Методы анализа угроз нарушения информационной безопасности ведомственного объекта информатизации

Учебное пособие

БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И. Д. ПУТИЛИНА

МЕТОДЫ АНАЛИЗА УГРОЗ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕДОМСТВЕННОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Учебное пособие

Санкт-Петербург
Наукоемкие технологии
2026

УДК 004.056.5:351.74
ББК 16.8
М54

Авторы:
В. Л. Акапьев, канд. пед. наук;
А. В. Борисенко, канд. физ.-мат. наук;
Е. Г. Ковалева, канд. техн. наук;
Е. А. Новикова, канд. юрид. наук;
Ю. А. Пироженко

Рецензенты:
Л. Д. Матросова, кандидат юридических наук, доцент, полковник полиции, начальник кафедры информационных технологий в деятельности ОВД Орловского юридического института МВД России имени В. В. Лукьянова;
Ю. А. Гончаров, заместитель начальника отдела специальной связи ЦИТСиЗИ УМВД России по Белгородской области

Акапьев, В. Л.
М54 Методы анализа угроз нарушения информационной безопасности ведомственного объекта информатизации: учебное пособие / В. Л. Акапьев, А. В. Борисенко, Е. Г. Ковалева, Е. А. Новикова, Ю. А. Пироженко. – СПб.: Наукоемкие технологии, 2026. – 104 с.

ISBN 978-5-00271-053-9

В пособии раскрываются основные теоретические понятия и практические подходы к обеспечению информационной безопасности объекта информатизации отдела Министерства внутренних дел Российской Федерации (ОМВД России).

Масштабное внедрение информационных технологий во все сферы человеческой жизни, активная цифровизация общества, вызывающие лавинообразный рост киберпреступности, вынуждают правоохранительные органы активизировать деятельность по пресечению угроз информационной безопасности в условиях цифровизации профессиональной деятельности.

Реализация столь сложной задачи невозможна без сформированной информационно-технологической компетентности сотрудников органов внутренних дел в части обеспечения информационной безопасности.

Издание способствует формированию знаний, умений, навыков и путей их реализации в области информационной безопасности как составного элемента профессиональной компетентности.

Пособие предназначено для курсантов, слушателей, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации и специалистов в области информационной безопасности.

ISBN 978-5-00271-053-9

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационная безопасность необходима для защиты конфиденциальных и ценных данных от несанкционированного доступа, использования, раскрытия, нарушения целостности, изменения или уничтожения.

Информационная безопасность помогает гарантировать, что критически важные функциональные операции будут продолжены в случае чрезвычайной ситуации, например, кибератаки или стихийного бедствия. Без надлежащих мер безопасности данные и системы организации могут быть скомпрометированы, что приведет к значительным простоям и снижению эффективности правоохранительной деятельности.

Кибератаки, такие как заражение вирусами, вредоносным программным обеспечением (ПО), фишинг и программы-вымогатели, становятся всё более изощрёнными и частыми. Информационная безопасность помогает предотвращать указанные атаки и минимизировать их последствия в случае их возникновения.

Организации также обязаны защищать данные о сотрудниках, такие как сведения о заработной плате, состоянии здоровья и личные данные. Эта информация часто становится целью киберпреступников, а ее кража может привести к краже личных данных и финансовому мошенничеству.

В мире цифровых технологий защита конфиденциальной информации стала не просто желательной, а необходимой. Информационная безопасность - это стратегии и технологии, используемые для предотвращения несанкционированного доступа, нарушения работы или кражи данных. Будь то здравоохранение, финансы, образование или государственное управление, организации полагаются на защищённые системы для поддержания доверия и операционной целостности. Но что такое информационная безопасность на практике и почему она так важна сегодня?

Информационная безопасность защищает цифровую и физическую информацию от несанкционированного доступа, использования, раскрытия, нарушения работы, изменения или уничтожения. Она направлена на защиту конфиденциальной информации путём обеспечения её конфиденциальности, целостности и доступности. Сфера её применения включает сетевую, прикладную и операционную безопасность, а также физический и административный контроль. Такой комплексный подход позволяет противостоять угрозам, начиная от кибератак и заканчивая человеческим фактором. Четкое понимание того, что такое информационная безопасность, помогает организациям применять эффективные меры для защиты активов и поддержания доверия.

Не менее важно соблюдение политики информационной безопасности правоохранительных органов, которая имеет решающее значение для защиты персональных данных, обеспечения бесперебойной работы и укрепления доверия общественности.

Информационная безопасность стала ключевым элементом работы правоохранительных органов. Рост числа киберпреступлений, распространение цифровых доказательств и растущая зависимость полиции от технологий сделали информационную безопасность критически важным компонентом защиты правоохранительных органов и их способности служить обществу и защищать его.

По мере того, как киберпреступники становятся всё более изощрёнными, правоохранительные органы должны укреплять собственную цифровую защиту, чтобы быть на шаг впереди, а также использовать информационную безопасность для борьбы с растущим числом киберугроз.

Информационная безопасность играет важнейшую роль в работе современных правоохранительных органов в эпоху цифровых технологий. Поскольку правоохранительные органы сталкиваются с растущим числом киберугроз и всё больше полагаются на цифровые инструменты и данные, информационная безопасность обеспечивает основу для стабильной работы, эффективности расследований информационных инцидентов, улучшения информационного обеспечения правоохранительной деятельности и защиты конфиденциальной информации.

Настоящее учебное издание посвящено рассмотрению общих положений обеспечения информационной безопасности и нормативных требований по ее обеспечению, а также определению возможных угроз для объектов информатизации подразделений органов внутренних дел (ОВД), методике оценки защищенности данной категории объектов и организации их комплексной защиты.

Пособие разработано в соответствии с Федеральным государственным образовательным стандартом высшего образования, основными образовательными и рабочими программами учебных дисциплин «Информационные системы, технологии и основы информационной безопасности органов внутренних дел» и «Основы кибербезопасности».

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Основные термины и определения

Конфиденциальная информация, такая как персональные данные, финансовая отчётность, коммерческая тайна и интеллектуальная собственность, должна быть надёжно защищена, чтобы не попасть в чужие руки. Такая информация представляет ценность и может быть использована для кражи личных данных, мошенничества или других злонамеренных целей.

Многие отрасли, такие как здравоохранение, финансы и государственное управление, подчиняются строгим нормативным требованиям и законам, которые обязывают их защищать конфиденциальные данные. Несоблюдение этих требований может привести к юридическим и финансовым санкциям, а также нанести ущерб репутации организации.

Правоохранительные органы всё чаще подвергаются атакам со стороны киберпреступников и недружественных государственных структур. Программы-вымогатели могут выводить из строя диспетчерские системы, утечка данных может поставить под угрозу конфиденциальных информаторов, а фишинговые атаки могут лишить сотрудников доступа к критически важным инструментам управления делами.

В связи с тем, что для эффективной защиты информации необходимо, чтобы и законодатель (разработчик руководящих документов в заданной области), лицо, ответственное за защиту информации на конкретных объектах, и контролирующий орган «говорили на одном языке», целесообразно определить и рассмотреть понятийную область, используемую в работе, на примере основных терминов и определений [55].

Информационная безопасность (InfoSec) - это защита важной информации от несанкционированного доступа, раскрытия, использования, изменения или нарушения. Она помогает обеспечить доступ к конфиденциальным данным организации для уполномоченных пользователей, а также сохранить конфиденциальность и целостность данных [20].

Нам необходимо защищать информационные активы, которые могут включать в себя финансовые, конфиденциальные, персональные данные, сведения ограниченного распространения или содержащие государственную тайну. Эти активы могут представлять собой цифровые файлы и данные, бумажные документы, физические носители и даже человеческую речь. На протяжении всего жизненного цикла данных InfoSec контролирует такие функции, как инфраструктура, программное обеспечение, тестирование, аудит и архивирование [18].

Информационная безопасность, основанная на принципах, которым уже несколько десятков лет, постоянно развивается, чтобы обеспечить защиту все более гибридных и мультиоблачных сред в условиях постоянно меняющегося ландшафта угроз. Учитывая, что характер этих угроз меняется, для

обновления технологий и процессов, используемых для защиты, необходимо взаимодействие нескольких команд [21].

Защита информации - это целенаправленная деятельность по предотвращению утечки защищаемой информации, а также по недопущению несанкционированных и непреднамеренных воздействий на нее [28].

Защита информации (или информационная безопасность, согласно определению Национального института безопасности и стандартов) - это защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения работы, изменения или уничтожения [69].

Технический канал утечки информации (ТКУИ) - представляет собой совокупность объекта разведки, технического средства разведки (ТСР), используемого для получения информации об этом объекте, и физической среды, в которой происходит распространение информационного сигнала [21].

Несанкционированный доступ к информации - это доступ к информации, осуществляемый с нарушением установленных правил разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Защита информации от утечки - это комплекс мер, направленных на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на создание существенных препятствий для получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

Защита информации от несанкционированного доступа - это защита информации, нацеленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами прав или правил разграничения доступа к защищаемой информации [24].

Техническая защита информации - это защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [59].

Физическая защита информации - это защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты [31].

Безопасность информации (данных) - это состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Безопасность данных представляет собой практику защиты цифровой информации от несанкционированного доступа, повреждения или хищения на протяжении всего жизненного цикла данных. Она включает физическую защиту оборудования и устройств хранения данных, а также

административный контроль и управление доступом. Кроме того, она охватывает логическую защиту программных приложений, организационные политики и процедуры [30].

Защищаемая информация - это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Объект информатизации - это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [12].

Защищаемый объект информатизации - это объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Объект защиты информации - это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Угроза (безопасности информации) - это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Охраняемые сведения - это сведения, содержащие государственную тайну или сведения, отнесенные к другой категории конфиденциальной информации.

Технический демаскирующий признак объекта - это характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.

Автоматизированная система (АС) - это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [13].

Средства вычислительной техники (СВТ) - это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Штатные средства - это совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Выделенное помещение (ВП) - это специальное помещение, предназначенное для проведения собраний, совещаний, бесед и других мероприятий речевого характера по секретным или конфиденциальным вопросам.

Способ защиты информации - это порядок и правила применения определенных принципов и средств защиты информации [61].

Фактор, воздействующий на защищаемую информацию - это явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Термины «информационная безопасность», «ИТ-безопасность», «кибербезопасность» и «защита данных» часто (и не совсем корректно) используются как взаимозаменяемые. Хотя эти области имеют точки пересечения и дополняют друг друга, они различаются, в первую очередь, по охвату решаемых задач.

Информационная безопасность - это общий термин, обозначающий меры, принимаемые организацией для защиты информации. Он включает физическую защиту ИТ-активов, защиту конечных устройств, шифрование данных, сетевую безопасность и многое другое [63].

Информационная безопасность также подразумевает защиту физических и цифровых ИТ-активов и центров обработки данных, но не включает защиту бумажных документов и других аналоговых носителей информации. Она ориентирована на защиту технологических активов, а не самой информации как таковой [17].

Кибербезопасность сосредоточена на защите цифровых информационных систем. Основная цель состоит в защите цифровых данных и активов от киберугроз. Несмотря на масштабность решаемых задач, сфера применения кибербезопасности ограничена, поскольку она не связана с защитой бумажных или аналоговых данных [60].

1.2. Информация, подлежащая защите

Для обеспечения эффективной защиты информации, с которой ведется работа в органах внутренних дел, необходимо, прежде всего, определить, какая же из всей циркулирующей в ОВД информации подлежит защите. При этом основные требования по защите информации будут непосредственно определяться степенью ее конфиденциальности [4].

Существуют различные признаки, по которым осуществляется классификация информации. С точки зрения организации защиты целесообразно начать с ее классификации по категории доступа [48].

В статье 5 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ указано: «Информация в зависимости от категории доступа к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами **(информация ограниченного доступа)**»[1].

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

государственной тайне, и конфиденциальную (в том числе, имеющую пометку «для служебного пользования»). Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне». Перечень сведений, отнесенных к государственной тайне, опубликован в ст. 5 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»[2]. Конкретные перечни сведений, подлежащих засекречиванию, разрабатываются и вводятся в действие соответствующими ведомственными приказами. Существует три степени секретности такой информации:

- особой важности;
- совершенно секретно;
- секретно.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Определение состава защищаемой информации представляет собой первоначальный этап построения системы защиты. От точности его выполнения зависит эффективность функционирования разрабатываемой системы. Общий подход состоит в том, что защите подлежит вся конфиденциальная информация, то есть сведения, составляющие государственную тайну, информация, составляющая коммерческую тайну, и служебная информация. При этом конфиденциальная информация должна защищаться от утечки и утраты [52].

К информации, нашедшей свое отражение в различных физических полях, относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, **информация ограниченного доступа**, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера или служебные сведения.

1.3. Перечень объектов защиты

Для обсуждения информации ограниченного доступа (совещаний, обсуждений, конференций, переговоров и т.п.) используются специальные помещения (служебные кабинеты, актовые залы, конференц-залы и т.п.),

[2] Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (последняя редакция) // СПС «КонсультантПлюс».

