обстановки, затрудняющей работу различных систем контроля, в составе которых используется радиопередающая и радиоприемная аппаратура. Диапазон частот 0,1...1500 МГц, интегральное значение выходной мощности 25 Вт.

Прибор предназначен для защиты от утечки информации и маскировки информативных побочных электромагнитных излучений и наводок персональных компьютеров и электровычислительной техники, подавления приемников дистанционного управления. Изделие камуфлировано в малогабаритную сумку для видеокамеры (рис. 6.18).



Рис. 6.18. Широкополосный генератор радишума ПРП-1500

Фильтр сетевой помехоподавляющий ЛФС-100-3Ф

Прибор предназначен для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации за счет наводок по трехфазным цепям электропитания напряжением до 380 В, частотой $50 \pm 0,5$ Гц с максимальным рабочим током до 100 А, а также для подавления помех в диапазоне частот 0,1 – 1000 МГц (рис. 6.19).



Рис. 6.19. Фильтр сетевой помехоподавляющий «ЛФС-100-3Ф»

Изделие применяется для обеспечения электромагнитной развязки по цепям электропитания радиоэлектронных устройств, средств вычислительной техники и электросетей промышленных и других объектов. Включается в трехфазную четырехпроводную сеть напряжением $(380 \pm 10\%)$ В частоты 50 Гц без соблюдения полярности. Режим работы изделия автоматический, круглосуточный. Проходит сертификацию ФСТЭК России.

Программно-аппаратный комплекс защиты объектов информационных технологий от разведки ПЭМИН ЛГШ-504

Программно-аппаратный комплекс предназначен для генерации и излучения широкополосного высокочастотного сигнала в диапазоне частот от 0,009 до 1000 МГц (рис. 6.20).



Рис. 6.20. ПЭМИН «ЛГШ-504»

Особенность изделия ЛГШ-504 — возможность плавной и независимой регулировки уровня спектральной плотности излучения в семи поддиапазонах частот. Это позволяет сформировать необходимую форму спектра излучения при установке в зависимости от требуемых условий эксплуатации.

Изделие ЛГШ-504ВЧ — широкополосный генератор (от 0,009 до 1000 МГц) со встроенной антенной. Выполнено в виде плоской тонкой (до 17 мм) излучающей пластины, которую возможно «закамуфлировать» под картину или рисунок на стене. У изделия имеется возможность плавной и независимой регулировки уровня спектральной плотности излучения в шести поддиапазонах частот. Средние частоты разделительных фильтров: 75, 225, 375, 525, 700, 900 МГц.

Средняя частота разделительного фильтра 15 МГц, для улучшения эффективности применения которого необходимо использовать внешние рамочные антенны в виде четырех петель провода, уложенных по периметру плоскости (стены, пола, потолка). Рекомендуется

размещать внешние рамочные антенны в двух и более взаимно перпендикулярных плоскостях.

***Средство активной защиты информации от утечки
за счет побочных электромагнитных излучений и наводок «Соната-РЗ»***

Изделие является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа «А» и «Б», соответствует Требованиям к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ФСТЭК России, 2014) по 1 классу защиты, может применяться в выделенных помещениях до 1 категории включительно (рис. 6.21).

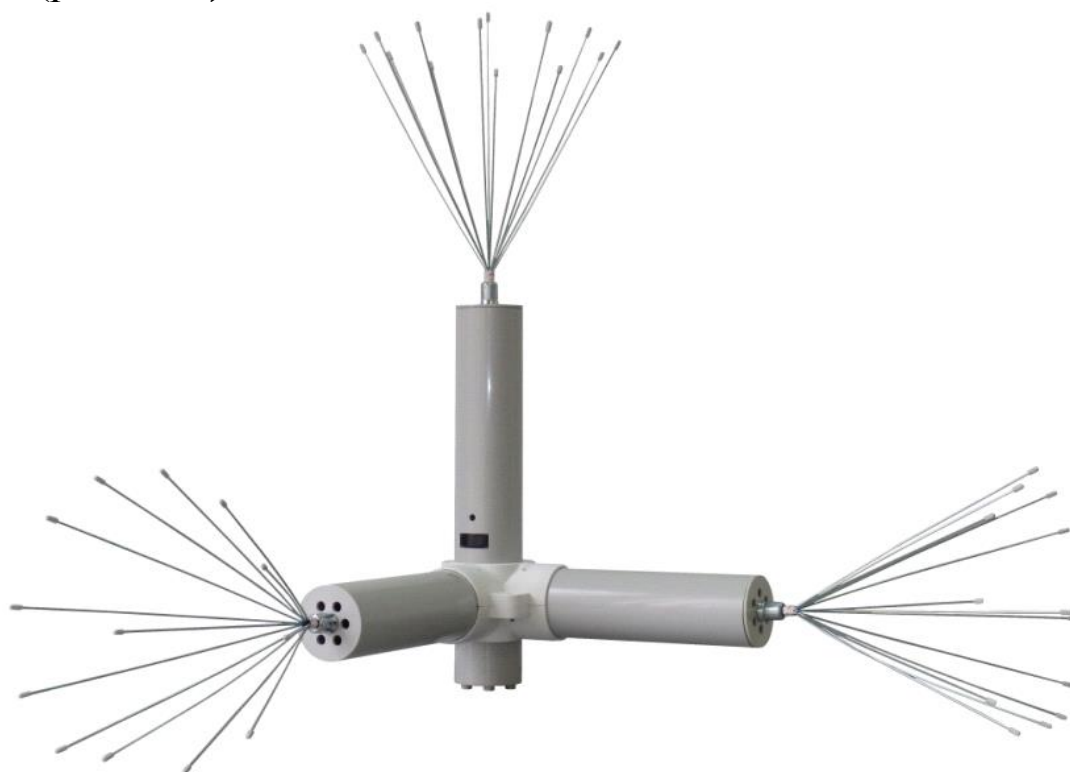


Рис. 6.21. «Соната-РЗ»

«Соната-РЗ» конструктивно может быть выполнена как система из трех систем автоматической защиты (САЗ) «Соната-РЗ.1», установленных вдоль трех взаимно перпендикулярных осей, либо в виде единого блока.

Изделие может быть включено в состав комплекса технических средств защиты информации (ТСЗИ). В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления «Соната-ДУ4.1» в комплексе с блоком питания «Соната-ИП4.х».

В отсутствие пульта управления или подключения к комплексу ТСЗИ, включение/отключение осуществляется путем включения (отключения) сетевой вилки в (от) розетку сети 220 В.

ГШ-2500МС, генератор шума

Предназначен для маскировки информативных побочных электромагнитных излучений и наводок (ПЭМИН) персональных компьютеров, рабочих станций на объектах вычислительной техники до 2 категории включительно путём формирования и излучения в окружающее пространство электромагнитного поля шума и путём наведения маскирующего сигнала в отходящие цепи и инженерные коммуникации в широком диапазоне частот (рис. 6.22).



Рис. 6.22. ГШ-2500МС, генератор шума

Генератор выполнен по 2 классу защиты и может применяться в выделенных помещениях до 2 категории включительно.

Состоит из блока генератора с излучающей антенной и блока питания.

Конструктивно блок генератора размещён в пластмассовом литом корпусе. Излучающая система состоит из стержня и рамочной

антенны, заключённой в пластиковую оболочку и зафиксированной на боковых стенках металлического шасси блока генератора с помощью фигурных гаек. Предусмотрена возможность поворота плоскости рамочной антенны относительно корпуса блока генератора, вокруг проходящей через боковые стенки корпуса оси. При этом антенна может поворачиваться на угол $\pm 180^\circ$ и фиксироваться в этих пределах под любым углом с помощью фигурных гаек на боковых стенках металлического шасси блока генератора.

Один генератор обеспечивает маскировку (защиту) информации устройств вычислительной техники, размещенной в помещении площадью $\sim 40 \text{ м}^2$.

Для защиты информации от утечки за счёт ПЭМИН в больших вычислительных центрах, в терминальных залах, мощных вычислительных комплексах рекомендуется использовать несколько генераторов, размещая их по периметру объекта. Максимальное расстояние между соседними генераторами должно быть не более 20 метров.

Электромагнитные поля, создаваемые генератором на расстоянии более 1 м от антенны, не превышают допустимого уровня при восьмичасовом пребывании персонала на рабочих местах и соответствуют ГОСТ 12.1.006, СанПиН 2.2.4.1191, а на расстоянии 10 м удовлетворяют требованиям ГКРЧ № 05-10-03-001 и ГОСТ Р 51318.22.

Технические характеристики генератора соответствуют «Требованиям к средствам активной защиты информации от утечки за счёт ПЭМИН» (ФСТЭК России, 2014).

Генератор оснащён:

- системой визуальной и звуковой индикации нормального и аварийного режимов работы;
- счётчиком времени наработки в режиме формирования маскирующего сигнала;
- технологическим выходом для контроля и измерения основных эксплуатационных характеристик.

В генераторе предусмотрена:

- регулировка интегрального уровня выходной мощности;
- защита органов регулировки от несанкционированного изменения и обнаружения несанкционированного доступа к ним.

Электропитание генератора осуществляется от сети переменного тока напряжением $(220 \pm 22 - 33) \text{ В}$ и частотой $(50 \pm 1) \text{ Гц}$ через сетевой адаптер напряжением $(5 \pm 0,4) \text{ В}$, потребляемый ток по цепи 5 В не

более 500 мА (возможно подключение к USB порту персонального компьютера).