которые называются **выделенными помещениями (ВП)**. В выделенных помещениях часто устанавливаются вспомогательные технические средства и системы (ВТСС), которые непосредственно не задействуются для обработки конфиденциальной информации. Это, как правило, системы и средства городской автоматической телефонной связи, системы и средства охранной и пожарной сигнализации, системы и средства оповещения и сигнализации, системы и средства кондиционирования, системы и средства проводной радиотрансляции сети и приема программ радиовещания и телевидения, системы и средства электрочасофикации и иные технические средства и системы. Выделенные помещения располагаются в пределах **контролируемой зоны (КЗ)**, под которой понимается пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств [1].

Информация может существовать в различных формах в виде совокупности некоторых символов (знаков) на носителях различных типов. В связи со стремительным развитием информатизации общества все большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. Таким образом, АС представляет собой совокупность следующих компонентов:

- технических средств обработки и передачи информации;
- программного обеспечения;
- самой информации на различных носителях;
- обслуживающего персонала и пользователей системы.

Одним из основных аспектов проблемы обеспечения безопасности АС является определение, анализ и классификация возможных угроз информации, обрабатываемой в конкретной АС. Перечень потенциальных угроз, оценка их возможностей является основой для разработки модели злоумышленника, которая являются базовой информацией для построения оптимальной системы защиты [27].

1.4. Нормативные требования к обеспечению информационной безопасности

В процессе реализации действующих требований по обеспечению информационной безопасности (ИБ) на практике возникает один вопрос: какой результат мы получим, так как наша задача состоит не в выполнении бумажных требований, а в том, чтобы информационные системы компании или организации не были взломаны и действия по обеспечению информационной безопасности приносили необходимый результат?

А этот результат был оптимально достижим с тем, чтобы затраты на выполнение нормативных требований по ИБ не превышали тот потенциальный ущерб, который может быть в случае невыполнения этих требований. Основная задача: найти баланс между нормативными требованиями и результативной ИБ [53].

В так называемом «трехглавом» законе «Об информации, информационных технологиях и защите информации» четко оговаривается, что обладатель информации обязан принимать меры по защите информации. И только в отдельных случаях, которые установлены законодательством Российской Федерации, мы обязаны защищать информацию или какие-то иные информационные активы, как нам это предписывает государство, тот или иной государственный орган – регулятор, который определяет правила по ИБ[3].

Во всех остальных случаях, когда государство не устанавливает обязательных требований, обладатели информации вольны самостоятельно выбирать те стандарты, подходы, которыми они будут руководствоваться при построении, мониторинге, эксплуатации системы информационной безопасности в своей организации или предприятии[4].

Таким образом, требования по защите выбираются:

- на основе законодательных актов;
- на основе ведомственных стандартов и приказов;
- самостоятельно.

Основных законов по защите информации, принятых в Российской Федерации, на самом деле не так и много, потому что векторов регулирования всего семь [5]. В составе законодательных актов, устанавливающих обязательные требования по кибербезопасности, в первую очередь необходимо выделить Федеральный закон «О персональных данных» № 152-ФЗ, регламентирующий обязательные требования по защите персональных данных субъектов информационного взаимодействия[5]. Под него разработаны соответствующие подзаконные акты: постановления Правительства, ведомственные приказы и т.д. Причем необходимо обратить внимание на тот факт, что этот закон о персональных данных, а не о защите персональных данных.

Очень часто наши регуляторы подменяют два понятия: защита прав субъектов персональных данных и защита самих персональных данных. Защита персональных данных - это только небольшая часть от всего набора мероприятий, которые защищают наши права, ведь мы все субъекты персональных данных. Но иногда имеет место некий перекос: ведь защищать права у нас не всегда любят, умеют и хотят, а вот защитить некую сущность, установить какие-то ограничительные требования по защите самих

[3] Ст. 6 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[4] Ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[5] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

персональных данных и ответственность за утечки, связанные с персональными данными, законодатель всегда готов, поэтому буйным цветом расцветает наше законодательство.

При этом иногда регуляторы и законодатели подменяют некоторые термины, но специалисты в области информационной безопасности должны четко разбираться, в чём отличие защиты прав субъектов от защиты самих персональных данных [54].

Второе направление в области ИБ возглавляет так называемый «трехглавый» закон об информации, информационных технологий и защите информации[6]. Он является всеобъемлющим в том, что касается защиты информации, так как именно от него развивается правовое направление, связанное с защитой информации в государственных информационных системах, защитой государственных информационных ресурсов. Именно из него вытекает разработка, в частности, таких ключевых подзаконных актов, как Приказ ФСТЭК России от 11.02.2013 № 17[7] и Постановление Правительства РФ № 676 по вводу в эксплуатацию государственных информационных систем[8]. Указанный закон предшествует разработке модели угроз[9], согласованию модели угроз ФСТЭК И ФСБ[10], согласование технического задания по требованиям защиты информации и т.д.

Благодаря ему получила развитие тема баг-баунти[11], так как все публичные государственные информационные системы (ГИС) должны будут выноситься на программу по баг-баунти, прежде чем они будут введены в эксплуатацию [41].

Также необходимо выделить Федеральный закон № 187[12] со значительным количеством подзаконных актов по безопасности критической инфраструктуры[13]. Имеет место Федеральный закон № 161 по национальной

---

[6] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[7] Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // СПС «КонсультантПлюс».

[8] Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СПС «КонсультантПлюс».

[9] «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) // СПС «КонсультантПлюс».

[10] Постановление Правительства РФ от 18.09.2012 № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю» // СПС «КонсультантПлюс».

[11] Баг-баунти (от англ. bug bounty) - открытый конкурс по поиску уязвимостей в продукте.

[12] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // СПС «КонсультантПлюс».

[13] Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев

платежной системе[14] и в его составе статья 27, посвященная обеспечению защиты в платежных системах. Стоит отметить закон № 395-1 «О банках банковской деятельности»[15], который наделяет Центральный банк правом регулировать вопросы защиты информации в кредитных организациях, а кредитной организации обязаны эти требования выполнять. Конечно же есть закон о Центральном банке[16], который обязывает выполнять и некредитные финансовые организации требования ЦБ, согласованные с ФСТЭК и ФСБ по вопросам защиты информации [40].

Нельзя обойти стороной и нашумевший майский указ Президента № 250[17], который установил и новые требования по практической результативной ИБ, и требования по наличию заместителей генеральных директоров и руководителей организации, которые отвечают за кибербезопасность в организации, тем самым подняв тему информационной безопасности на более высокий уровень.

Имеется закон о коммерческой тайне[18], но он очень по касательной затрагивает проблему защиты информации, потому что, с одной стороны, да, есть коммерческая тайна и её надо соблюдать, защищать и т.д., но в законе чётко прописано, что требования по защите информации устанавливает сам обладатель, владелец этой самой коммерческой тайны. И хотя раньше в 2006 году были приняты для служебного пользования (ДСП) требования ФСТЭК по защите коммерческой тайны[19], они не получили широкого распространения. Складывается странная ситуация: есть коммерческая тайна и правообладатель готов защищать свои права в суде в случае ее утечки, но ему придётся самостоятельно реализовывать режим коммерческой тайны и самостоятельно разрабатывать меры по защите этой самой коммерческой тайны, хотя можно ориентироваться и на существующие приказы ФСТЭК и ФСБ, взяв из них то, что лучше всего подходит для решения конкретных задач [38].

Существует закон № 5485-1 «О государственной тайне»[20], который важен и нужен для тех специалистов, которые обрабатывает сведения, составляющие государственную тайну.

значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изм. и доп., вступ. в силу с 21.03.2023) // СПС «КонсультантПлюс».

[14] Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[15] Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1 (последняя редакция) // СПС «КонсультантПлюс».

[16] Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ// СПС «КонсультантПлюс».

[17] Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

[18] Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[19] «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006 г. // СПС «КонсультантПлюс».

[20] Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (последняя редакция) // СПС «КонсультантПлюс».

Стоит упомянуть Проект указа по государственной системе защиты информации[21], который 23 января 2023 года был размещен на Федеральном портале проектов нормативных правовых актов (regulation.gov.ru). В случае его принятия законодательная сфера в области информационной безопасности получит дополнительное ускорение, потому что Проект распространяется не только на организации, которые являются государственными (госкорпорации, госорганы, муниципальные организации и др.), он распространяет требования по защите информации на все организации, обрабатывающие информацию, обладателям которой является государство, то есть и на коммерческие в том числе. Соответственно, в состав этих требование войдет и аттестация, и обязательная сертификация, и т.д.

Идет речь если не о переделе рынка информационных услуг, то о необходимости коммерческих организаций, которые сотрудничали с государством, но защищали информацию так как считали нужным, кардинально пересматривать свои отдельные подходы и требования по защите информации.

Необходимо остановиться на основополагающих приказах, детально описывающих Требования по информационной безопасности. Стоит начать с приказа № 17 ФСТЭК по защите государственных и муниципальных информационных систем. Документ публичный и доступен как на сайте ФСТЭК, так и на сайтах различных правовых систем. Практика подсказывает, что лучше ориентироваться на сайты правовых систем, так как на них документы размещены в более актуальной версии, не содержащие каких-либо ошибок. Нужно признать, что на сайтах регуляторов далеко не всегда документы своевременно и оперативно обновляются, и там иногда встречаются отдельные ошибки.

Приказ № 21 ФСТЭК регулирует защиту персональных данных, обрабатываемых в информационных системах персональных данных[22]. Он применяется для всех коммерческих операторов персональных данных, потому что для государственных структур, в которых персональные данные обрабатываются в ГИС, применяются требования приказа № 17 ФСТЭК.

Помимо приказа № 21 ФСТЭК по линии персональных данных действует еще ряд документов других регуляторов. Например, у Минцифры по биометрическим персональным данным издан приказ № 930[23].

---

[21] Проект Указа Президента РФ «Об утверждении Положения о государственной системе защиты информации в Российской Федерации» (по состоянию на 23.01.2023) // СПС «КонсультантПлюс».

[22] Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс».

[23] Приказ Минцифры России № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» // СПС «КонсультантПлюс».

Приказ № 31 ФСТЭК[24] по защите информации в информационных системах, связанных с оборонно-промышленным комплексом. В отличие от трех предыдущих документов, которые являются открытыми, этот приказ относится к категории ограниченного доступа.

Приказы № 235[25] и № 239[26] ФСТЭК России устанавливают требования к созданию субъектами критической информационной инфраструктуры (КИИ) Российской Федерации систем безопасности значимых объектов КИИ и по обеспечению их устойчивого функционирования.

Приказ № 378 ФСБ России по криптографической защите персональных данных[27].

Приказ № 524 ФСБ по криптографической защите информации в государственных информационных системах[28]. Необходимо обратить внимание на нестыковки данного документа с приказом № 17 ФСТЭК в части классификации информационных систем, поэтому на практике не просто сочетать эти два документа.

Отдельную группу представляют национальные стандарты в области кибербезопасности, разработанные банком России. Начнем с ГОСТ 57580.1[29], устанавливающего базовый набор защитных мер для финансовых кредитных и некредитных организаций. По своей сути и идеологически он не имеет значительных отличий от требований ФСТЭК и расходится только в количестве этих требований: в приказах ФСТЭК их насчитывается порядка 160 – 190, в зависимости от приказа, а у ЦБ их около 400. Сами требования почти идентичны, но различия заключаются в уровне детализации и разъяснениях по реализации заявленных требований [5].

Также имеют место отдельные положения Банка России по частным вопросам защиты информации в различных контурах: при переводе денежных средств, в рамках национальной платёжной системы, в кредитных и не кредитных финансовых организациях, на участке платежной системы банка

[24] Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // СПС «КонсультантПлюс».

[25] Приказ Федеральной службы по техническому и экспортному контролю от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // СПС «КонсультантПлюс».

[26] Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

[27] Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // СПС «КонсультантПлюс».

[28] Приказ ФСБ РФ от 24.10.2022 № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» // СПС «КонсультантПлюс».

[29] ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 04.03.2025).

России и т.д. В таких документах, которых достаточно много, указаны базовые требования, обязательные для всех, и отсылка на выполнение требований ГОСТа 571780.1.

Есть основания считать, что в текущем году многие документы ЦБ обновятся в части обязательных ссылок на принятые в конце декабря 2022 года два ГОСТа 57580.3[30] и 575804[31], соответственно регулирующие вопросы операционной надежности и нейтрализации рисков реализации информационных угроз. Указанные ГОСТ формируют, с точки зрения Центрального Банка, две линии обеспечения кибербезопасности.

Нельзя не упомянуть международные требования стандарта PCI DSS[32] от PCI council, требования SWIFT Cyber Security Program, которые распространяются на финансовые организации, подключенные к SWIFT, и другие очень узкие или отраслевые требования, которые нельзя отнести к всеобъемлющим и представляющим интерес только для организаций, работающим в конкретной сфере деятельности.

Таких подходов, стандартов и проектов передового опыта может быть достаточно много. Это могут быть и российские требования, и зарубежные, которых значительно больше, потому что за рубежом подход к организации информационной безопасности отличается от отечественного: помимо чисто обязательной истории, применимой к отдельным видам организаций, есть и большой пласт энтузиастов – коммерческих и некоммерческих организаций, которые разрабатывают какие-то лучшие практики[33] и учат их сочетать с требованиями законодательства. Так сложилось исторически, что в России инициативных разработчиков, да и самих общепризнанных стандартов, не так много [6].

Хотя в последнее время такая гитхабификация в отрасли ИБ происходит в России и появляются сообщества, которые ставят перед собой задачу разработки проектов в области информационной безопасности, которые не противоречат требованиям российского законодательства, так как в текущей геополитической ситуации западные стандарты нам не всегда подходят[34].

Все в значительной степени зависит от развивающейся в мире ситуации, но необходимо помнить, что, если государство не установило какие-то обязательные требования, либо эти требования не полны, специалисты и руководители должны ориентироваться на иные практики и рекомендации в

[30] Национальный стандарт РФ ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200194981 (дата обращения: 18.03.2025).

[31] ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200194982 (дата обращения: 22.03.2025).

[32] PCI DSS (Payment Card Industry Data Security Standard) - стандарт безопасности данных индустрии платежных карт.

[33] Лу́чшая пра́ктика (англ. best practice) - формализация уникального успешного практического опыта.

[34] Гитхабификация Информационной Безопасности // https://habr.com/ru/companies/microsoft/articles/487584/

области ИБ, которые в достаточно большом количестве по разным направлениям существует в мире.

К лучшим практикам (стандартам) с требованиями по защите принято относить:

ISO 270xx[35];
NIST CSF[36];
ASD 4 / 8 / 37 защитных мер;
CIS Controls (Top 20)[37];
CoBIT;
ITIL;
O-ISM3;
и другие.

Исторически одними их первых в России появились Требования по защите информации в государственных информационных системах[38], которые в дальнейшем были расширены на муниципальные информационные системы и на все системы, обрабатывающие информацию, собственником которых является государство. Такие действия указывают на то, что государство хочет контролировать и устанавливать требования в отношении тех информационных активов, которыми оно обладает. При этом не важно, где эти активы располагаются: в государственных органах, муниципальных структурах или коммерческих организациях.

При наличии требований и стандартов возникает вопрос: как определить требования по защите? Проблема в том, что регулирующие документы не содержат сплошной перечень требований, так как их набор зависит от ряда условий. В основном определяющими, какие требования по защите необходимо реализовать, являются два условия:

- актуальные угрозы;
- значимость или ценность информационной системы или обрабатываемой в ней информации.

Соответственно, в зависимости от того, как будут определены актуальность угроз и значимость информации, будет получен класс, уровень или категория информационной системы или объекта информационной инфраструктуры. Если речь идет о персональных данных, то это Постановление Правительства № 1119[39], в котором говорится о том, что существуют уровни защищённости персональных данных. В случае со 149-ФЗ

[35] ISO/IEC 27000 - серия международных стандартов, включающая стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC).
[36] NIST Cybersecurity Framework (CSF) - это добровольная платформа, которая состоит из стандартов, рекомендаций и рекомендаций по управлению рисками, связанными с кибербезопасности.
[37] CIS TOP 20 Controls - это базовый набор действий, которые в совокупности нацелены на защиту от наиболее распространенных атак на предприятия и их системы безопасности.
[38] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (в редакции приказа ФСТЭК России от 15.02.2017 № 27, от 28.05.2019 № 106) // СПС «КонсультантПлюс».
[39] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс».

и, соответственно, с приказом № 17 ФСТЭК речь идет о классах защищённости, например, ГИС, АСУТП. В ГОСТах Центрального Банка речь также идет о классах защищенности. В отношении информационных систем персональных данных (ИСПДн) – это уровни защищенности.

Когда речь заходит об объектах критической информационной инфраструктуры, то, опираясь на Постановление Правительства № 127[40], необходимо определять категории значимости объектов критической информационной структуры (КИИ) от одной до трёх. Существует и четвертая категория, к которой относят незначимые объекты, на которые каких-то обязательных требований в области законодательства по информации защите не распространяется, но, если этот объект относится и к ИСПДн, и к какому-либо классу АСУТП или ГИС, на него будут в обязательном порядке распространяться соответствующие требования к ИСПДн, АСУТП, ГИС, либо требование ГОСТа Банка России.

Соответственно, в каждом из ранее упомянутых приказов или иных уровней нормативных актов описана процедура определения актуальности угрозы. Это может быть либо высокоуровневая процедура, как в Постановлении Правительства № 1019, либо детальная процедура как в методике оценки угроз ФСТЭК, либо пока не очень детальная процедура оценки рисков как в документах Центрального банка.

Но каждая из этих процедур позволяет определить перечень того, что является для нас недопустимым, то есть какие недопустимые события требуется сделать невозможными в нашей организации. В дальнейшем можно будет определить, как эти недопустимые события, эти угрозы могут быть реализованы в нашей инфраструктуре и какие элементы инфраструктуры будут задействованы, то есть какие целевые ключевые системы может задействовать хакер, чтобы осуществить несанкционированное воздействие в отношении конкретной инфраструктуры, бизнеса или госуправления [4].

Затем по простой процедуре, описанной в документах регуляторов, определяется значимость или ценность систем или информации и, опираясь на эти два параметра, регуляторы предлагают очень простую формулу определения конкретного уровня защищенности или класса защищенности, для которого предлагается (не требуется, а предлагается) выбирать защитные меры.

И это достаточно важный момент, который следует рассмотреть отдельно, так как описанные выше четыре или три класса защищенности информационных систем – это очень грубая трактовка. Очевидно, что на практике системы очень разные. И, даже работающие в одной сфере системы, могут иметь различную реализацию, использовать разные информационные технологии, разные правила политики ИБ и т.д. Поэтому невозможно унифицировать все действия по обеспечению информационной безопасности,

[40] Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СПС «КонсультантПлюс».

как невозможно заставлять всех их выполнять. В этом как раз и заключается некая свобода творчества, которую предоставили все регуляторы администрации и специалистам в области информационной безопасности [5].

Раньше такого не было и где-то до 2012 года действовали жесткие требования, которые надо было реализовывать в любых случаях. Например, действовало правило ФСТЭК, по которому пароль должен быть не менее восьми символов. Возникала проблема: как на смартфоне или телефоне, с помощью которых ведется обработка персональных данных, имеющих пин, максимум, из четырех символов, выполнить требование на восемь символов? То есть физически выполнить это требование на подобных устройствах было невозможно. Естественно, что перечень таких примеров можно продолжать очень долго. Возникали десятки-сотни различных ситуаций, поэтому регуляторы пошли навстречу и приняли решение, согласно которому будет предложен каталог защитных мер, из которого можно выбирать то, что важно, нужно, полезно, релевантно и позволит выполнить требования законодательства и защититься от угроз недопустимых событий.

Но, поскольку далеко не все обладают нужной квалификацией, чтобы самостоятельно выбрать из двухсот или четырехсот, если речь идет о Центральном Банке, защитных мер релевантные, регуляторы пошли по пути разработки базового, или рекомендуемого, набора защитных мер, тем самым оказывая помощь, на что стоит ориентироваться, если субъект ИБ не готов тратить время, ресурсы на составление своего уникального перечня защитных мер, которые подходят именно ему.

Поэтому в настоящее время сформировалось два пути выбора защитных мер. Первый заключается в том, чтобы взять базовый набор средств ИБ и его реализовывать. Второй вариант - сделать нечто под себя и реализовывать то, что адекватно для конкретной структуры. Тем самым находится некий баланс между требованиями законодательства и затратами на его реализацию.

Но есть и второй вопрос. Практически во всех документах говорится о необходимости включения в базовый набор защитных мер защиту Wi-Fi, но, если нет Wi-Fi, зачем его туда включать? Зачем реализовывать мероприятия по мониторингу беспроводного эфира, внедрению беспроводных систем обнаружения вторжения, разграничения доступа и так далее?

Приведенные примеры показывают, почему не всегда срабатывает базовый набор, поэтому в ряде случаев, а, может быть, и в большинстве случаев, рекомендуется самостоятельно разработать набор защитных мер и, в случае с Wi-Fi, его просто исключают из базового набора, потому что такая технология не используется.

Возможны различные решения и, главное, все действующие сегодня приказы, стандарты, требования позволяют реализовать этот подход. Ошибочно рассуждать о том, что регулирующие документы не позволяют реализовать те или иные меры защиты информации. Это не так. Документы позволяют реализовать всё, что необходимо, просто с ними надо внимательно работать и с их помощью реализовать защитную меру. Не внедрить какой-то продукт, а реализовать защитную меру, а она может быть реализована по-

разному: и с помощью продуктов, и сервисов, и т.д. Конечно, проще всего применять готовый инструментарий, который автоматизирует рутинные задачи и обладает всеми необходимыми регалиями от регуляторов, либо по линии ФСТЭК, либо по линии ВСБ, либо по линии Минобороны в зависимости от какие требования на принимаемые решения распространяются.

Данное решение принимается на усмотрение субъекта ИБ, который может использовать любой из описанных сценариев за редким исключением, когда устанавливается, что для решения той или иной задачи необходимо применять определенный класс продуктов или этот класс продуктов должен соответствовать определенным требованиям и требуется подтверждение выполнения указанных требований.

Такое подтверждение может быть реализовано самостоятельно в виде добровольной сертификации, или оценки соответствия, или испытания. Либо это обязательная сертификация, когда необходимо сдать в испытательную лабораторию, имеющую аккредитацию ФСТЭК, либо Минобороны, либо ФСБ, и будут проведены все необходимые испытания и выдан сертификат о соответствии предъявляемым требованиям.

Необходимо учитывать требования различных устанавливающих документов. В некоторых предъявляются требования к реализации той или иной защитной меры, но, в большинстве случаев, принятие решения остается за субъектом ИБ, потому что заранее не всегда можно жестко прописать способы защиты той или иной информации, информационной системы, того или иного процесса и в этом плане творческий подход помогает реализовывать, с одной стороны, требования законодательства, с другой стороны, сделать это сбалансированно с учетом имеющихся ресурсов и возможностей хакеров, которые против вас действуют [6].

И, наконец, а что, если ничего не делать? Этот закономерный вопрос, который в Российской Федерации звучит не только в части кибербезопасности, имеет также очевидный ответ: все под ответственность субъекта ИБ.

Действующее законодательство предусматривает:

- административную ответственность (ст. ст. 13.11, 13.12, 19.5, 19.7 КоАП);
- уголовную ответственность (ст. ст. 137, 138, 159, 183, 272 – 274, 171 УК РФ);
- дисциплинарную ответственность (ст. ст. 81, 90, 195, 237 ТК РФ);
- гражданскую ответственность (ст. 1095 ГК РФ).

На практике самый распространенный вариант связан с наступлением административной ответственности. В Кодексе Российской Федерации об административных правонарушениях имеются отдельные статьи, которые за невыполнение требований по информационной безопасности предусматривают штрафные санкции. В настоящее время планируется введение оборотных штрафов за, например, утечки персональных данных, что может радикально изменить сложившуюся ситуацию.

Существует уголовная ответственность за нарушение правил эксплуатации объектов КИИ при нанесении ущерба таким объектам, за утечки информации, за нарушения финансовой, налоговой, банковской и иных видов тайн. Имеет место дисциплинарная ответственность, но это уже внутренняя дело каждой организации. Законодательством предусмотрена гражданская ответственность, которая не так часто применяется в области информационной безопасности.

При этом надо понимать, что существует законодательство, а есть правоприменительная практика, которая имеет свою специфику. Поэтому необходимо учитывать все факторы для построения сбалансированной, как с точки зрения законодательства, так и с точки зрения фактической результативной действенности, системы информационной безопасности.

Специалисты в области ИБ для построения эффективной системы безопасности предлагают дорожные карты, включающие в свой состав следующие элементы:

- определение недопустимых событий;
- определение целевых и ключевых систем;
- усиление защищенности с целью снижения рисков от возможных угроз (харденинг) инфраструктуры;
- модернизация бизнес-процессов;
- выстраивание мониторинга и реагирования;
- обучение работников;
- проведение регулярных киберучений, которые проверяют насколько процесс обучения был эффективен и появились ли у сотрудников навыки безопасности;
- внедрение программы непрерывного измерения эффективности и оптимальности информационной безопасности;
- поддержание цифровой устойчивости;
- внешняя оценка системы через Bug Bounty.

С одной стороны, такая дорожная карта позволит выполнить требования законодательства и защитить себя от таких недопустимых событий, как административное и уголовное наказание, а, с другой, создаст условия для развития собственного бизнеса и сегмента оказания электронных услуг государством юридическим и физическим лицам, то есть баланса между двумя сторонами.

Вопреки сложившемуся мнению в действующем законодательстве имеется немалое количество примеров, отражающих не «бумажную», а реальную информационную безопасность. В нем отражаются требования определить самое важное с точки зрения реализации системы ИБ, требования по построению центра противодействия киберугрозам. Не просто SOC[41], который в основном занимается мониторингом, а именно центр противодействия, который помимо мониторинга включает в себя и харденинг, и защиту, и реагирования.

[41] Центр мониторинга информационной безопасности (Security Operations Center, SOC).

В разных документах прописаны эти требования и, конечно же, требования по оценке результативности ИБ в виде киберучений, в виде планов реагирования, в виде пентестов, поисков уязвимости, непрерывного мониторинга и так далее. Необходимо обратить внимание, что рассмотренные нормы и документы, в том числе измененные в 2022 году и, которые будут еще изменяться в дальнейшем, уже содержат немалое количество пунктов и требований по результативной ИБ.