ГШ-К-1800МС, генератор шума

Предназначен для защиты объектов вычислительной техники (ОВТ) от утечки информации за счет побочных электромагнитных излучений (ПЭМИ) путем формирования и излучения в окружающее пространство электромагнитного поля шума в широком диапазоне частот (рис. 6.23).



Рис. 6.23. ГШ-К-1800МС, генератор шума

Используется на ОВТ до 2 категории включительно.

Устанавливается в системный блок персонального компьютера.

Имеет счетчик учета общего времени наработки, регулировку мощности шумового сигнала, защиту органов регулировки от несанкционированного изменения и обнаружения несанкционированного доступа к ним.

Соответствует техническим условиям ТИДН.464217.011ТУ.

Соответствует «Требованиям к средствам активной защиты информации от утечки за счет ПЭМИН» (ФСТЭК России, 2014).

ЛГШ-221: генератор шума для сети 220В

Сетевой генератор шума «ЛГШ-221» предназначен 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 наводок путем формирования маскирующих шумоподобных помех (рис. 6.24).



Рис. 6.24. ЛГШ-221: генератор шума для сети 220В

Изделие «ЛГШ-221» соответствует типу «Б» - средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.

Изделие «ЛГШ-221» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.

Изделие «ЛГШ-221» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).

Изделие «ЛГШ-221» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.

Конструкция Изделия «ЛГШ-221» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкциониро-

ванного изменения и обнаружение несанкционированного доступа к ним.

Изделие «ЛГШ-221» имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».

Дополнительная антенна для Соната-РЗ.1(РЗ) для корректировки спектра в области 0,01-100 МГц

Дополнительная антенна Веер применяется для повышения уровней электромагнитного поля шума в диапазоне частот до 100 МГц. Для использования совместно с Соната-РЗ необходимо использование трех антенн (рис. 6.25).

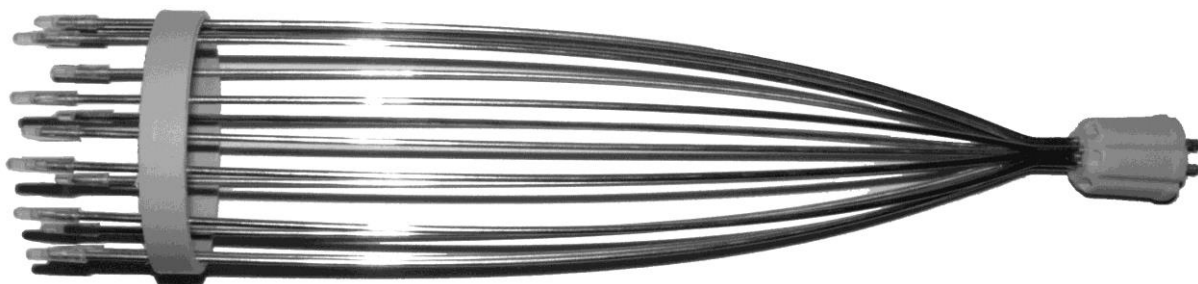


Рис. 6.25. Дополнительная антенна для Соната-РЗ.1(РЗ)

Пассивные средства защиты (экранирование)

Крышка специальная экранирующая 190мм, tower

Вариант 1(Tower 190) –для установки на системный блок с шириной по задней стенке, мм, от 188 до 192 (рис. 6.26).



Рис. 6.26. Крышка специальная экранирующая 190мм, tower

Специальная металлическая (экранирующая) крышка предназначена:

- для снижения уровня побочного электромагнитного излучения от незадействованных разъемов системного блока компьютера;
- выполнения организационно-режимных мер, исключающих несанкционированный доступ к интерфейсным разъемам и внутрь системного блока персонального компьютера.

Крышка специальная экранирующая предназначена для выполнения «Требований по технической защите информации, содержащей сведения, составляющие государственную тайну».

Крышка специальная экранирующая является металлической, экранирующей.

Крышка специальная экранирующая имеет места для опечатывания, что исключает несанкционированный доступ к разъемам под крышкой.

Крышка специальная экранирующая выпускается в двух типоразмерах, с двумя типами креплений к корпусам системных блоков, что позволяет применять крышку с большинством стандартных системных блоков персональных компьютеров, в том числе с высотой больше высоты крышки.

Крышка специальная экранирующая, slim

Специальная крышка предназначена для выполнения «Требований по технической защите информации, содержащей сведения, составляющие государственную тайну» (Требования), утвержденных приказом ФСТЭК России № 025 от 20.10.2016 г.:

снижения уровня побочного электромагнитного излучения от незадействованных разъемов системного блока компьютера;

выполнения организационно режимных мер, исключающих несанкционированный доступ к интерфейсным разъемам и внутрь системного блока персонального компьютера (рис. 6.27).



Рис. 6.27. Крышка специальная экранирующая, slim

Активная виброакустическая защита (СВАЗ)

Соната СА-4Б Генератор-акустоизлучатель

Генератор-акустоизлучатель Соната СА-4Б представляют собой электроакустический преобразователь со встроенным генератором электрического шумового напряжения. Предназначен для работы в

составе системы защиты информации от утечки по акустическим и виброакустическим каналам Соната-АВ модель 4Б.



Рис. 6.28. Соната СА-4Б Генератор-акустоизлучатель

Излучатель Соната СА-4Б позволяет реализовать изменение настроек системы виброакустической защиты в ходе эксплуатации. Это может быть использовано для повышения комфорта использования выделенного помещения ("включена/выключена аппаратура звукоусиления", "работа с документами/совещание" и т.п.). Этот функционал доступен при использовании блока питания и управления Соната-ИП4.х и пульта дистанционного управления Соната-ДУ4.1 или Соната-ДУ4.3.

Для выполнения начальных настроек генератора-излучателя Соната СА-4Б используются блоки питания и управления Соната-ИП4.х в режиме программатора.

Соната СА-4Б1 Генератор-акустоизлучатель

Генератор-акустоизлучатель Соната СА-4Б1 представляют собой электроакустический преобразователь со встроенным генератором электрического шумового напряжения. Предназначен для работы в составе системы защиты информации от утечки по акустическим и виброакустическим каналам Соната-АВ модель 4Б (рис. 6.29).



Рис. 6.29. Соната СА-4Б1 Генератор-акустоизлучатель

Излучатель Соната СА-4Б1 позволяет реализовать изменение настроек системы виброакустической защиты в ходе эксплуатации. Это может быть использовано для повышения комфорта использования выделенного помещения ("включена/выключена аппаратура звукоусиления", "работа с документами/совещание" и т.п.). Этот функционал доступен при использовании блока питания и управления Соната-ИП4.х и пульта дистанционного управления Соната-ДУ4.1 или Соната-ДУ4.3.

Для выполнения начальных настроек генератора-излучателя Соната СА-4Б1 используются блоки питания и управления Соната-ИП4.х в режиме программатора.

Соната СВ-4Б Генератор-вибровозбудитель

Генератор-вибровозбудитель Соната СВ-4Б представляют собой электроакустический преобразователь со встроенным генератором электрического шумового напряжения. Предназначен для работы в составе системы защиты информации от утечки по акустическим и виброакустическим каналам Соната-АВ модель 4Б (рис. 6.30).



Рис. 6.30. Соната СВ-4Б Генератор-вибровозбудитель

Излучатель Соната СВ-4Б позволяет реализовать изменение настроек системы виброакустической защиты в ходе эксплуатации. Это может быть использовано для повышения комфорта использования выделенного помещения («включена/выключена аппаратура звукоусиления», «работа с документами/совещание» и т.п.). Этот функционал доступен при использовании блока питания и управления Соната-ИП4.х и пульта дистанционного управления Соната-ДУ4.1 или Соната-ДУ4.3.

Для выполнения начальных настроек генератора-излучателя Соната СВ-4Б используются блоки питания и управления Соната-ИП4.х в режиме программатора.

ЛВП-2а, акустический излучатель

Акустический излучатель «ЛВП-2а» предназначен для возбуждения маскирующих акустических помех в различных закрытых пространствах (таких, как междверные проемы, воздуховоды и др.) (рис. 6.31).



Рис. 6.31. ЛВП-2а, акустический излучатель

Может использоваться в системах виброакустического зашумления генераторов шума серии ЛГШ-4хх.

Защита проводных линий

Телефонные аппараты (в том числе при положенной трубке) или другие технические средства могут быть использованы для прослушивания разговоров, ведущихся в помещениях, где они установлены. Средства защиты, устанавливаемые в проводные линии, обеспечива-

ют защиту речевой информации от утечки за счет акустоэлектрических преобразований, ВЧ-навязывая, ВЧ-прокачки

Соната-ВК4.1 Размыкатель телефонной линии

Размыкатель телефонной линии Соната-ВК 4.1 предназначен для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям (рис. 6.32).



Рис. 6.32. Соната-ВК4.1 Размыкатель телефонной линии

Корунд – устройство защиты телефонного аппарата (ТА), подключаемого к аналоговой телефонной линии, от утечки через него речевой информации в режиме ожидания вызова (серт.ФСТЭК)

Устройство защиты Корунд предназначено для исключения утечки информации через абонентскую линию аналоговых АТС, является ПСЗ и представляет собой фильтр. Устройство обеспечивает затухание сигналов малого уровня от ТА в сторону абонентской линии. Защита аналоговых АТС и от микрофонного эффекта (рис 6.33).



Рис. 6.33. Корунд – устройство защиты телефонного аппарата

МП-10 –защищенный источник питания для устройств защиты от утечки информации и другого радиоэлектронного оборудования, устанавливаемых в выделенных помещениях

Устройство защиты МП-10 предназначено для исключения утечки информации по сети питания от технических средств при акустическом воздействии на них (рис. 6.34).



Рис. 6.34. МП-10 –защищенный источник питания

Устройство подает напряжение питания 12 В на технические средства, если напряжение в сети переменного тока больше 170 В, и автоматически отключает если напряжение менее 30 В. При пропадании шумового сигнала происходит автоблокировка и технические средства отключаются.

Работоспособность устройства МП-10 автоматически проверяется с помощью светящихся светодиодов.

Для блокировки сигналов акустоэлектрических преобразований и ВЧ навязывания в первичную цепь (220 В) включены:

- генератор шумового сигнала;
- шунтирующие ВЧ конденсаторы;
- фильтр.

Устройство обеспечивает активный и пассивный уровень защиты.

МП-1А в евророзетке, устройство аналогового ТА

Устройство защиты МП-1А предназначено для исключения утечки информации через абонентскую линию аналоговых АТС в режиме ожидания вызова. В нём одновременно используются как пассивные средства защиты (ПСЗ), так и активные средства защиты (АСЗ). Устройство содержит генератор шума, нелинейные цепи и узел подавления сигналов малого уровня, с помощью которых обеспечивается введение шумового сигнала в абонентскую линию, затухание сигнала малого уровня от телефонного аппарата (ТА) в сторону абонентской линии и защита информации от утечки при активных методах воздействия в режиме ожидания вызова. Устройство отличается малыми габаритами и низкой потребляемой мощностью по сравнению с ближайшими прототипами типа Гранит-8,11,12, это позволяет разместить его внутри телефонных розеток. Эксплуатационные расходы по изделию не требуются (рис. 6.35).



Рис. 6.35. МП-1А в евророзетке – устройство аналогового ТА

МП-2 – средство исключения утечки по трансляционной сети

Предназначено для защиты аналогового телефонного аппарата (ТА), подключаемого к аналоговой телефонной линии, от утечки через него речевой информации в режиме ожидания вызова (рис. 6.36).



Рис. 6.36. МП-2 – средство исключения утечки по трансляционной сети

Позволяет блокировать утечку акустической информации из помещения где установлен ТА в режиме положенной трубки.

Габариты изделия позволяют устанавливать его в телефонную розетку.

Устройство содержит фильтр подавления ВЧ сигнала и нелинейные цепи.

МП-3 – средство для исключения утечки информации в сеть питания при акустическом воздействии на изделие и пропадании сетевого напряжения

Предназначено для исключения утечки информации в сеть питания при акустическом воздействии на изделие и пропадании сетевого напряжения. МП-3 может быть использовано для защиты от утечки информации любого изделия, которое потребляет от сети переменного тока напряжением 220 В не более 170 Вт (рис. 6.37).



Фото 6.37. МП-3 – средство для исключения утечки информации в сеть питания

МП-4, устройство защиты для исключения утечки информации от вторичных источников при акустическом воздействии

Устройство защиты МП-4 предназначено для исключения утечки информации от вторичных источников при акустическом воздействии на них и обеспечивает защиту при активных методах воздействия. Устройство содержит генератор шума и схему контроля, с помощью которых обеспечивается введение шумового сигнала в цепь вторичных часов и контроль его наличия (рис. 6.38).



Фото 6.38. МП-4 – устройство защиты для исключения утечки информации от вторичных источников при акустическом воздействии

МП-5 – устройство защиты громкоговорителя системы оповещения или однопрограммного приемника системы оповещения

Устройство предназначено для защиты громкоговорителя системы оповещения, или однопрограммного приемника от утечки через них акустической информации. Устройство обеспечивает защиту при активных методах воздействия (рис. 6.39).



Рис. 6.39. МП-5 – устройство защиты громкоговорителя системы оповещения или однопрограммного приемника системы оповещения

МП-7 Гвард, защита телефонного аппарата (ТА), подключаемого на цифровой порт АТС, от утечки через акустоэлектрические преобразователи телефона акустических сигналов помещения (без исследований ТА и монтажа)

Устройство защиты МП-7 (ГВАРД) предназначено для защиты телефонного аппарата (ТА), подключаемого на цифровой порт АТС, от утечки через акустоэлектрические преобразователи телефона акустических сигналов помещения (рис. 6.40).



Рис. 6.40. МП-7 Гвард – защита телефонного аппарата (ТА), подключаемого на цифровой порт АТС, от утечки через акустоэлектрические преобразователи телефона акустических сигналов помещения (без исследований ТА и монтажа)

Устройство исключает режим прослушивания помещения (в так называемом «полицейском режиме»).

Для телефонных аппаратов, в которых обнаружен акустический канал утечки через элементы схемы и конструкции телефона (паразитные каналы), вместе с изделием МП-7 (ГВАРД) дополнительно должно применяться устройство защиты МП-1Ц, что в таких случаях исключает утечку информации, а также обеспечивает защиту при активных методах воздействия в режиме ожидания вызова.

Изделие может устанавливаться в выделенных помещениях до 2 категории включительно.

МП-8, Сигма-РА, устройство защиты помещений от утечки речевой и другой акустической информации через телефонный аппарат

Устройство защиты МП-8 («Сигма-РА») предназначено для защиты помещений от утечки речевой и другой акустической информации через телефонный аппарат (ТА) в режиме ожидания вызова (при положенной трубке на рычаги ТА) в аналоговых телефонных линиях (ТЛ). телефонного аппарата (ТА) (рис 6.41).



Рис. 6.41. МП-8, Сигма-РА – устройство защиты помещений от утечки речевой и другой акустической информации через телефонный аппарат

Устройство исключает несанкционированный доступ к электроакустическим преобразователям внутри ТА для дистанционного получения акустической информации из помещения, где он установлен.

Устройство обеспечивает защиту при активных методах воздействия.

Устройство МП-8 может устанавливаться в выделенных помещениях до 3 категории включительно.

Блокираторы сотовой связи

БАРХАН-1 – блокиратор GSM-900/1800, EGSM, 3G-2100-2170МГц, CDMA2000-450, P_{вых}=1.85Вт, R_{max}=15м (с опциями WiFi/BT и 4G)

Устройство предназначено для технического ограничения использования мобильных телефонов на контролируемых территориях. Может использоваться для санкционированного блокирования работы абонентских терминалов (на совещаниях, в местах с повышенными требованиями по соблюдению тишины и др.), а также для защиты информации от утечки с использованием каналов сотовой связи (акустический и видео контроль, определение местоположения объекта, дистанционное управление различными устройствами и пр.) (рис. 6.42).



Рис. 6.42. БАРХАН-1 – блокиратор GSM-900/1800, EGSM, 3G-2100-2170МГц, CDMA2000-450, $P_{\text{вых}}=1.85\text{Вт}$, $R_{\text{max}}=15\text{м}$ (с опциями WiFi/BT и 4G)

Блокиратор сотовой связи «Бархан-1»:

- блокирует все известные стандарты сотовой связи;
- эстетичный внешний вид прибора (отсутствие внешних антенн);
- 12 месяцев гарантии;
- наличие Санитарно-Гигиенического Сертификата РФ;
- возможность отключения EGSM для повышения радиуса подавления других стандартов;
- возможность отключения DAMPS для повышения радиуса действия подавления других стандартов;
- круглосуточный режим работы в широком диапазоне температур окружающей среды;
- четыре независимых канала со своими антенными системами;
- плавная регулировка радиуса действия позволяет подавлять связь не далее нужного радиуса, не мешая работе мобильных телефонов вне контролируемого помещения;
- простота установки и использования.

Кедр-3М – блокиратор сотовой связи (GSM-900/1800, E-GSM, 3G, 4G (LTE800, LTE2600, WiMAX), CDMA2000, DECT, WiFi, Bluetooth, ZigBee, радиус до 60м)

«КЕДР-3М» применяется для защиты от утечки информации по каналам стандартов GSM-900/1800, E-GSM, UMTS (3G), WiMax (4G), NMT-450, WiFi, Bluetooth, CDMA2000 1X, DECT, во время проведения совещаний и переговоров (рис. 6.43).



Рис. 6.43. Кедр-3М – блокиратор сотовой связи (GSM-900/1800, E-GSM, 3G, 4G (LTE800, LTE2600, WiMAX), CDMA2000, DECT, WiFi, Bluetooth, ZigBee, радиус до 60м)

В результате работы изделия происходит потеря сети связи пользовательского терминала с базовой станцией.

«КЕДР-3М» оснащен регуляторами мощности каждого диапазона для обеспечения локальной работы в пределах выделенного помещения.

КЕДР-5М – блокиратор сотовой связи (GSM-900/1800, 3G, 4G (LTE800, LTE2600, WiMAX), CDMA2000, DECT, WiFi, Bluetooth, ZigBee, радиус до 40м)

Изделие «КЕДР-5М» предназначено для блокирования работы всех типов устройств несанкционированного прослушивания и передачи данных, аудио- и видео передатчиков, использующих стандарты GSM-900/1800, 3G и 4G, DECT, CDMA, WiFi-2.4, WiFi-5.0, BLUETOOTH, ZigBee (рис. 6.44).