Знание нормативной базы, регламентирующей реализацию мероприятий по обеспечению информационной безопасности, позволит решить проблему кибербезопасности организации наиболее эффективно и с наименьшими затратами [34].

Вопросы и задания для самоконтроля:

1. Сформулируйте свой подход к понятию «информационная безопасность».
2. В чем, с Вашей точки зрения, заключается необходимость защиты информации?
3. Дайте определение техническим каналам утечки информации.
4. В чем, с Вашей точки зрения, заключается сущность «несанкционированного доступа к информации»?
5. Какие меры, с Вашей точки зрения, направлены на предотвращение неконтролируемого распространения защищаемой информации?
6. В чем сущность технической защиты информации?
7. Сформулируйте свое видение безопасности информации.
8. Каким образом выделить защищаемый объект информатизации?
9. В чем заключается сущность угрозы безопасности информации?
10. Как определить демаскирующий признак объекта защиты?
11. В чем заключается принципиальная разница между понятиями «информационная безопасность» и «кибербезопасность»?
12. Определите фактор, воздействующий на защищаемую информацию.
13. Какая информация подлежит защите?
14. Классифицируйте информацию, подлежащую защите.
15. Перечислите задачи, которые необходимо решить для достижения цели информационной безопасности Российской Федерации.
16. Опишите основное содержание Доктрины информационной безопасности Российской Федерации.
17. Опишите основное содержание Стратегии национальной безопасности Российской Федерации.
18. Опишите основное содержание 149-ФЗ – главный закон об информации в России.
19. Опишите основное содержание федерального закона от 21.07.1993 № 5485-1-ФЗ «О государственной тайне».
20. Охарактеризуйте основное содержание федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

21. В чем заключается основное содержание федерального закона от 6.04.2011 № 63-ФЗ «Об электронной подписи»?

22. В чем заключается основное содержание федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»?

23. В чем заключается основное содержание указа Президента РФ № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»?

24. Сформулируйте понятие и приведите классификацию стандартов в области информационной безопасности.

25. Дайте характеристику стандартов группы ISO/IEC 27000.

26. Какие органы исполнительной власти являются ключевыми в области технической защиты информации?

27. Что такое сертификация, сертификат соответствия?

28. Дайте понятие системе сертификации.

29. Перечислите участников системы сертификации.

30. Дайте понятие обязательной и добровольной сертификации.

31. На соответствие какому стандарту осуществляется сертификация системы управления (менеджмента) информационной безопасности?

32. В чем, с Вашей точки зрения, заключаются организационные методы обеспечения безопасности информации?

33. Сформулируйте основные положения политики безопасности организации.

ГЛАВА 2. ОПРЕДЕЛЕНИЕ ВОЗМОЖНЫХ УГРОЗ ДЛЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

2.1. Угрозы безопасности информации

Угроза безопасности информации – потенциальное возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации. Возможности источников, создающих угрозу безопасности информации, обусловлены совокупностью способов несанкционированного и (или) случайного доступа к информации, в результате которого возможно нарушение конфиденциальности, целостности и доступности. А именно:

1. Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой закрытой информации, хранящейся в информационной системе или участвующей в информационном обмене между взаимодействующими системами.
2. Угрозы нарушения целостности – это угрозы, связанные с вероятностью изменения информации ограниченного доступа, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования;
3. Угрозы доступности (осуществление действий, препятствующих реализации права санкционированного доступа к информационным ресурсам). Нарушение доступности выражается в создании таких условий, при которых доступ к информации будет блокироваться или будет возможен за время, которое не обеспечит выполнение служебных задач [4].

Носителями угроз безопасности информации являются источники угроз. Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной появления угрозы безопасности информации. Источники угроз преследуют при этом следующие цели: ознакомление со сведениями ограниченного распространения, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба [27].

С учетом наличия прав доступа и возможностей осуществления несанкционированного доступа к информации и (или) к объекту информатизации все источники угроз информационной безопасности подразделяются на два типа:

– внешние нарушители (тип I) – лица, не имеющие права доступа к объекту информатизации и реализующие угрозы безопасности информации из-за границ информационной системы;

– внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе и ее структурным блокам.

Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые оператором организационные меры по допуску субъектов к работе в информационной системе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц.

Для внешнего нарушителя необходимо рассматривать все возможные угрозы безопасности информации, после чего определить список актуальных угроз и принять меры по обеспечению защиты информации [10].

На рисунке 2.1 приведена классификация угроз безопасности информации по используемой уязвимости:

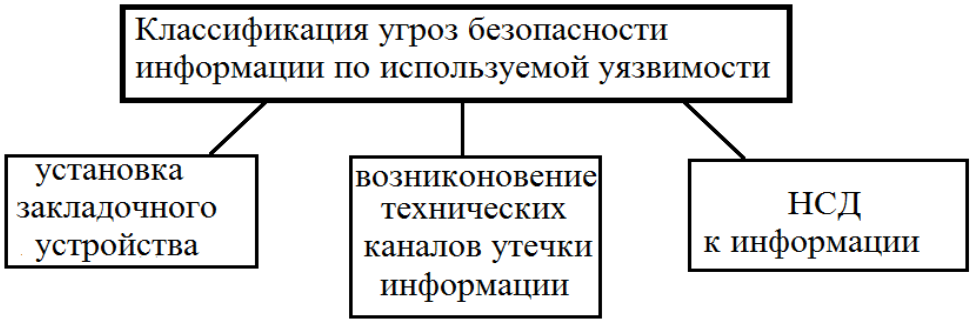

Рис. 2.1. Классификация угроз безопасности информации по используемой уязвимости

Каждая из представленных видов угроз безопасности информации (БИ) характеризуется понятием, основными особенностями и средством перехвата информации. Проведение детального анализа выявленных угроз позволит сформировать представление о реальных возможностях злоумышленника при осуществлении им попыток получения закрытой информации.

2.2. Угроза безопасности информации, возникающая вследствие установки закладочного устройства

Закладочное устройство – элемент средства получения информации, скрытно внедряемый 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). Знание конструктивных особенностей и схемных решений построения закладочных устройств позволяет выявить их сильные и слабые стороны и выбрать оптимальные способы противодействия [29].

Закладочные устройства можно классифицировать по нескольким признакам:

– радиозакладочные устройства, излучающие в эфир;

– закладочные устройства, не излучающие в эфир (с передачей перехваченной информации по каналам передачи данных, сетям управления, питания и т.д.).

В первую группу входят радиозакладочные устройства, предназначенные для получения аудиоинформации по акустике помещения, телевизионные закладочные устройства, предназначенные для получения аудио- и визуальной информации, и радиозакладочные устройства в телефонных линиях связи, устройствах обработки и передачи информации, сетях питания и управления. Передача перехваченной информации происходит радио- или телевизионным радиосигналом.

К закладочным устройствам с передачей информации без излучения в эфир можно отнести группу закладочных устройств в линиях связи, питания, управления и охранной сигнализации с использованием этих линий связи для передачи перехваченной информации.

Существенное значение для организации каналов передачи перехваченной информации в радиодиапазоне имеет антенная система, используемая в закладочном устройстве. В качестве таковой могут быть использованы: а) собственное антенное устройство, б) случайная антенна. В качестве собственной антенны используется, как правило, четвертьволновая антенна, имеющая круговую диаграмму направленности, что способствует реализации злоумышленником попыток съема информации, так как не требует выполнения особых условий для установки аппаратуры перехвата, однако размеры антенны зависят от используемого диапазона. Зачастую ситуация кардинально меняется, если в качестве передающей антенны используются участки линии передач, в которые монтируются закладочные устройства, так называемые случайные антенны [9].

Сеть электропитания здания и ее компоненты могут быть использованы злоумышленником для установки и питания закладочных устройств, а также передачи перехваченной информации. Проводные системы скрытого аудиоконтроля используются для негласного получения и передачи аудиоинформации по проводным линиям. Прием сигналов аудиоинформации осуществляется специальными приемниками. Закладочные устройства могут быть закамуфлированы под розетку, различные переходники, в лампах, электрических светильниках, торшерах и т.п.

Одной из существенных особенностей закладочных устройств, передающих по сети электропитания, является неограниченное время их работы. Замаскированные под широко используемые в быту и работе предметы, такие как удлинители, тройники, настенные лампы и другие бытовые электроприборы, закладочные устройства могут работать достаточно долгое время, не вызывая подозрений.

Съем информации, обрабатываемой в технических средствах и системах, возможен путем установки в них электронных устройств перехвата информации. Данные устройства представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Электронные устройства перехвата информации, устанавливаемые в технических средствах,

называют аппаратными закладочными устройствами [25]. Наиболее часто такие закладочные устройства устанавливаются в технических средствах иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью ЗУ информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а затем по команде передается на контрольный пункт перехвата.

2.3. Технические каналы утечки информации

Под техническим каналом утечки информации понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал (рис. 2.2) [15].

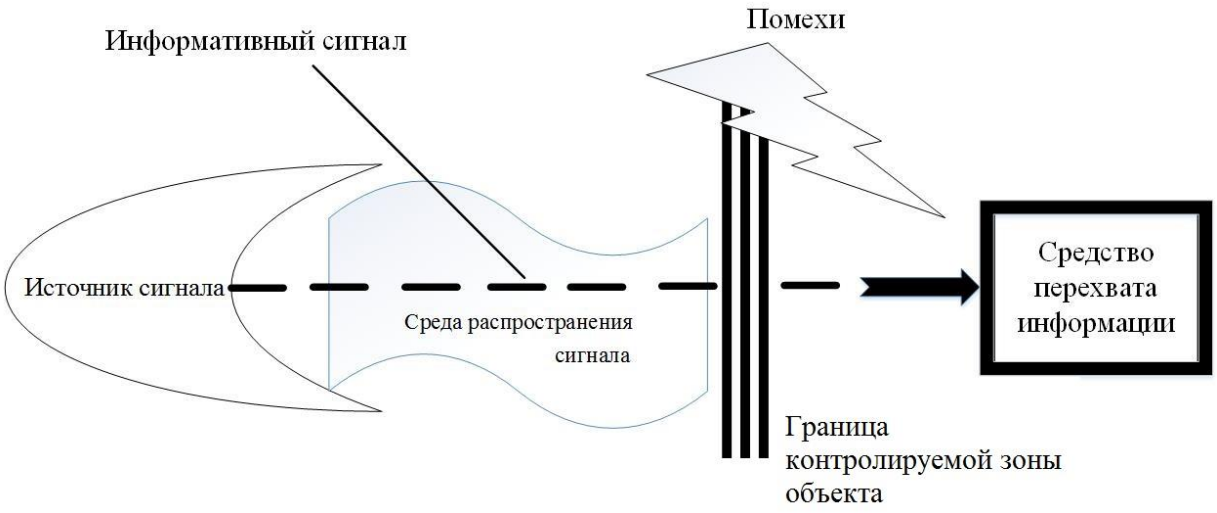

Рис. 2.2. Схема технического канала утечки информации

Другими словами, под техническим каналом утечки информации понимают способ получения с помощью технического средства разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления. Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т.д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

Защита информации от утечки по техническим каналам – это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны [46].

В основе утечки информации лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных и других полей, и материальных объектов от источника к средству разведки.

Причины и условия утечки информации при всех своих различиях имеют много общего. Причины утечки информации связаны, как правило, с нарушением норм (требований) по защите информации (в том числе и за счет человеческого фактора), отступлением от правил обращения с руководящими документами, техническими средствами, образцами продукции и другими материалами, в той или иной степени содержащими конфиденциальную информацию.

Условия включают различные факторы и обстоятельства, которые складываются в процессе научной, производственной, отчетной или иной деятельности подразделения и создают предпосылки для утечки информации. К таким факторам и обстоятельствам могут, относиться: недостаточное знание сотрудниками подразделения правил работы со сведениями, составляющими государственную тайну, непонимание важности защиты, доверенной им информации, использование неаттестованных технических средств обработки конфиденциальной информации, текучесть кадров, в том лиц, ответственных за защиту информации на конкретных объектах информатизации [47].

Кроме того, утечке информации способствуют:

– стихийные бедствия (шторм, ураган, смерч, землетрясение, наводнение);

– катастрофы (пожар, взрывы);

– неисправности, отказы, аварии технических средств и оборудования.

В повседневной деятельности подразделений ОВД присутствует информация различной степени конфиденциальности, которую в соответствии с действующим законодательством необходимо защищать [2]. Но, прежде чем непосредственно защищать всю циркулирующую в подразделения ОВД информацию, необходимо определить, как значимость (степень конфиденциальности, секретности информации), так и возможность получения злоумышленниками охраняемых сведений ОВД. Поскольку в подразделениях ОВД присутствуют также и сведения, составляющие государственную тайну (ГТ), важность вопросов защиты информации (ЗИ) от всех возможных угроз (обеспечение комплексности в защите информации) неоспорима [27].

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть воздушные, жидкие и твердые среды, например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т.п. Для приема и измерения параметров сигналов служат технические средства разведки (ТСР). В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата ТСР технические каналы утечки можно разделить на технические каналы утечки информации по ПЭМИ и наводкам, технические

каналы утечки акустической (речевой) информации, технические каналы утечки информации при ее передачи по каналам связи, а также технический канал утечки видовой информации [49].