Рис. 6.44. КЕДР-5М – блокиратор сотовой связи (GSM-900/1800, 3G, 4G (LTE800, LTE2600, WiMAX), CDMA2000, DECT, WiFi, Bluetooth, ZigBee, радиус до 40м)

Применяется для защиты от утечки информации по каналам указанных выше стандартов в выделенных помещениях, во время проведения совещаний и переговоров.

Эффективный радиус действия изделия подбирается экспериментальным путем в районе эксплуатации, и в идеальных условиях увеличивается до 40 метров.

ЛГШ-701– подавитель сотовой связи

Изделие ЛГШ-701 предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи работающих в стандартах (рис. 6.45):

IMT-MC-450(NMT-450i)

GSM900

E-GSM900

DSC/GSM1800

DECT1800

CDMA2000 1x

CDMA-800

AMPS/N-AMPS/D-AMPS-800/CDMA-800



Рис. 6.45. ЛГШ-701 – подавитель сотовой связи

Блокиратор сотовой связи ЛГШ-701 выпускается в двух модификациях: ЛГШ-701 (базовая) и ЛГШ-701М. Различия между модификациями заключаются в том, что они работают в разных диапазонах сотовой связи. Изделие ЛГШ-701 в модификации М вместо стандарта IMT-MS-450 блокирует работу сетей стандарта AMPS/N-AMPS/D-AMPS-800/CDMA-800.

Принцип работы заключается в генерации шумового сигнала, который подается на выходы антенн. В приборе имеются три выхода и, соответственно, три антенны. По каждому из выходов возможна плавная регулировка мощности излучения. Использование стандартного выходного разъема типа CP50-73 (аналог BNC) с волновым сопротивлением 50 Ом позволяет использовать внешние антенные устройства как для увеличения дальности подавления, так и для формирования требуемой формы зоны подавления отдельно для каждого диапазона частот.

Изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания, созданных на основе сотовых телефонов всех вышеперечисленных стандартов.

ЛГШ-702 – подавитель Bluetooth и WiFi

Изделие ЛГШ-702 предназначено для блокирования (подавления) работы устройств, работающих в стандартах Bluetooth и WiFi (рис. 6.46).

Изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания, несанкционированной передачи данных, а также, для блокирования работы радиоис-

полнительных устройств, созданных с использованием стандартов Bluetooth и WiFi.

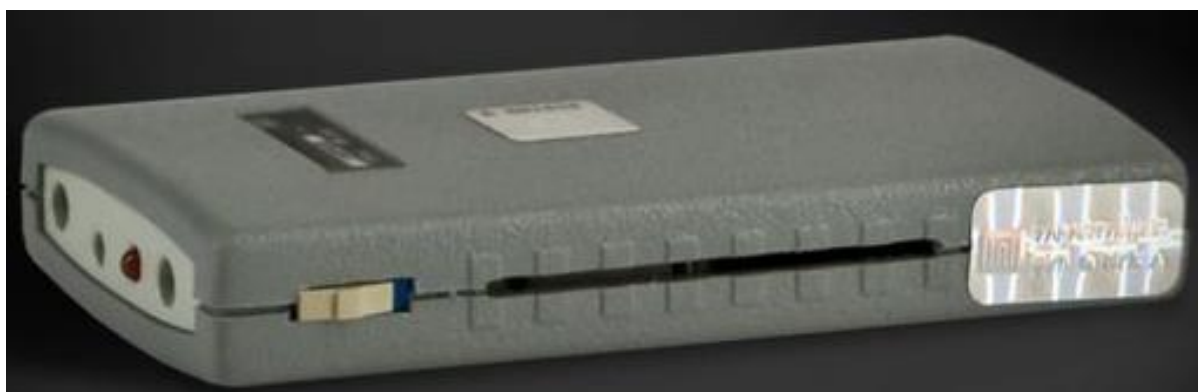


Рис. 6.46. ЛГШ-702 – подавитель Bluetooth и WiFi

Включение и выключение генератора осуществляется выключателем «Питание», расположенном на боковой грани Изделия. Включенному состоянию генератора соответствует свечение светодиода.

Включать изделие рекомендуется только по мере необходимости.

Мощность (а соответственно, и дальность подавления) регулируется. Необходимо-достаточный уровень излучения выставляется по месту установки.

Принцип действия генератора основан на излучении шумового сигнала от автогенератора и подачи этого сигнала на выход антенны. Антенна находится внутри корпуса устройства.

При включении изделия происходит потеря связи пользовательским терминалом, а после выключения изделия пользовательский терминал возвращается в нормальный режим работы.

ЛГШ-711 – подавитель сотовой связи

Изделие ЛГШ-711 предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи, работающих в стандартах (рис. 6.47):

IMT-MC-450(NMT-450i)

GSM900

E-GSM900

DSC/GSM1800

DECT1800

CDMA2000 1x

CDMA-800

AMPS/N-AMPS/D-AMPS-800/CDMA-800



Рис. 6.47. ЛГШ-711 – подавитель сотовой связи

Принцип работы заключается в генерации шумового сигнала, который подается на выходы антенн. В приборе имеются три выхода и, соответственно, три антенны. По каждому из выходов возможна плавная регулировка мощности излучения.

Использование стандартного выходного разъема типа CP50-73 (аналог BNC) с волновым сопротивлением 50 Ом позволяет использовать внешние антенные устройства как для увеличения дальности подавления, так и для формирования требуемой формы зоны подавления отдельно для каждого диапазона частот.

Изделие может быть использовано для блокировки работы устройств несанкционированного прослушивания, созданных на основе сотовых телефонов всех вышеперечисленных стандартов.

ЛГШ-719 – блокиратор сотовой связи и сигналов 3G, LTE, Bluetooth, WiFi

Блокиратор сотовой связи ЛГШ-719 предназначен для блокировки (подавления) связи между базовыми станциями и мобильными

телефонами сетей сотовой связи, работающих в стандартах (рис. 6.48):

- IMT-MC-450;
- GSM900;
- DSC/GSM1800, (DECT1800);
- IMT-2000/UMTS (3G);
- 4G-2600 (LTE, WiMAX);
- 4G-800;
- Bluetooth;
- WiFi.



Рис. 6.48. ЛГШ-719 – блокиратор сотовой связи и сигналов 3G, LTE, Bluetooth, WiFi

Блокираторы беспроводной связи предназначены для блокирования работы устройств несанкционированного получения информации, работающих в стандартах сетей сотовой связи и в стандартах Bluetooth и WiFi.

Принцип работы заключается в генерации шумовой помехи в необходимом диапазоне частот. При этом возможна плавная регулировка мощности помехового сигнала в каждом из диапазонов, что

позволяет обеспечить блокирование беспроводных стандартов связи только в границах защищаемого помещения.

ЛГШ-719 прост в установке и эксплуатации, не требует специальных навыков. Отличительной характеристикой является наличие 7 независимых каналов регулировки мощности по каждому диапазону частот, что позволяет создавать зоны блокирования исходя из ваших требований.

ЛГШ-719 прост в установке и эксплуатации, не требует специальных навыков. Отличительной характеристикой является наличие 7 независимых каналов регулировки мощности по каждому диапазону частот, что позволяет создавать зоны блокирования исходя из ваших требований.

Изделие ЛГШ-719 в модификации М вместо стандарта IMT-МС-450 подавляет работу сетей стандарта AMPS/N-AMPS/D-AMPS-800/CDMA-800.

ЛГШ-719 Кейс, блокиратор сотовой связи и сигналов 3G, LTE, Bluetooth, WiFi

Блокиратор сотовой связи ЛГШ-719 Кейс предназначен для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах (рис. 6.49):

IMT-МС-450,
GSM900,
DSC/GSM1800, (DECT1800),
IMT-2000/UMTS (3G),
4G (LTE, WiMAX)
Bluetooth,
WiFi.

Изделие избавит Вас от несанкционированного съема информации через стандарты сотовой связи и заблокирует работу устройств несанкционированного прослушивания, созданных на основе сотового телефона, цифровых каналов передачи данных Bluetooth и WiFi. Блокиратор подавляет работу сотовой связи в местах, где требуется полная тишина и может применяться в конференц-залах, комнатах для переговоров, в музеях, театрах, галереях, церквях и учебных аудиториях.



Рис. 6.49. ЛГШ-719 Кейс – блокиратор сотовой связи и сигналов 3G, LTE, Bluetooth, WiFi

ЛГШ-719 Кейс прост в установке и эксплуатации, не требует специальных навыков. Отличительной характеристикой является наличие 6 независимых каналов регулировки мощности по каждому диапазону частот, что позволяет создавать зоны блокирования исходя из ваших требований.

Фильтры сетевые помехоподавляющие (пассивная защита электропитания)

ЛФС-10-1Ф –фильтр сетевой помехоподавляющий до 10А

Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц (рис. 6.50).



Рис. 6.50. ЛФС-10-1Φ – фильтр сетевой помехоподавляющий до 10А

«ЛФС-10-1Φ» соответствует типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания.

ЛФС-10-1Φ» соответствует документу «Требования к пассивным средствам защиты информации от побочных электромагнитных наводок на линии электропитания» (ФСТЭК России, 2015), – по 1 классу защиты.

ЛФС-100-3Φ, сетевой фильтр 100А

Фильтр сетевой помехоподавляющий «ЛФС-100-3Φ» предназначен для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации за счет наводок по трехфазным цепям электропитания напряжением до 380 В, частотой 50+0,5 Гц с максимальным рабочим током до 100 А (рис. 6.51).