При выявлении технических каналов утечки информации основные технические средства и системы (ОТСС) необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ОТСС и их элементами). Под ОТСС понимают технические средства, непосредственно обрабатывающие защищаемую информацию. Такими средствами могут быть: электронно-вычислительная техника, режимные АТС, системы оперативно-командной связи, системы звукоусиления, звукового сопровождения и т.д.

Наряду с ОТСС в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке закрытой информации, но использующиеся совместно с ОТСС и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрофикации, радиофикации, часофикации, электробытовые приборы и т.д. В качестве канала утечки информации наибольшую опасность представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), т.е. зоны, в которой исключено несанкционированное появление лиц и транспортных средств.

Кроме соединительных линий ОТСС и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками [16].

В зависимости от характера информации можно выделить визуальный канал утечки информации. В этом случае применяются следующие способы получения информации:

– наблюдение за объектами;
– съемка объектов.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации можно разделить на:

– электромагнитные;
– электрические.

Под акустической понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации

является человеческая речь, акустическая информация называется речевой [14].

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на:

- воздушные (прямые акустические);
- вибрационные (виброакустические);
- оптико-электронные;
- электроакустические.

Информация после обработки в ОТСС может передаваться по каналам связи, где также возможен ее перехват. В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. Технические каналы утечки информации при ее передаче по каналам связи можно разделить на:

- электромагнитные;
- электрические;
- индукционные.

2.4. Технический канал утечки видовой информации

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства. Для наблюдения днем - оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и т.д.), телекамеры, для наблюдения ночью - приборы ночного видения, телевизионные камеры, тепловизоры.

Для наблюдения с большой дистанции используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния - камуфлированные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

Съемка объектов проводится для документирования результатов наблюдения и более подробного анализа объектов. Для съемки объектов используются телевизионные и фотографические средства. При съемке объектов также, как и при наблюдении за ними, использование различных технических средств обусловлено условиями съемки и временем суток. Для съемки объектов днем с большого расстояния используются фотоаппараты и телевизионные камеры с длиннофокусными объективами или совмещенные с телескопами [8].

Для съемки объектов днем с близкой дистанции применяются камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи или передачи изображений по радиоканалу.

Съемка объектов ночью обычно осуществляется с близкого расстояния. Для достижения этой целей используются портативные фотоаппараты и телевизионные камеры, совмещенные с приборами ночного видения, или тепловизоры, а также портативные закамуфлированные телевизионные камеры высокой чувствительности, совмещенные с устройствами передачи информации по радиоканалу.

2.5. Каналы утечки информации, обрабатываемой техническими средствами

К электромагнитным относятся каналы утечки информации, возникающие из-за наличия различного вида побочных электромагнитных излучений (ПЭМИ) ОТСС. Возникновение угрозы утечки по каналам ПЭМИ возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации в ОТСС. Перехват побочных электромагнитных излучений ОТСС осуществляется средствами радио-, радиотехнической разведки, размещенными за пределами контролируемой зоны. В ОТСС носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) меняются по закону информационного сигнала [39]. При прохождении электрического тока по токоведущим элементам ОТСС вокруг них (в окружающем пространстве) ОТСС возникает электрическое и магнитное поле. Поэтому элементы можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Причинами возникновения электрических каналов утечки информации могут быть:

– наводки электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;

– просачивание информационных сигналов в цепи электропитания ОТСС;

– просачивание информационных сигналов в цепи заземления ОТСС.

При излучении элементами ОТСС (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ОТСС и посторонних проводников или линий ВТСС возникают наводки электромагнитных излучений ОТСС [9]. Уровень наводимых сигналов в большей степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины соединительных линий ОТСС и посторонних проводников. Пространство вокруг ОТСС, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется (опасной) зоной 1.

Просачивание информационных сигналов в цепи электропитания происходит при возникновении магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором

выпрямительного устройства. Помимо этого, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания [16].

Кроме заземляющих проводников, служащих для непосредственного соединения ОТСС с контуром заземления, гальваническую связь с землей так же могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Эти проводники вместе с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы. Так же, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

2.6. Технические каналы утечки речевой информации

В том случае, когда источником информации является голосовой аппарат человека, информация называется речевой. Речевой сигнал - сложный акустический сигнал, основная энергия которого сконцентрирована в диапазоне частот от 300 до 3400 Гц. Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн). Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Итак, в своем начальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. Вторичными же источниками являются различного рода преобразователи акустических и вибрационных колебаний. К данным устройствам относятся: громкоговорители, телефоны, микрофоны, акселерометры и др.

В зависимости от среды распространения речевых сигналов и способов их перехвата технические каналы утечки информации подразделяются на акустические, вибрационные, акустоэлектрические, оптико-электронные [3].

Распространение речевых сигналов в акустических каналах утечки информации происходит в воздушной среде. Для перехвата речевых сигналов применяются высокочувствительные микрофоны и специальные направленные микрофоны, которые соединяются с портативными звукозаписывающими устройствами или со специальными миниатюрными передатчиками.

Для перехвата акустической (речевой) информации используются:

– портативные диктофоны и проводные микрофонные системы скрытой звукозаписи;

– направленные микрофоны;

– акустические радиозакладочные устройства (передача информации по радиоканалу);

– акустические сетевые закладочные устройства (передача информации по сети электропитания 220 В);

– акустические ИК – закладочные устройства (передача информации по оптическому каналу в ИК- диапазоне длин волн);

– акустические телефонные закладочные устройства (передача информации по телефонной линии).

Речевая информация, перехваченная закладочным устройством, может быть отправлена по радиоканалу, сети электропитания, оптическому (ИК) каналу, соединительным линиям ВТСС, посторонним проводникам, инженерным коммуникациям в ультразвуковом (УЗ) диапазоне частот. Прием информации, передаваемой закладочными устройствами, обычно осуществляется приемником, функционирующим в соответствующем диапазоне длин волн. Однако существуют исключения из этого правила. Например, в случае передачи информации по телефонной линии с вызовом от внешнего абонента прием можно осуществлять с обычного телефонного аппарата. Использование портативных диктофонов и закладочных устройств требует проникновения в контролируемое помещение. В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

В виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.). Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры). Вибродатчик, соединенный с электронным усилителем называют электронным стетоскопом. Как правило, для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Имеется возможность передачи информации закладочными устройствами по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по инженерным коммуникациям) [64].

Оптико-электронный (лазерный) канал утечки акустической информации возникает при облучении лазерным лучом колеблющихся под действием акустического речевого сигнала отражающих поверхностей помещений (оконных стекол, зеркал и т.д.). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемным устройством оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация [3].

Акустоэлектрические каналы утечки информации образуется за счет преобразований акустических сигналов в электрические. У некоторых элементов ВТСС, в том числе трансформаторы, катушки индуктивности,

электромагниты вторичных электрочасов, телефонных аппаратов и т.п., при определенных условиях возможно изменение параметров (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы, либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля. ВТСС, помимо указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и др. Эффект акустоэлектрического преобразования называется «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации. Перехват акустоэлектрических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей. Так, подключение таких средств к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, приводит к реализации возможности прослушивания разговоров, ведущиеся в помещениях, где установлены эти аппараты [51].

2.7. Технические каналы утечки информации при ее передаче по каналам связи

Перехват электромагнитных излучений передатчиков средств связи, модулированных информационным сигналом, осуществляется портативными средствами радиоразведки. Рассматриваемый канал наиболее часто используется для прослушивания телефонных разговоров, проводимых по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи. Самый простой способ - это непосредственное параллельное подключение к линии связи. Однако факт подключения просто обнаружить, так как оно приводит к изменению характеристик линии связи за счет падения напряжения. Поэтому средства перехвата подключаются к линии связи или через согласующее устройство, минимально снижающее падение напряжения, или через специальное устройство компенсации падения напряжения. Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи [44]. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал, как правило, используется для перехвата телефонных переговоров. Устройства, подключаемые к телефонным линиям связи и совмещенные с устройствами передачи информации по радиоканалу, часто называют телефонными закладочными устройствами.

Наиболее часто используемый способ контроля проводных линий связи, не требующий контактного подключения - индукционный. В индукционном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики применяются в основном для съема информации с симметричных высокочастотных кабелей. Современные индукционные датчики способны регистрировать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающей кабель. Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного получения информации могут модифицироваться радиопередатчиками с целью передачи ее на контрольный пункт перехвата [45].

2.8. Угрозы несанкционированного доступа к информации

Несанкционированный доступ к информации (НСД) определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системой. К основным способам НСД относятся:

– непосредственное обращение к объектам доступа;

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

– модификация средств защиты, позволяющая осуществить НСД;

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

Перед тем, как организовывать защиту АС от угрозы НСД к информации необходимо рассмотреть возможности потенциального злоумышленника, чтобы принятые, впоследствии, меры по защите оказались максимально действенными [39].

В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является

иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Следствием реализации угроз НСД к информации является нарушения свойств ее безопасности: нарушение конфиденциальности (копирование, неправомерное распространение); нарушение целостности (уничтожение, изменение); нарушение доступности (блокирование).

Нарушение конфиденциальности может возникнуть в случае утечки информации:

– копирования ее на физические носители информации;

– передачи ее по каналам передачи данных;

– при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;

– при «сборке мусора» нарушителем в процессе эксплуатации.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

– микропрограммы, данные и драйвера устройств вычислительной системы;

– программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;

– программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;

– программы и данные прикладного программного обеспечения;

– программы и данные специального программного обеспечения;

– промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение целостности информации в АС может быть вызвано внедрением в нее вредоносной программы, программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы [7].

Нарушение доступности информации осуществляется путем формирования (модификации) исходных данных, которые при обработке

вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры. Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств, средств обработки информации; средств ввода/вывода информации; средств хранения информации; аппаратуры и каналов передачи; средств защиты информации.

Защита операционной системы является сложной задачей, так как внутренняя структура современных операционных систем чрезвычайно многообразна, имеет в своем составе множество взаимодействующих элементов. Поэтому соблюдение адекватной политики безопасности представляет собой более трудную, комплексную задачу. Возможности НСД на практике в значительной степени зависят от архитектуры и конфигурации конкретной операционной системы [32]. Однако имеются методы НСД, которые могут применяться практически к любым операционным системам:

– кража пароля (подглядывание за пользователем, когда тот вводит пароль);

– получение пароля из файла, в котором пароль был сохранен пользователем;

– сканирование жестких дисков компьютера;

– превышение полномочий (используются ошибки в программном обеспечении или в администрировании операционной системы);

– отказ в обслуживании (целью НСД является частичный или полный вывод из строя операционной системы).

Так же возможны угрозы безопасности информации, связанные с осуществлением различного рода физических воздействий на технические средства обработки защищаемой информации в целях нарушения их целостности или хищения носителей информации.

Таким образом, были обозначены основные угрозы безопасности информации, приведена характеристика данных угроз и применяемые средства для съема информации. Необходимость рассмотрения всех угроз без исключения продиктована важностью защищаемой информации. Игнорирование, на первый взгляд, несущественной и труднореализуемой угрозы безопасности впоследствии может обернуться утечкой защищаемой информацией и несостоятельностью всей разработанной системы защиты информации.

Вопросы и задания для самоконтроля:

1. Как Вы думаете, в чем заключаются угрозы безопасности информации?
2. Дайте определение «bug bounty».
3. Как выглядит классификация угроз безопасности информации по используемой уязвимости?

4. В чем заключается угроза безопасности информации, возникающая вследствие установки закладочного устройства?
5. Что подразумевается под техническим каналом утечки информации?
6. Какие факторы способствуют утечке информации.
7. Есть ли необходимость в классификации защищаемой информации?
8. Дайте классификацию технических каналов утечки информации.
9. Сформулируйте способы получения информации.
10. Каким образом можно классифицировать технические каналы утечки акустической (речевой) информации?
11. Что представляет собой технический канал утечки видовой информации?
12. Что можно отнести к техническим каналам утечки речевой информации?
13. Каковы причины возникновения электрических каналов утечки информации?
14. Что можно использовать для перехвата акустической (речевой) информации?
15. В чем заключается сущность перехвата электромагнитных излучений?
16. Назовите современные способы совершения кибератак. Приведите примеры вредоносных программ.
17. Сформулируйте основные способы защиты от вредоносного программного обеспечения.
18. Что называют оконечными устройствами? Привести примеры.
19. В чем заключаются причины некорректной работы антивирусной программы?
20. Укажите организационные методы обеспечения безопасности информации.
21. Укажите технические методы обеспечения безопасности информации.
22. Сформулируйте понятие технических методов обеспечения безопасности информации.
23. Сформулируйте правила обработки информации.
24. Опишите угрозы несанкционированного доступа к информации.
25. Перечислите правила использования программ.
26. Сформулируйте понятие политики безопасности организации.
27. В чем состоит необходимость обновления используемых на компьютере программ?
28. Дайте понятие Брандмауэру (межсетевому экрану).
29. В каком случае может возникнуть нарушение конфиденциальности информации?
30. Укажите средства защиты от нежелательной корреспонденции.
31. Перечислите принципы обеспечения безопасности сети.
32. Каким образом осуществляется нарушение целостности информации?

33. Опишите методы, НСД, которые могут применяться практически к любым операционным системам.

34. Возможны ли угрозы безопасности информации, связанные с осуществлением различного рода физических воздействий на технические средства обработки защищаемой информации?

ГЛАВА 3. ОЦЕНКА ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОМВД РОССИИ

При оценке защищенности объекта информатизации выделение наиболее потенциально опасных угроз представляет собой ключевую задачу. Необходимо четко понимать, что ее решение находится в зависимости от целого перечня факторов и имеет тенденцию к изменению в зависимости от поставленных оперативных задач [2].

После рассмотрения основных угроз безопасности информации и изучения их особенностей необходимо осуществить корректировку описанных угроз относительно рассматриваемого объекта информатизации (ОИ) [14].

Так, угрозы безопасности информации, возникающие при ее передаче по каналам связи, не могут быть реализованы в следствие возникновения объективной причины – отсутствие подключения ОИ к каналам связи передачи данных. Поэтому дальнейшее рассмотрение угроз, возникающих при передаче информации по каналам связи, является нецелесообразным.

Таким образом, после проведения корректировки угроз безопасности информации, составлен скорректированный перечень угроз непосредственно для рассматриваемого ОИ:

- угроза безопасности информации вследствие возникновения визуального канала утечки информации;
- угроза безопасности информации, возникающая вследствие установки закладочного устройства;
- угроза безопасности информации вследствие возникновения электромагнитного канала утечки информации;
- угроза безопасности информации вследствие возникновения электрического канала утечки информации;
- угроза безопасности информации вследствие возникновения акустического канала утечки речевой информации;
- угроза безопасности информации вследствие возникновения виброакустического канала утечки речевой информации;
- угроза безопасности информации вследствие возникновения оптико-электронного канала утечки речевой информации;
- угроза безопасности информации вследствие возникновения акустоэлектрического канала утечки речевой информации;
- угроза безопасности информации из-за осуществления НСД к информации [30].

По итогам составленного скорректированного перечня угроз необходимо провести объективную оценку исходной защищенности объекта информатизации ОМВД России от каждой из выявленных угроз безопасности информации.

Для оценки защищенности объекта информатизации от утечки информации по визуальному каналу будем применять экспертно-

документальный метод. Введем исходные условия, конкретизирующие защищаемый объект.

Объект информатизации, а именно, служебный кабинет, предназначен для проведения мероприятий по вопросам, содержащим информацию ограниченного доступа. Кабинет расположен на 2 этаже здания ОМВД России. Наружные стены помещения выполнены из кирпича. Перекрытия пола и потолка железобетонные. Внутренние перегородки выполнены из кирпича, железобетона. Фальшпол и фальшпотолок в помещении отсутствуют. Окна в помещении - стеклопакеты с одной открывающейся створкой, с внутренней стороны оборудованы прозрачными светлыми шторами. Окна выходят на помещения, в которых находятся отделы ОМВД России (рис. 3.1).

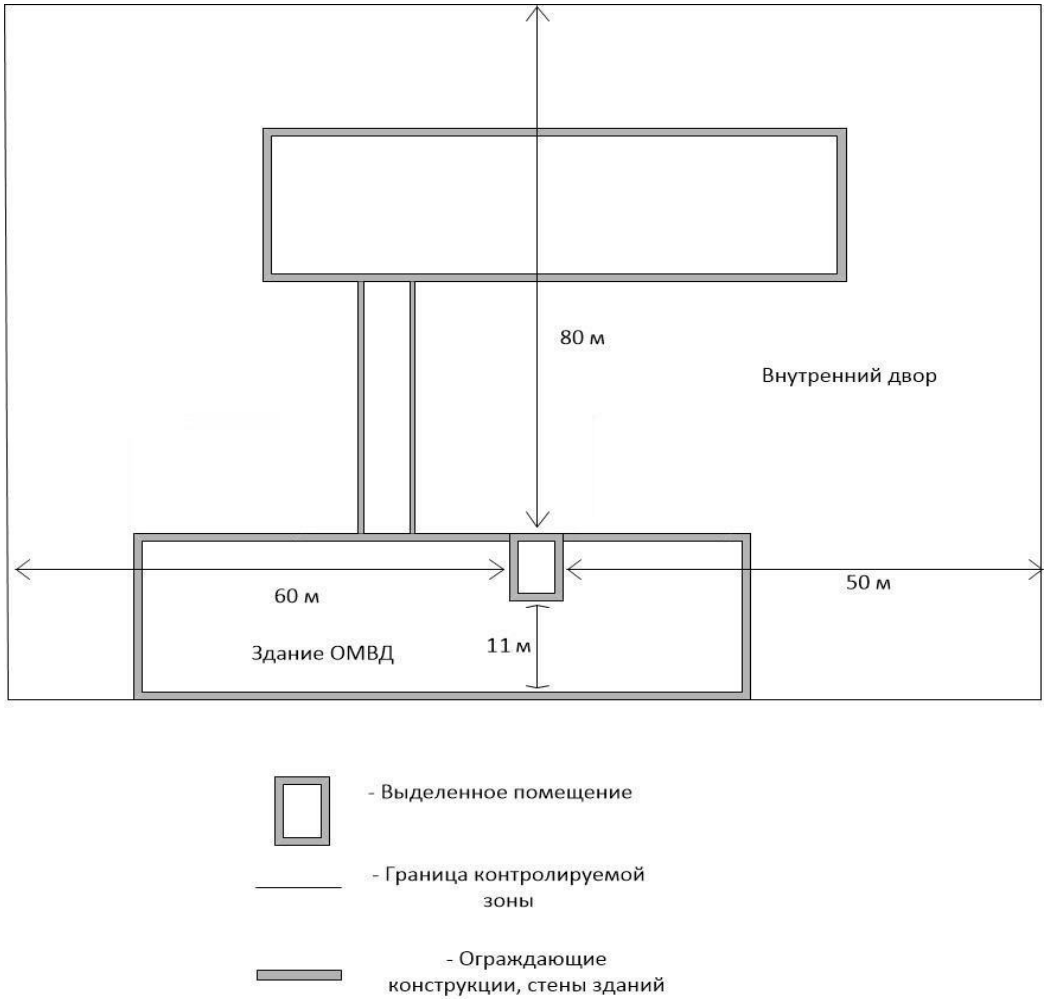

Рис. 3.1. Расположение ОИ относительно границ КЗ

В помещении находится автоматизированная система в составе монитора, системного блока, клавиатуры и компьютерной мыши. АС должна соответствовать требованиям по защите информации, предъявляемые ко второй группе защищенности АС от НСД.

Также в помещении имеется система охранной сигнализации, состоящей из датчика объема и магнитоконтактного датчика, и систему пожарной сигнализации, состоящей из двух дымовых пожарных извещателей.

Окна помещения расположены напротив второго корпуса ОМВД России, что ограничивает возможность съема визуальной информации для внешних нарушителей, т.е. нарушителей, не являющихся сотрудниками ОМВД России. Возможность съема визуальной информации внутренними нарушителями (являющимися сотрудниками ОМВД России) существует. Но тот факт, что все сотрудники ОМВД России являются доверенными субъектами, прошедшими ряд проверок при поступлении на службу, определяет низкую возможность реализации указанной угрозы.

Анализ защищенности объекта начнем с оценки эффективности защиты информации от утечки вследствие установки закладочного устройства. Для этого мероприятия по обнаружению и противодействию работе закладочных устройств необходимо подразделить на организационные и технические [17].

Наиболее разноплановыми являются организационные мероприятия, которые могут включать в свой состав: проведение «аналитической работы по выявлению возможных мест установки закладочных устройств (с учетом особенностей их работы); организацию работы службы безопасности по контролю излучений в эфире, сетях связи, управления; анализ частотного диапазона и способов работы закладочных устройств» [42].

В результате проведения поиска закладочного устройства методом визуального осмотра помещения и проверки соответствия состава АС технической документацией признаков и наличия самого закладочного устройства не обнаружено.

Технические мероприятия, в свою очередь, связаны с непосредственным обнаружением закладочных устройств, а также мероприятиями, направленными на выявление каналов утечки информации от технических средств с использование контрольно-измерительной аппаратуры.

В рассматриваемое помещение на протяжении длительного времени было исключено несанкционированного появление посторонних лиц. Раннее обработка закрытой информации в данном помещении и проведение в нём каких-либо мероприятий, связанных со служебной деятельностью, не проводились.

Принимая во внимание предложенную методику поиска, по итогам проведения организационных и технических мероприятий по обнаружению закладочного устройства, можно сделать вывод об отсутствии закладочных устройств в рассматриваемом помещении. Делать заключение об отсутствии данной угрозы в технических средствах, установленных в помещении следует только после проведения специального исследования, а также проведения специальных проверок технических средств иностранного производства на предмет наличия в них электронных устройств негласного получения информации [23].

3.1. Оценка эффективности защиты информации от утечки информации по электромагнитному каналу

Для оценки эффективности защиты информации от утечки информации по электромагнитному каналу будем применять инструментальный метод. В помещение находится ОТСС, на котором обрабатывается информация ограниченного доступа, а именно автоматизированная система в составе монитора, системного блока, клавиатуры и компьютерной мыши.

Для оценки защищенности объекта информатизации от утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН) используется программно-аппаратный комплекс «Навигатор-П5Г» (рис. 3.2).

Рис. 3.2. Состав ПАК «Навигатор»

В ПАК «Навигатор» реализованы различные методы поиска ПЭМИН. Представленные методы отличаются по степени участия в них пользователя. Даже самые слабые сигналы должны исследоваться для достижения максимальной полноты и достаточности результатов. Их корректно возможно разобрать лишь оператору, обладающему достаточным опытом и профессиональной интуицией. Поэтому на практике удобней пользоваться не одним методом, а комбинировать для получения наиболее точного результата исследования [66].

Исследованию ПЭМИН подлежат различные элементы ПК. Однако практический опыт показал, что наибольшие излучение формирует монитор. Соответственно, обнаружив ПЭМИН монитора и выполнив мероприятия по защите информации от утечки по данному каналу, можно обеспечить защиту от утечки по каналу ПЭМИН других элементов и устройств. Порядок проведения работы состоит в последовательности выполнения следующих действий: поисковой этап и исследование ПЭМИН.

Результаты расчета зон R2, r1, r1' для ОИ 1 категории, полученные с помощью ПАК Навигатор приведены в таблице 3.1.

Таблица 3.1.

Результаты расчета R2, r1, r1' для 1 категории

№	Интервал, МГц	Частоты, МГц	R2 для стационарных средств, м	R2 для возимых средств, м	R2 для носимых средств, м	r1, м	r1', м
1	0.0100000 - 64.800710	32.400355	15.0	15.0	15.0	2.2	0.7
2	64.800710 - 129.601420	97.201352	15.0	9.0	6.0	1.5	0.4
3	518.405680 - 583.206390	550.808335	15.0	5.0	3.0		
4	583.206390 - 648.007100	615.609333	30.0	10.0	5.0		
5	648.007100 - 712.807810	680.313655	3.0	2.0	1.0		
Итого			**30.0**	**15.0**	**15.0**	**2.2**	**0.7**

Результаты расчета зон R2, r1, r1' для ОИ 2 категории, полученные с помощью ПАК «Навигатор» приведены в таблице 3.2.

Таблица 3.2.

Результаты расчета R2, r1, r1' для 2 категории

№	Интервал, МГц	Частоты, МГц	R2 для стационарных средств, м	R2 для возимых средств, м	R2 для носимых средств, м	r1, м	r1', м
1	0.0100000 - 64.800710	32.400355	9.0	9.0	9.0	1.6	0.6
2	64.800710 - 129.601420	97.201352	10.0	7.0	4.0	1.1	0.3
3	518.405680 - 583.206390	550.808335	8.0	3.0	2.0		
4	583.206390 - 648.007100	615.609333	15.0	5.0	3.0		
5	648.007100 - 712.807810	680.313655	2.0	2.0	1.0		
Итого			**15.0**	**9.0**	**9.0**	**1.6**	**0.6**

Результаты расчета зон R2, r1, r1' для ОИ 3 категории, полученные с помощью ПАК «Навигатор» приведены в таблице 3.3.

Таблица 3.3.

Результаты расчета R2, r1, r1' для 3 категории

№	Интервал, МГц	Частоты, МГц	R2 для стационарных средств, м	R2 для возимых средств, м	R2 для носимых средств, м	r1, м	r1', м
1	0.0100000 - 64.800710	32.400355	8.0	8.0	8.0	1.4	0.5
2	64.800710 - 129.601420	97.201352	8.0	6.0	4.0	0.9	0.2
3	518.405680 - 583.206390	550.808335	5.0	3.0	2.0		

№	Интервал, МГц	Частоты, МГц	R2 для стационарных средств, м	R2 для возимых средств, м	R2 для носимых средств, м	r1, м	r1', м
4	583.206390 - 648.007100	615.609333	12.0	4.0	3.0		
5	648.007100 - 712.807810	680.313655	2.0	1.0	1.0		
Итого			**12.0**	**8.0**	**8.0**	**1.4**	**0.5**

Таким образом, для первой категории максимальное расстояние, на котором возможен съем информации злоумышленником по каналам ПЭМИН равен 30 м; для второй категории – 15 м; 3 категории на расстоянии 12 м. Так как минимальное расстояние до границы контролируемой зоны согласно исходным данным об объекте информатизации составляет 11 м, следовательно, возникает необходимость применения средств защиты информации, которые должны быть оправданными, необходимыми и окупаемыми [65].