Рис 6.51. ЛФС-100-3Φ – сетевой фильтр 100А

Изделие применяется для обеспечения электромагнитной развязки по цепям электропитания радиоэлектронных устройств, средств вычислительной техники и электросетей промышленных и других объектов.

Изделие включается в трехфазную четырехпроводную сеть напряжением (380+10%) В частоты 50 Гц без соблюдения полярности.

Режим работы Изделия автоматический, круглосуточный.

Фильтр сетевой ФСП-3Ф-15А-ИН-1,5

3-х фазный фильтр ФСП-3Ф-15А-ИН предназначен для защиты радиоэлектронных устройств от утечки информации по цепям заземления и электропитания напряжением 380/220В 50Гц, а также защиты их от высокочастотных и импульсных сетевых помех. Выполнен 5-проводным, с изолированной нейтралью, с рабочим током до 15А по каждой фазе. Может использоваться в цепи постоянного тока до 300В на ток до 30А (рис. 6.44).

Выпускается в 2-х модификациях: ФСП-3Ф-15А-ИН – базовая модель, ФСП-3Ф-15А-ИН-1,5 – с уменьшенным реактивным током утечки фазы на корпус.

При параллельном включении фильтров их соответствующие характеристики суммируются.



Рис. 6.52. Фильтр сетевой ФСП-3Ф-15А-ИН-1,5

ФСПК-10 – сетевой фильтр для защиты информации от утечки

Защитное устройство (ЗУ) предназначено для защиты информации по однофазным двухпроводным сетям электропитания с заземляющим проводом напряжением 220В, частотой 50 Гц, с максимальным рабочим током 10А в диапазоне частот 0,15 МГц – 1000 МГц (рис. 6.53).



Рис. 6.53. ФСПК-10 – сетевой фильтр для защиты информации от утечки

ФСПК-100 – сетевой фильтр для защиты информации от утечки

Защитные устройства (ЗУ) предназначены для подавления напряжений помех в трехфазных четырехпроводных сетях электропитания напряжением 220/380В, частотой 50 Гц, с максимальным рабочим током 100 А в диапазоне частот от 20 кГц до 1000 МГц (рис. 6.54).

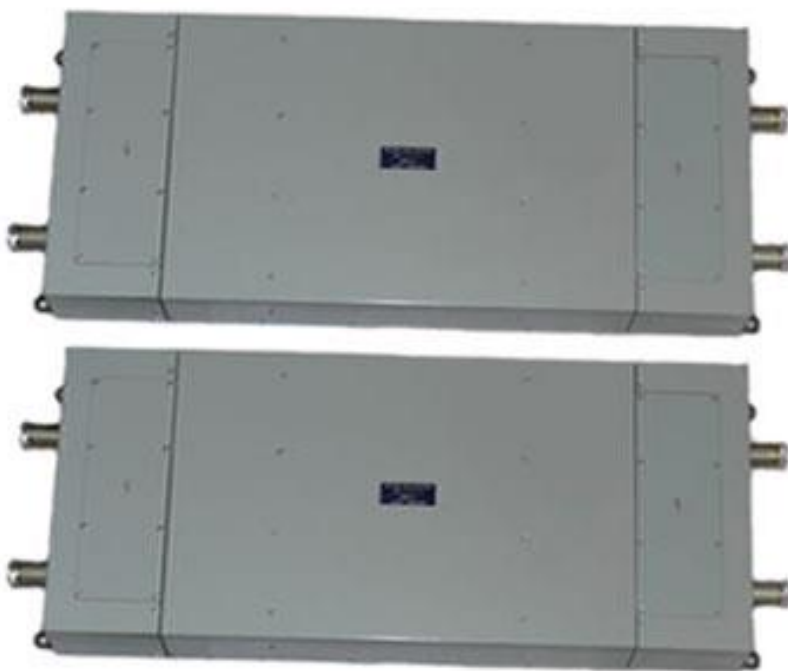


Рис. 6.54. ФСПК-100 – сетевой фильтр для защиты информации от утечки

ФСПК-40 – сетевой фильтр для защиты информации от утечки

Защитное устройство (ЗУ) предназначено для защиты информации по однофазным двухпроводным сетям электропитания с заземляющим проводом напряжением 220В, частотой 50 Гц, с максимальным рабочим током 40А в диапазоне частот 0,15 МГц – 1000 МГц (рис. 6.55).



Рис. 6.55. ФСПК-40 – сетевой фильтр для защиты информации от утечки

СТБ 211 – средство активной защиты информации от утечки за счет ПЭМИН

Средство активной защиты информации СТБ 211 предназначено для защиты сведений, обрабатываемых техническими средствами и системами (до 2 категории включительно) от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Средство защиты информации СТБ 211 может устанавливаться в выделенных помещениях до 1 категории включительно (рис 6.56).



Рис 6.56. СТБ 211 – средство активной защиты информации от утечки за счет ПЭМИН

ST 500 ПИРАНЬЯ – многофункциональный поисковый прибор

Поисковый прибор ST 500 ПИРАНЬЯ предназначен для поиска идентификации и локализации подслушивающих устройств (рис. 6.57).

Поисковые возможности прибора ST 500 ПИРАНЬЯ:

- поиск и локализация радиопередающих подслушивающих устройств;
- идентификация цифровых протоколов обнаружения радиосигналов: GSM, CDMA, Bluetooth, LTE, WiFi;
- идентификация сигналов базовых станций и мобильных устройств цифровой связи;
- поиск и локализация активных проводных подслушивающих устройств;
- активация электретных кабельных микрофонов путём подачи в линию напряжения смещения;
- поиск и локализация подслушивающих устройств, передающих информацию в инфракрасном диапазоне.



Фото 6.57. ST 500 ПИРАНЬЯ –многофункциональный поисковый прибор

Функционально прибор ST 500 ПИРАНЬЯ состоит из четырех каналов обнаружения.

Каналы для обнаружения беспроводных подслушивающих устройств:

СЕЛЕКТИВНЫЙ ВЧ ДЕТЕКТОР предназначен для обнаружения аналоговых и цифровых (использующих стандарты GSM, LTE, Bluetooth, WiFi) радиопередающих подслушивающих устройств в диапазоне частот 20 - 6 000 МГц;

ИК ДЕТЕКТОР предназначен для обнаружения ИК передатчиков (подслушивающих устройств, использующих для передачи информации инфракрасный диапазон частот).

Каналы для обнаружения проводных подслушивающих устройств:

ПРОВОДНОЙ ПРИЕМНИК предназначен для обнаружения высокочастотных сигналов подслушивающих устройств, передающих информацию по силовым и слаботочным проводным линиям в диапазоне частот 100 – 180 МГц;

УСИЛИТЕЛЬ НИЗКОЙ ЧАСТОТЫ предназначен для обнаружения НЧ сигналов подслушивающих устройств.

СКОРПИОН 3.5 – скоростной поисковый приемник радиосигналов

Поисковый приемник радиосигналов Скорпион 3.5 предназначен для автоматического обнаружения сигналов, излучаемых нелегальными радиопередатчиками и подавление каналов их приема. Скорпион 3.5 выпускается с 1997 года, однако и до сегодняшнего дня остается одним из лучших портативных поисковых приемников в своем классе (рис. 6.58).



Рис. 6.58. СКОРПИОН 3.5 – скоростной поисковый приемник радиосигналов

В отличие от большинства аналогов Скорпион 3.5 представляет собой универсальное комбинированное устройство, сочетающее функции поискового приемника, радиочастотомера, интерсептора и постановщика помех. При регулировке чувствительности приемника с помощью входного аттенюатора и исключения из поиска частот известных сигналов, время сканирования всего диапазона не превышает 10 секунд. В этом случае прибор может использоваться для непрерывного радиоконтроля с постоянным сканированием заданного диапазона частот. Функции приемника постоянно расширяются за счет обновления версий программного обеспечения.

Основные функциональные возможности поискового приемника Скорпион 3.5:

- производить изучение радиоэлектронной обстановки с запоминанием частот сигналов;
- обнаруживать и определять местоположение передатчика с использованием разнесенного приема на две антенны и контроля уровня гармоник;
- подавлять канал приема сигнала обнаруженного передатчика путем постановки на его частоте прицельной помехи;
- обнаруживать работающие телефоны сотовой связи стандарта GSM (в том числе при скачках частоты передачи) с индикацией частоты и возможностью автоматической блокировки (при работе на фиксированных частотах);
- обнаруживать радиотелефоны стандарта DECT;
- осуществлять поиск в одном или двух программируемых участках диапазона частот;
- просматривать и редактировать три буфера памяти обнаруженных сигналов и исключенных каналов приема;
- проверять работоспособность приемников, индикаторов поля, частотомеров и других технических средств при помощи встроенного тестового генератора.

ОПТИК-2 – профессиональный обнаружитель скрытых видеокамер

Обнаружитель скрытых видеокамер ОПТИК-2 предназначен для поиска и локализации скрытых, камуфлированных в интерьер видеокамер (в том числе с объективом типа «pin-hole») независимо от их состояния и типа передачи или записи видеосигнала (рис. 6.59).

Поиск объектива видеокамеры методом световой оптической локации. При обнаружении объектива скрытой камеры в объективе

ОПТИК-2 будет наблюдаться точечное пятно зеленого или красного цвета — результат отражения подсветки от видеокамеры.