3.2. Оценка эффективности защиты информации от утечки информации по акустическому каналу

При рассмотрении защищенности объекта информатизации по акустическому каналу источником информации, как правило, является речь человека, поэтому такая информация называется «речевой» (рис. 3.3).

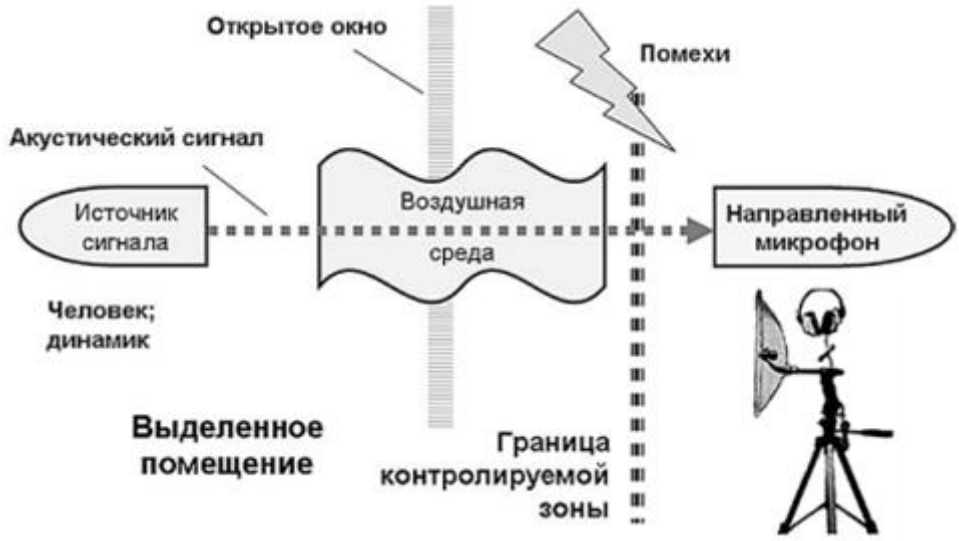

Рис. 3.3. Акустический канал утечки информации

В качестве источников информации могут выступать: человек или акустические системы, элементы систем громкоговорящей связи, которые могут быть использованы в качестве резонаторов звукового диапазона частот.

При определении технического канала утечки информации очень важным параметром является среда распространения информационного

сигнала. Соответственно, для воздушного канала – это воздух, в среде которого основными средствами перехвата информации являются: портативные устройства звукозаписи (диктофоны); закладные устройства с передачей по радиоканалу, оптическому каналу, электросети и др. Не стоит забывать про прослушивание из-за недостаточной звукоизоляции помещения [14].

Когда речь заходит о вибрационных каналах, то здесь средой распространения выступают строительные конструкции или инженерные системы, к которым относятся стены, трубы, элементы отопления и т.д. К вибрационным относится добыча информации с помощью электронных стетоскопов, которые преобразовывают акустический сигнал в электрический с последующим усилением для лучшего прослушивания. Также можно перехватить сигнал стетоскопами и передать его по оптическому каналу в инфракрасном диапазоне, так как данный спектр не видим человеческому глазу, что позволяет злоумышленнику его скрыть. Кроме того, инфракрасный сигнал позволяет передать сигнал при наличии помех. Возможен перехват информации стетоскопами с передачей через инженерные коммуникации и металлоконструкции.

В оптоэлектронном канале источником является вибрация поверхности, например, оконных поверхностей, с которых как раз и снимают акустический сигнал лазерные микрофоны.

Средой распространения в электроакустическом канале выступают электрические цепи и устройства, которые могут находиться в помещении. Перехват акустического сигнала может осуществляться через выносные технические средства связи с микрофонным эффектом путем подключения их к соединительным линиям. В качестве таки устройств могут выступать стационарные и мобильные телефоны, компьютеры и даже провода, улавливающие вибрации и превращающие их в электрический сигнал, который может быть передан и записан.

Существует не менее интересный способ перехвата акустического сигнала через выносные технические средства связи путем высокочастотного навязывания, при котором злоумышленник посылает высокочастотный сигнал, не слышимый человеком, модулирующий обычный акустический сигнал в результате чего обычный провод, не предназначенный для передачи звука, начинает работать как антенна, передающая звук, захваченный в помещении. Злоумышленник на другом конце провода восстанавливает оригинальный звук.

В параметрических ТКУИ средой распространения является электромагнитное поле, позволяющее осуществлять перехват акустического сигнала путем высокочастотного облучения специальных полуактивных закладок (микрофонов или микропередатчиков), которые улавливают звуки, но работают только тогда, когда на них воздействует определенный сигнал. Такой сигнал активирует закладочное устройство и оно начинает передавать записанный звук или акустический сигнал с помощью радиоволн. В качестве

другого способа выступает перехват акустического сигнала путем приема паразитных электромагнитных импульсов.

Для оценки защищенности объекта информатизации от утечки информации по акустическому каналу будут применяться экспертно-документальный и инструментальный методы [62] с использованием программно-аппаратного комплекса «Спрут-7М» [56].

Комплекс может работать как в автономном режиме, так и под управлением ПК. В автономном режиме комплекс позволяет всего одному человеку провести весь комплекс аттестационных испытаний помещения на оценку защищённости его от утечки по техническим каналам.

Программное обеспечение позволяет намного расширить возможности комплекса, например, проведение спектрального узкополосного анализа в полосе частот 1,5 кГц, оценка эффективности утечки речевой информации за счёт акустоэлектрических преобразований по симметричным и несимметричным линиям, оценка сигнала плюс шум, оценка действия средств активной защиты в помещении.

Методы и средства контроля защищенности информации ограниченного доступа включают оценку эффективности защиты информации, контроль за состоянием защитных потенциальных рисков и проверку соответствия организации и эффективности защиты информации установленным требованиям. Для проведения проверки существуют две основные методики оценки защищенности технических средств: методика соответственно специальных исследований и методика измеренного и рассчитанного соотношения сигнал-шум на границе контролируемой зоны [57].

Выберем контрольные точки (КТ) на внешних поверхностях ограждающих конструкций, которые схематично показаны на рис. 3.4:

КТ 1–на стене 2 (со стороны окна);

КТ 2– на стене 4 (со стороны коридора);

КТ 3, КТ 4 – на стенах 1 и 3 соответственно (на стенах, граничащих с соседними кабинетами);

КТ 5 – на полу;

КТ 6 – на потолке;

КТ 7 – на двери.

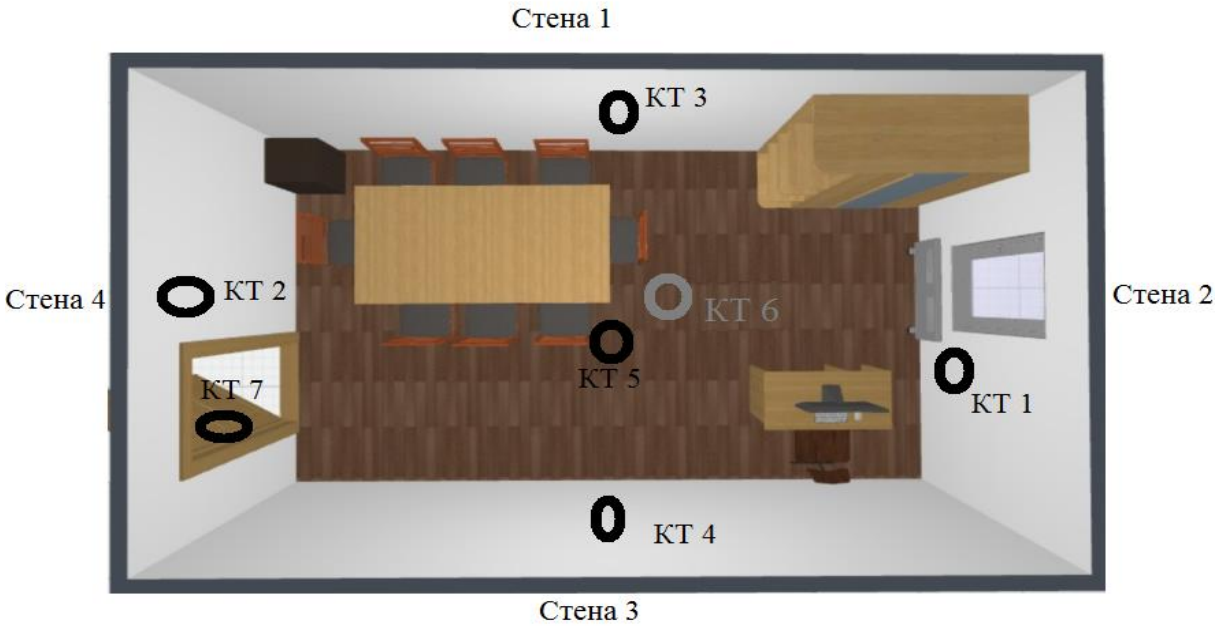

Рис. 3.4. Схема объекта информатизации

На рис. 3.5 показана схема измерений, проведенных на стене со стороны окна.

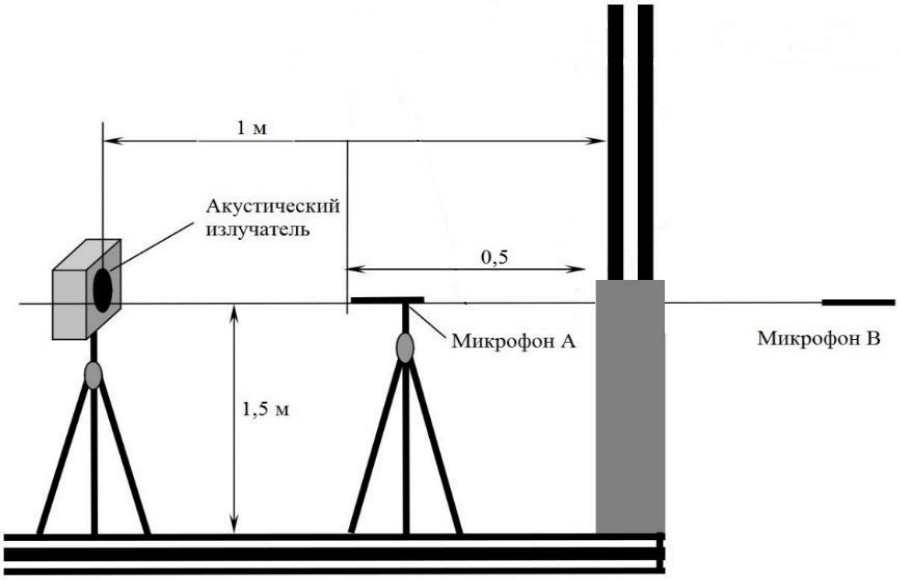

Рис. 3.5. Схема измерений на стене 2

Необходимо отметить, что для получения более объективных показаний измерений для данной строительной конструкции замеры проводились в двух контрольных точках КТ 1а и КТ 1б, расположение которых приведено на рис. 3.6.

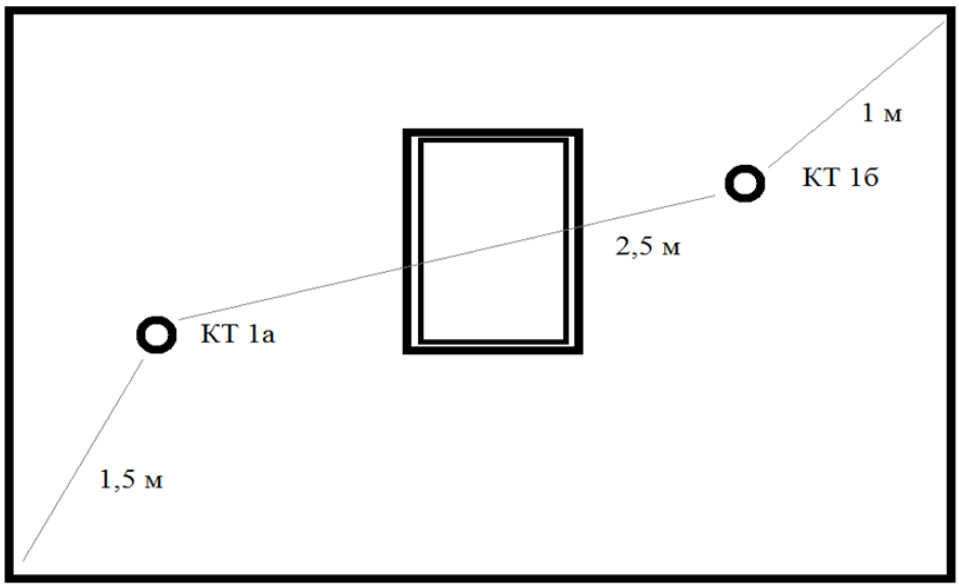

Рис. 3.6. Схема размещения контрольных точек на стене 2

Полученные значения в результате инструментального контроля приведены в таблице 3.4.