Рис. 6.59. ОПТИК-2 – профессиональный обнаружитель скрытых видеокамер

Бинокляр ОПТИК-2 позволяет проводить более качественный осмотр объекта. Меньшая утомляемость оператора по сравнению с монокулярами (нет необходимости закрывать один глаз). Зелёная подсветка позволяет находить видеокамеры защищённые специальными полосовыми фильтрами, используемыми для противодействия всем обнаружителям, использующим только красную подсветку. Встроенный аккумулятор позволяет не заботиться об элементах питания. 6,5 кратное увеличение позволяет детально рассмотреть самые мелкие и труднодоступные элементы интерьера

Основные конкурентные преимущества обнаружителя ОПТИК-2:

- бинокляр позволяет проводить более качественный осмотр объекта;
- меньшая утомляемость оператора по сравнению с монокулярами (нет необходимости закрывать один глаз);
- зелёная подсветка позволяет находить видеокамеры, защищённые специальными полосовыми фильтрами, используемыми для противодействия всем обнаружителям, использующим только красную подсветку;
- встроенный аккумулятор позволяет не заботиться об элементах питания;
- 6,5-кратное увеличение позволяет детально рассмотреть самые мелкие и труднодоступные элементы интерьера.

Профессиональный обнаружитель скрытых видеокамер ОПТИК-2 выполнен в виде бинокля в обрезиненном металлическом корпусе. Излучение создаваемое светодиодной подсветкой обнаружителя ОПТИК-2 безопасно для кратковременной прямой засветки глаз. В приборе ОПТИК-2 не используется лазерное излучение.

RAKSA-120 – селективный индикатор поля

Селективный индикатор поля RAKSA-120 предназначен для обнаружения в ближней зоне и определения местоположения радиопередающих устройств, использующихся для негласного съема аудио - и видеоинформации. Работа с индикатором RAKSA-120 не требует специальной профессиональной подготовки (рис. 6.60).



Рис. 6.60. RAKSA-120– селективный индикатор поля

Изделие выпускается в двух версиях:

- локальная (для внутреннего, российского, рынка);
- экспортная, под наименованием RAKSA-Idet.

Индикатор поля RAKSA-120 позволяет обнаруживать:

- сотовые телефоны стандартов GSM 850/ 900E/ 1 800/ 1 900, UMTS 850/ 900/ 1 800/ 1 900/ 2 100, CDMA 450 (A-H)/ 800/ 1 900 для локальной версии;
- сотовые телефоны стандартов GSM 850/ 900E/ 1 800/ 1 900, UMTS 850/ 900/ 1 800/ 1 900/ 2 100, CDMA 450 (A-H)/ 800/ 1 900,

GSM 900E/ 1 800, UMTS 900/ 2 100, CDMA 450 (A) для экспортной версии;

- беспроводные телефоны стандарта DECT;
- устройства Bluetooth и Wi-Fi;
- беспроводные видеокамеры;
- радиопередатчики с аналоговой модуляцией (АМ, ЧМ, ФМ);
- радиопередатчики с цифровой модуляцией и непрерывной несущей (FSK, PSK и др.);
- радиопередатчики с широкополосной модуляцией с полосой до 10 МГц.

По принципу действия селективный индикатор поля RAKSA-120 представляет собой скоростной супергетеродинный приемник с низкой ПЧ и синтезатором частоты. Время цикла сканирования и анализа всех цифровых и аналоговых сигналов не превышает 1,5 секунды. Индикатор поля RAKSA-120 может работать в режимах охраны, обзора, поиска, поиска с вычитанием спектра и мониторинга цифровых сигналов.

Язык интерфейса русский (локальная версия RAKSA-120) и мультиязычный — английский, немецкий, французский, итальянский, испанский (экспортная версия RAKSA-Idet).

Отличительные особенности индикатора поля RAKSA-120:

- селективный прием радиосигналов;
- высокая скорость сканирования и анализа;
- обнаружение широкополосных и цифровых сигналов;
- адаптация к фону в режиме охраны;
- возможность поиска с вычитанием спектра;
- аудиоконтроль сигналов;
- измерение частоты и уровня сигнала;
- журнал событий тревоги;
- бесшумная индикация тревоги (вибросигнал);
- отсутствие внешней антенны.

Индикатор поля RAKSA-120 может работать в режимах охраны, обзора, поиска, поиска с вычитанием спектра и мониторинга цифровых сигналов.

СМА-100 –усилитель для обследования проводных линий

Усилитель для обследования проводных линий СМА-100 используется для обнаружения и идентификации подслушивающих устройств, передающих информацию по проводным линиям, таким

как телефонные линии, компьютерные сети, линии питания, сигнализации и т.д.(рис. 6.61).



Рис. 6.61. СМА-100 – усилитель для обследования проводных линий

СМА-100 разработан согласно последним требованиям технической безопасности и гарантирует хорошие результаты обнаружения во многих ситуациях.

Особенности усилителя СМА-100:

- имеет встроенный АС/ DC вольтметр, селективные звуковые фильтры с широким динамическим диапазоном;
- имеет сбалансированный вход с высоким сопротивлением обеспечивает гарантированное подключение к подозрительной проводной линии;
- обеспечивает напряжение смещения, настраиваемое между 14,5 В и +14,5 В, которое используется для активации возможных приборов, которые чувствительны к току или к напряжению. Генератор напряжения смещения соответствует параметрам большинства линий.

Все эти функции используют сложную автоматическую схему усиления, что позволяет данному прибору превосходить по характеристикам большинство аудио усилителей.

ST111 – детектор поля

Индикатор электромагнитного поля ST111 является профессиональным поисковым прибором, предназначенным для обнаружения и определения местоположения радиоизлучающих специальных технических средств негласного получения информации. К таким средствам, прежде всего, относят: радиомикрофоны, телефонные радиоретрансляторы, радиостетоскопы, скрытые видеокамеры с передачей информации по радиоканалу, радиомаяки систем слежения за перемещением объектов, сотовые телефоны, радиостанции и радиотелефоны (рис. 6.61).



Рис. 6.61. ST111 – детектор поля

Принцип действия ST111 основан на широкополосном детектировании электрического поля.

Основным изменением в ST111 по сравнению с предыдущей моделью ST110 является встроенная в основной блок СВЧ – антенна детектор.

SEL C-200 АРКАМ –электронный детектор скрытых видеокамер

Обнаружитель скрытых видеокамер SEL C-200 АРКАМ предназначен для мгновенного дистанционного обнаружения и поиска скрытых видеокамер и устройств, находящихся в активном состоянии (ведущих съёмку) (рис. 6.62).



Рис. 6.62. SEL C-200 АРКАМ –электронный детектор скрытых видеокамер

Детектор камер SEL C-2200 АРКАМ находит «паразитные» излучения, свойственные электронным цифровым схемам, которыми обладают любые видеокамеры и устройства получения, обработки (записи) и передачи видеоинформации.

В отличие от обнаружителей видеокамер, работающих по оптическому принципу или нелинейных локаторов, прибор SEL C-200 АРКАМ не требует пристального монотонного осмотра всего помещения, людей и предметов, а позволяет в течение считанных секунд определить наличие рядом с вами скрытой видеокамеры вне зависимости от её типа, камуфляжа и способа передачи видеоинформации.

Электронный детектор камер SEL C-200 АРКАМ отличается простотой управления, вместе с тем является по сути уникальным «карманным» высокоточным электронным измерительным комплексом, состоящим из скоростного измерительного приёмника электромагнитных помех (приёмника ЭМП), анализатора спектра сигналов и микро-ЭВМ для обработки данных.

Работа прибора SEL C-200 АРКАМ основана на обнаружении и анализе определённых участков электромагнитного спектра на предмет присутствия «паразитных» излучений, свойственных только электронным схемам видеокамер.

Обнаружив электромагнитные шумовые сигналы, похожие на паразитное излучение от видеокамер, SEL C-200 АРКАМ исследует и анализирует их по всем спектральным составляющим, сравнивая с «образами» сигналов, хранящимися в памяти прибора.

В изделии SEL C-200 АРКАМ предусмотрено самостоятельное формирование «белого» списка сигналов от локализованных «неопасных» источников — это позволяет автоматически исключать их при дальнейшей работе по поиску скрытых видеокамер.

Дальность обнаружения видеокамер зависит от электромагнитной обстановки в зоне поиска, а также характеристик источника (уровня сигнала, степени экранирования и т.п.) и может колебаться от 2 до 25 метров. Электронный обнаружитель скрытых видеокамер SEL C-200 АРКАМ является новейшей модификацией обнаружителей SP-102 Arcam и SEL SP-101 АРКАН. Его отличают повышенная чувствительность и уникальный цифровой алгоритм обнаружения информативного сигнала по уровню ниже уровня фонового шума.

Rohde& Schwarz®PR100 –мониторинговый приёмник

Портативный приемник R&S®PR100 был специально разработан для приложений радиомониторинга в полевых условиях. Функции приемника и концепция управления оптимизированы для задач мониторинга. Кроме того, его можно использовать для множества других приложений (рис. 6.62).



Рис. 6.62. Rohde& Schwarz®PR100 –мониторинговый приёмник

Приёмник R&S®PR100 работает в широком диапазоне частот от 9 кГц до 7,5 ГГц. Независимо от того, используется ли он для мониторинга излучения, обнаружения помех или обнаружения миниатюрных передатчиков, приемник всегда сочетает в себе высокую мобильность с максимальной простотой эксплуатации. Приемник и R&S®HE400 карманным направленная антенна вместе образуют компактную приемную систему. Приемник также можно использовать вместе с другими антеннами, например широкополосными все-направленными антеннами.

Основные возможности мониторингового приёмника Rohde&Schwarz®PR100:

- быстрое панорамное сканирование во всем диапазоне частот от 9 кГц до 7,5 ГГц;
- спектр ПЧ 10 МГц и демодуляция с полосой пропускания от 150 Гц до 500 кГц;
- отображение спектра и спектрограммы (водопада) на цветном экране 6,5 дюйма;
- сохранение данных измерений на встроенную SD-карту приемника;
- интерфейс LAN для удаленного управления и вывода данных;
- эргономичный и прочный дизайн для портативного использования;
- небольшой вес: 3,5 кг., включая аккумулятор;
- ручное определение источников с R&S®HE400 с портативными направленными антеннами (от 9 кГц до 7,5 ГГц);
- автоматическое определение местоположения источников излучения с помощью алгоритмов пеленгации (от 20 МГц до 6 ГГц);
- отображение цифровых карт на R&S®PR100;
- триангуляция на основе нескольких результатов пеленгования, определенных вручную или автоматически.

КРОНА-М12 – Портативный анализатор спектра реального времени

Анализатор спектра КРОНА-М12 предназначен для решения задач радиомониторинга, обнаружения и поиска новых и несанкционированных сигналов, исследования и регистрации сигналов в режиме реального времени. Позволяет осуществлять поиск подслушивающих устройств как в радиоэфире, так и в проводных коммуникациях и инфракрасном диапазоне (рис. 6.63).



*Рис. 6.63. КРОНА-М12 –портативный анализатор спектра
реального времени*

Основные возможности портативного анализатора спектра КРОНА-М12:

- сверхвысокая скорость сканирования – до 25 ГГц/ сек.;
- малые габариты и вес – выполнено в едином компактном экранированном корпусе;
- встроенные аккумуляторы обеспечивают автономную работу до 4 часов;
- режим «Водопад» позволяет оценить изменения с течением времени и обнаружить даже замаскированные сигналы;
- оснащается комплектом для обследования проводных линий и ИК диапазона;
- мультисенсорный дисплей позволяет управлять комплексом без дополнительных устройств ввода;
- возможно подключение клавиатуры и мыши для стационарной работы.

Программно-аппаратные средства защиты от несанкционированного доступа (НСД)

Secret Net– средство защиты информации от несанкционированного доступа

SecretNet является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие требованиям регулирующих документов: федеральных законов «О персональных данных», «О коммерческой тайне», № 5485-1-ФЗ «О государственной тайне».

Возможности:

- аутентификация пользователей;
- разграничение доступа пользователей к информации и ресурсам автоматизированной системы;
- доверенная информационная среда.

Особенности:

- контроль утечек и каналов распространения конфиденциальной информации;
- контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;
- затирание остаточной информации при освобождении и удалении областей памяти компьютера и запоминающих устройств;
- централизованное управление системой защиты, оперативный мониторинг и аудит безопасности;
- масштабируемая система защиты, возможность применения SecretNet (сетевой вариант) в организации с большим количеством филиалов;
- защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов (VDI).

Варианты развертывания SecretNet:

- автономный режим — предназначен для защиты небольшого количества (до 20-25) рабочих станций и серверов. При этом каждая машина администрируется локально;
- сетевой режим (с централизованным управлением) — предназначен для развертывания в доменной сети с ActiveDirectory. Данный вариант имеет средства централизованного управления и позволяет применить политики безопасности в масштабах организации. Сетевой

вариант SecretNet может быть успешно развернут в сложной доменной сети (domaintree/forest).

- сертифицированная система защиты информации накладного типа для автономных и сетевых АРМ (применима для сложных сетевых инфраструктур).

Предназначена для защиты конфиденциальной информации (редакции «К» и «С»), в том числе содержащейся в автоматизированных системах (АС) до класса защищенности 1Г включительно, в государственных информационных системах (ГИС) до 1 класса защищенности включительно, в информационных системах персональных данных (ИСПД) для обеспечения 1 уровня защищенности ПД, в автоматизированных системах управления производственными и технологическими процессами (АСУПП) до 1 класса защищенности включительно, а также для защиты информации, содержащей сведения, составляющие государственную тайну (редакция «С») до уровня «совершенно секретно» включительно.

Использование средств защиты информации необходимо в соответствии с закрепленными в приказах и руководящих документах регулятора группами мер, которые являются обязательными для выполнения:

- идентификация и аутентификация в информационной системе;
- управление доступом к компонентам информационной системы и информационным ресурсам;
- ограничение программной среды;
- регистрация событий безопасности в информационной системе;
- обеспечение целостности информационной системы и информации.

Указанные группы мер должны быть реализованы в ИСПД (приказ ФСТЭК России от 18.02.2013 № 21), в ГИС (приказ ФСТЭК России 11.02.2013 № 17), в АСУПП (приказ ФСТЭК России 14.03.2014 № 31), а также в автоматизированных системах классов 1Д и выше (Руководящий документ. Автоматизированные системы. Защиты от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации).

Ключевые особенности:

- сертификаты ФСТЭК России на соответствие требованиям регулятора к системам защиты информации от несанкционированного

доступа (СЗИ НСД), межсетевого экранирования (МЭ), системам обнаружения вторжений (СОВ), к средствам контроля съемных машинных носителей информации (СКН), а также к отсутствию недекларированных возможностей (НДВ);

- собственные сертифицированные механизмы управления информационной безопасностью, дублирующие (подменяющие) механизмы операционной системы (ОС) Windows;

- возможность применения в различных версиях и редакциях ОС MS Windows (от Windows XP до Windows 10) на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах, в виртуализированных средах.

Широкий набор дополнительных возможностей (помимо выполнения требований регуляторов к СЗИ НСД, МЭ, СОВ, СКН):

- контроль действий привилегированных пользователей;
- двухфакторная аутентификация с помощью аппаратных средств (USB-ключи, smart-карты);

- защита от утечек информации (элементы функциональности DLP-систем);

- «бесшовная» интеграция с другими решениями продуктовой линейки DallasLock;

- совместимость с решениями других производителей (InfowatchTrafficMonitor (ГК «InfoWatch»), Рутокен (закрытое акционерное общество (ЗАО) «Актив-софт»), AladdinToken (ЗАО «Аладдин Р.Д.»), Vipnet (открыто акционерное общество (ОАО) «ИнфоТеКС»), VPN/FW «Застава» (ОАО «Элвис-Плюс»), ESET NOD32 (общество с ограниченной ответственностью (ООО) «ИСС Дистрибьюшн»), ESMART Token® (Группа компаний ISBC);

- интеграция с SIEM-системами;
- расширенные возможности по централизованному управлению и построению надежных отказоустойчивых кластеров безопасности;

- элементы функциональности SIEM (графическое отображение статистики по событиям НСД).

Главной целью злоумышленника является получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т. д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав ин-

формации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе.

Защита информации ограниченного доступа представляет собой сложный процесс, охватывающий все стороны предотвращения утечки информации по любым каналам, которые могут существовать по объективным причинам или создаются преднамеренно для незаконного доступа к ней, вопросы исключения неправомерного использования сведений ограниченного доступа. Категории служебной информации ограниченного доступа имеют различную ценность (при утечке сведений разной категории масштаб последствий будет разным). Следовательно, требования к защите и организация защиты сведений разных категорий должны учитывать степень их ценности. Современная законодательная база Российской Федерации полностью устанавливает требования по защите, распространению (передаче) любой информации начиная с персональной и заканчивая государственной тайной. Также все федеральные законы в области информации предусматривают ответственность за нарушения в области информационной безопасности. Сотрудникам органов внутренних дел надлежит строго выполнять и соблюдать требования вышеуказанной нормативно-правовой базы.

В эпоху рыночной экономики это особенно актуально, где конкуренция является первостепенной составляющей, а добыча информации первым — это одна из гарантий успеха, причинение материального ущерба конкурентам или компроментация марки предприятия, организации (что, кстати, успешно реализуют Соединенные Штаты Америки в информационной войне против России).

Существование различных устройств шпионажа, которые работают по принципу радио закладки, лазерного луча для снятия вибраций с окон высокочастотного навязывания, прослушивания, доставляет значительные трудности обнаружения, устранения или защиты от них.

Как и средства защиты от хищения информации при совещаниях или переговорах активно развиваются в такт с новейшими технологиями, так и устройства шпионажа не стоят на месте. С каждым разом устройства становятся хитрее, непредсказуемее.

Если отделом безопасности руководит грамотный специалист, то составление организационного плана по защите информации на переговорах будет включать все аспекты для устранения угрозы.

Для проведения совещаний без каких-либо отрицательных последствий необходимо разрабатывать организационные и технические мероприятия. К организационным мероприятиям относятся: составления плана его проведения; рассмотрение наиболее подходящих помещений; контрольно-пропускной режим; состав участников; сроки проведения и длительность совещания; способы (методы) оповещения участников. К техническим мероприятиям можно отнести проверку измерительными приборами на наличие распространения неконтролируемых звуковых волн, установление защитных экранов и шумоподавления.

Таким образом, подчёркивая актуальность защиты информации, необходимо всем сотрудникам органов внутренних дел независимо от должности и звания серьезно подойти к вопросам защиты служебно и оперативно-значимой информации. Особое внимание на это следует уделять личному составу органов внутренних дел, непосредственно работающему с информацией и средствами получения, обработки, передачи и хранения как служебной, оперативно значимой информацией, так и с информацией, представляющей государственную тайну. Необходимо быть готовым к возможным попыткам злоумышленников похитить защищаемую информацию. Целесообразно на первоначальном этапе работы с информацией организовать работу личного состава. Правильная организация работы личного состава подразделений органов внутренних дел минимизирует риски, связанные с утечкой информации. В этих целях целесообразно периодически проводить профилактические и воспитательные беседы с личным составом подразделений по вопросам защиты информации. Также необходимо помнить о технических каналах утечки информации и каналах побочных электромагнитных излучений и своевременно применять перспективные специальные технические средства защиты.

Таким образом, государство, обладающее новыми технологиями в области защиты своих информационных ресурсов, будет способно

противостоять любым агрессиям, в том числе и военным. «Кто владеет информацией — тот владеет миром». Современная система защиты информации должна быть комплексной и включать как организационные, так и технические меры.

Вопросы и задания для самоконтроля

1. Классы угроз при рассмотрении потенциального риска утечки информации по каналам побочных электромагнитных излучений и наводок.
2. Разъяснить понятие «несанкционированный доступ к защищаемой информации».
3. Задачи обеспечения безопасности информации на организационном уровне.
4. Специальные технические средства выявления, сбора, передачи, приема и регистрация побочных электромагнитных излучений и наводок.
5. Принципы организации и функционирования системы безопасности.
6. Технические средства для съема информации с проводных линий связи.

ЗАКЛЮЧЕНИЕ

С каждым днём выражение «Тот, кто владеет информацией, тот владеет миром» или «Информированный человек, значит вооружённый» становится всё актуальнее. Развитие современного государства в мире невозможно без развития информационных технологий. Информационные технологии обуславливают значительное увеличение объема получаемой, обрабатываемой, передаваемой информации. Несмотря на это, человечество продолжает развивать информационные технологии во всех сферах. В последние десятилетия важность информации, а точнее, владение ею позволило некоторым развитым странам совершить существенный прорыв в области информационных технологий. Значительно возрос спрос на информацию определенного рода и применение её как в правомерных, так и неправомерных случаях.

Ввиду последних событий в мире, а именно возникновение очаговых вооруженных конфликтов, в том числе и на территории России, правительство вынужденно принимать меры, направленные на пресечение попыток получения информации незаконными способами. Такие меры должны распространяться и на силовые структуры государства — Вооружённые силы, Федеральную службу безопасности, Росгвардию, Министерство внутренних дел и другие ведомства с целью осуществления организационно-технических мероприятий, способствующих повышению уровня защиты информации, предотвращению утечки оперативно значимой или служебной информации органов внутренних дел.

При этом необходимо учитывать не только человеческий фактор, но и наличие и возможности современных технических и программных средств защиты информации. Современное специальное или специально созданное оборудование, а в большинстве случаев это шпионское оборудование, предназначенное для получения информации негласными, незаконными методами, позволяет снять или получить нужную для злоумышленника информацию двумя способами. Первый способ — это заинтересовать сотрудника в добровольной передаче информации путем подкупа (человеческий фактор — меркантильность). Но такой способ не всегда эффективен. Сотрудник полиции, владеющий служебной или другой информацией, относящейся к деятельности органов внутренних дел, в случае её незаконной передачи третьим лицам (заинтересованным или злоумышленни-

кам), осознает всю полноту последствий. В качестве второго незаконного способа получения информации с ограниченным кругом доступа к ней — это технические каналы утечки информации и побочные электромагнитные излучения. Этот способ считается наиболее эффективным при завладении незаконным образом сведениями, содержащими государственную тайну, служебную или оперативно значимую информацию. Он применяется злоумышленниками тайно, негласно, что практически делает его невидимым.

Возникает правомерный вопрос, а существуют ли способы защиты информации как от утечек по субъективным (то есть человеческий фактор), так и объективным причинам (например таких, как утечка информации по техническим каналам и каналам побочного электромагнитного излучения)? Практика показывает, что существует значительное количество средств, методов и способов защиты информации в информационных телекоммуникационных системах подразделений органов внутренних дел.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная

1. Бабаш, А.В. Информационная безопасность: лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – Москва: КноРус, 2019. – 432 с.
2. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. М.: Риор, 2020. – 400 с.
3. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – Москва: ДМК Пресс, 2019. – 474 с.
4. Ганиев, Р.Р. Исследование современных беспроводных систем обнаружения и предотвращения вторжения / Р.Р. Ганиев, И.С. Резников // Цифровой регион: опыт, компетенции, проекты. – 2019. – С. 150–153.
5. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – Москва: Инфра-М, 2020. – 64 с.
6. Ильина-Сидорова, И.А. Специфика защиты беспроводных сетей // Беспроводные технологии. – 2017. – № 2. – С. 50–53.
7. Маркина, С.А. Современные тенденции и проблемы цифровой трансформации / Маркина С.А., Артемов Р.В. // Вестник Академии знаний. – 2020. – №5 (40). – С. 267–268.
8. Остроух, А.В. Интеллектуальные информационные системы и технологии: монография / А.В. Остроух, А.Б. Николаев. – Санкт-Петербург: Лань, 2019. – 295 с.
9. Петров, С.В. Информационная безопасность: учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – Москва: АРТА, 2019. – 400 с.
10. Портникова К.В. Автоматизированные средства безопасности по защите информации в системе предприятия // Международный студенческий научный вестник. – 2020. – № 1. – С. 64–67
11. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В. Ф. Шаньгина. – Москва: Радио и связь, 2021. – 376 с.
12. Силаенков, А.Н. Проектирование системы информационной безопасности: учебное пособие – Омск: Изд-во ОмГТУ, 2019. – 126 с.
13. Синаторов, С.В. Информационные технологии: учебное пособие для средних специальных учебных заведений. – Москва: Дашков и К, 2019. – 448 с.
14. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие. – Москва: Форум, 2020. – 352 с.
15. Ямгуров Р.Р. Особенности российской защиты информации // Инновационная наука. – 2022. – №4-2. – С. 61–63.

Дополнительная

16. Baikal-T! – процессор российской компании Байкал Электроникс, основанный на ядрах MIPS Warrior P5600. URL: <https://www.ixbt.com/news/ht/188758> (дата обращения: 05.03.2023).

17. Численность населения России на 2022 г. URL: <https://www.vedomosti.ru> (дата обращения: 05.03.2023).

18. Инфографика: десятилетие утечек в США или почему случай с Facebook — это лишь верхушка теневого оборота данных в цифровую эпоху. URL: <https://www.infowatch.ru/analytics/reports/20159>. (дата обращения: 05.03.2023).

19. Интернет ресурс «Sudonull». URL: <https://sudonull.com/post/14689-5-Check-Point-for-maximum-Ips-Part-1> (дата обращения: 05.03.2023).

20. Интернет ресурс «Cloud Networks». URL: <https://cloudnetworks.ru/inf-bezopasnost/ids-ips/> (дата обращения: 05.03.2023).

21. Интернет ресурс Cloud. URL: <https://sbercloud.ru/ru/warp/blog/ips-ids-sistemy> (дата обращения: 05.03.2023).

22. Курманов Т. Н. Информационная безопасность локальных сетей // Студенческий форум. – 2022. – № 44. – С. 38–43.

23. Сайт компании «Juniper». URL: <https://www.juniper.net/ru/ru/research-topics/what-is-ids-ips.html> (дата обращения: 05.03.2023).

24. Сайт компании «GuardSite». URL: <https://www.guardsite.com/WIPS.asp> (дата обращения: 05.03.2023).

25. Сайт компании «AllTechnicalAssistance». URL: <http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/wips> (дата обращения: 05.03.2023).

26. Интернет ресурс «NetworkGuru». URL: <https://networkguru.ru/wireless-intrusion-prevention-system-wips-wifi/> (дата обращения: 05.03.2023).

27. Официальный сайт компании: «Эшелон комплексная безопасность» URL: <https://Npro-echelon.ru/production/65/11746> (дата обращения: 05.03.2023).

28. Сайт компании Акционерное общество (АО) «ЦБИ-сервис» [Электронный ресурс]: URL: <https://cbi-s.ru>.

29. Сайт компании ООО «ИНФОСЕКБЮР». URL: <https://infosecur.ru> (дата обращения: 05.03.2023).

30. Сайт компании «DetectorSystems» URL: <https://detsys.ru/> // HYPERLINK "https://detsys.ru/"detsys HYPERLINK "https://detsys.ru/". HYPERLINK "https://detsys.ru/"ru (дата обращения: 05.03.2023).

31. Сайт интернет-магазина «Kogr.org» URL: <http://kogr.org> (дата обращения: 05.03.2023).

Для заметок

Для заметок

Учебное издание

Мельников Николай Михайлович
кандидат технических наук
Никишкин Александр Владимирович
кандидат юридических наук
Ветрова Елена Викторовна

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Редактор *Свикиш Н.О.*
Компьютерная верстка *Свикиш Н.О.*
Дизайн обложки *Шеряй А.Н.*

ISBN 978-5-91837-832-8



EDN: YRZLSO



Подписано в печать 29.05.2024. Формат 60×84 ¹/₁₆
Печать цифровая 19,0 п. л. Тираж 100 экз. Заказ № 64/24

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1