Таблица 3.4.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 1а

Номер октавной полосы	Среднегеомет-рическая частота октавной полосы, Гц	Уровень акустического шума в контрольной точке $L_{шi}$, дБ	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(с+ш)i}$, дБ
1	250	46,19	59,53
2	500	42,45	62,17
3	1000	40,92	57,98
4	2000	39,34	56,84
5	4000	37,12	50,23

1. Вычисляем уровень акустического сигнала в КТ 1а для пяти октавных полос по следующей формуле:

$$L_{C_i} = 10\lg\{10^{0,1L_{(с+ш)i}} - 10^{0,1L_{ш_i}}\}$$

$$L_{C_1} = 10\lg\{10^{0,1*59,53} - 10^{0,1*46,19}\} = 59,32 \text{ дБ}$$

$$L_{C_2} = 10\lg\{10^{0,1*62,17} - 10^{0,1*42,45}\} = 62,12 \text{ дБ}$$

$$L_{3} = 10\lg\{10^{0,1*57,98} - 10^{0,1*40,92}\} = 57,89 \text{ дБ}$$

$$L_{C_4} = 10\lg\{10^{0,1*56,84} - 10^{0,1*39.34}\} = 56,76 \text{ дБ}$$

$$L_{C_5} = 10\lg\{10^{0,1*50,23} - 10^{0,1*37,12}\} = 50,01 \text{ дБ}$$

2. Рассчитываются отношения сигнал/шум в октавных полосах.

В случае акустического сигнала:

$$E_i = L_{c_i} - L_{ш_i}$$

$$E_1 = L_{c_1} - L_{ш_1} = 59,32 - 46,19 = 13,13 \text{ дБ}$$

$$E_2 = L_{c_2} - L_{ш_2} = 62{,}12 - 42{,}45 = 19{,}67 \text{ дБ}$$
$$E_3 = L_{c_3} - L_{ш_3} = 63{,}03 - 56{,}92 = 16{,}97 \text{ дБ}$$
$$E_4 = L_{c_4} - L_{ш_4} = 56{,}76 - 39{,}34 = 17{,}42 \text{ дБ}$$
$$E_5 = L_{c_5} - L_{ш_5} = 50{,}01 - 37{,}12 = 12{,}89 \text{ дБ}$$

Полученный результат E_i сравнивается с нормированным значением отношения «сигнал/шум» в октавных полосах E_{H_i}, приведенных в таблице Б1 НМД АРР[42]. После сравнения E_i с нормированными значениями можно сделать вывод о том, что нормы не выполняются, поэтому далее вычисляются октавные индексы артикуляции речи:

$$r_i = K_i \left| z - \frac{0{,}78 + 5{,}46\exp[-4{,}3 * 10^{-3}(27{,}3 - |E_i - A_i|)^2]}{1 + 10^{0{,}1|E_i - A_i|}} \right|$$

где $z = \begin{cases} 0, \text{если } E_i \le A_i \\ 1, \text{если } E_i > A_i \end{cases}$

A_i – формантный параметр спектра речевого сигнала в октавной полосе, дБ;

K_i – весовой коэффициент октавной полосы частот.

Таблица 3.5.

Числовые значения формантного параметра спектра речевого сигнала Ai и весового коэффициента Ki в октавных полосах

Наименование параметров	Среднегеометрические частоты октавных полос fcp.i, Гц				
	250	500	1000	2000	4000
Числовое значение формантного параметра спектра речевого сигнала в октавной полосе D Ai, дБ	18	14	9	6	5
Числовое значение весового коэффициента в октавной полосе Ki	0,03	0,12	0,2	0,3	0,26

3. Вычисляются октавные индексы артикуляции речи:

$$r_1 = 0{,}03 \left| 0 - \frac{0{,}78 + 5{,}46\exp[-4{,}3 * 10^{-3}(27{,}3 - |13{,}13 - 18|)^2]}{1 + 10^{0{,}1|13{,}13 - 18|}} \right|$$
$$r_1 = 0{,}01038$$
$$r_2 = 0{,}12 \left| 1 - \frac{0{,}78 + 5{,}46\exp[-4{,}3 * 10^{-3}(27{,}3 - |19{,}67 - 14|)^2]}{1 + 10^{0{,}1|19{,}67 - 14|}} \right|$$
$$r_2 = 0{,}08136$$
$$r_3 = 0{,}2 \left| 1 - \frac{0{,}78 + 5{,}46\exp[-4{,}3 * 10^{-3}(27{,}3 - |16{,}97 - 9|)^2]}{1 + 10^{0{,}1|16{,}97 - 9|}} \right|$$
$$r_3 = 0{,}14841$$

[42] Информационное сообщение Федеральной службы по техническому и экспортному контролю от 12.01.2016 № 240/24/87 «По вопросу продления сроков действия сертификатов соответствия на средства активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок и средства активной акустической и вибрационной защиты акустической речевой информации, эксплуатируемые на объектах информатизации» // СПС «Гарант».

$$r_4 = 0{,}3\left|1 - \frac{0{,}78 + 5{,}46\exp[-4{,}3 * 10^{-3}(27{,}3 - |17{,}42 - 6|)^2]}{1 + 10^{0{,}1|17{,}42-6|}}\right|$$

$$r_4 = 0{,}24702$$

$$r_5 = 0{,}26\left|1 - \frac{0{,}78 + 5{,}46\exp[-4{,}3 * 10^{-3}(27{,}3 - |12{,}89 - 5|)^2]}{1 + 10^{0{,}1|12{,}89-5|}}\right|$$

$$r_5 = 0{,}19238$$

4. Рассчитывается интегральный индекс артикуляции речи:

$$R = \sum_{i=1}^{5} r_i = 0{,}01038 + 0{,}08136 + 0{,}14841 + 0{,}24702 +$$

$$+0{,}19238 = 0{,}67956$$

5. Рассчитывается значение показателя противодействия АРР:

$$W = \begin{cases} 1{,}54R^{0{,}25}[1 - \exp(-11R)], & \text{если } R < 0{,}15 \\ 1 - exp\left(-\dfrac{11R}{1 + 0{,}7R}\right), & \text{если } R \geq 0{,}15 \end{cases}$$

Вследствие того, что $R \geq 0{,}15$ $(0{,}427457 \geq 0{,}15)$, то значение показателя противодействия АРР рассчитывается по формуле:

$$W = 1 - exp\left(-\frac{11R}{1 + 0{,}7R}\right)$$

$$W = 1 - exp\left(-\frac{11 * 0{,}67956}{1 + 0{,}7 * 0{,}67956}\right) = 0{,}99768$$

Аналогично приведенному способу при расчетах значений в КТ 1а произведены расчеты для КТ 1б. Полученные в результате инструментального контроля с использованием комплекса «Спрут 7М» значения измерений, а также рассчитанные значения для КТ 1б приведены в таблице 3.6.

Таблица 3.6.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 1б

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень акустического шума в контрольной точке $L_{ш}$, дБ	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(с+ш)\,i}$, дБ	Уровень акустического сигнала, L_{C_i}	Отношение сигнал/шум в октавных полосах, E_i	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, R	Показателя противодействия АРР, W
КТ 1б								
1	250	49,32	63,29	63,11	13,79	0,0109	0,5152	0.9943
2	500	51,74	61,76	61,31	9,57	0,0431		
3	1000	44,55	57,17	56,93	12,38	0,1215		
4	2000	48,87	55,43	54,37	5,48	0,1452		
5	4000	40,25	53,64	55,47	13,45	0,1944		

При акустических измерениях стены 4 (со стороны коридора) измерительные приборы размещаются согласно стандартной схеме (рис. 3.7).

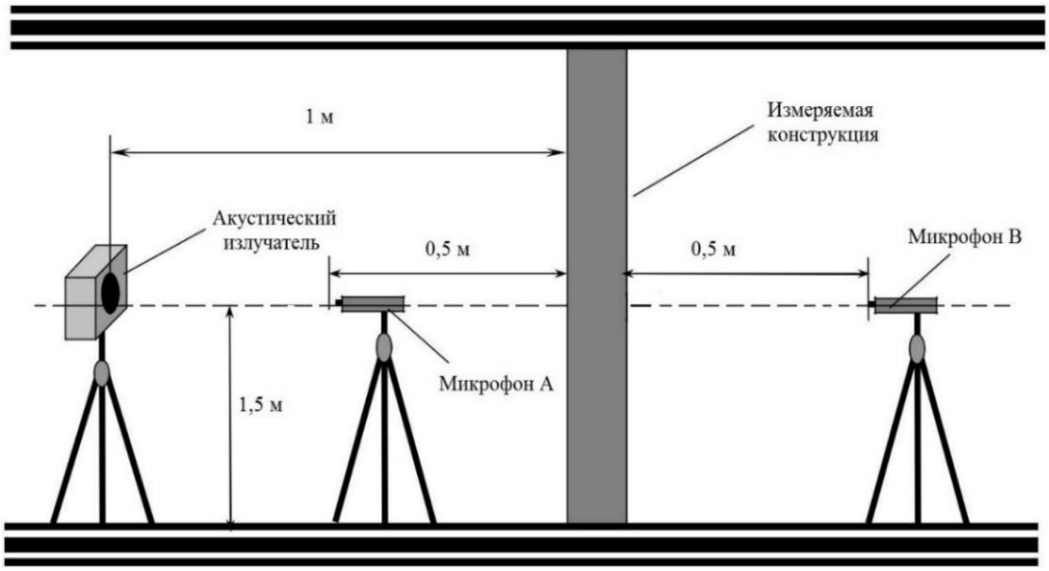

Рис.3.7. Схема измерения акустических характеристик стены

Измерения, проводимые на стене со стороны коридора, осуществлялись в трех точках: КТ 2а, КТ 2б, КТ 2в, расположение которых приведено на рис. 3.8.

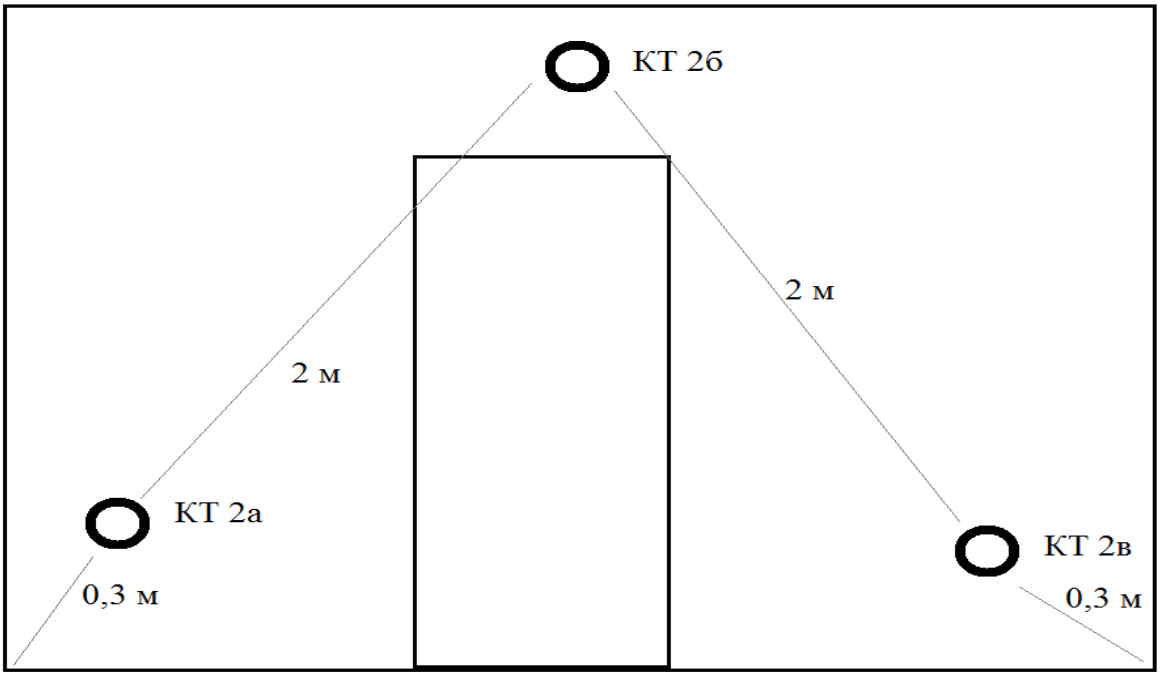

Рис. 3.8. Схема расположения контрольных точек на стене 2

Значения измерений, полученные в результате инструментального контроля с использованием комплекса «Спрут 7М», а также значения, рассчитанные для КТ 2а, КТ 2б, КТ 2в (на стене со стороны коридора) по методике, примененной для КТ 1а, приведены в таблице 3.7.

Таблица 3.7.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 2а, КТ 2б, КТ 2в

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень акустического шума в контрольной точке $L_{ш}$, дБ	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(с+ш)\,i}$, дБ	Уровень акустического сигнала, L_{C_i}	Отношение сигнал/шум в октавных полосах, E_i	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, R	Показателя противодействия APP, W
КТ 2а								
1	250	41,57	56,68	56,54	14,97	0,0118	0,5407	0,9952
2	500	40,76	53,62	53,39	13,68	0,0551		
3	1000	44,51	52,74	52,03	7,52	0,0909		
4	2000	37,32	47,15	46,67	9,35	0,1821		
5	4000	33,14	47,49	47,32	14,19	0,2008		
КТ 2б								
1	250	44,96	52,63	51,82	6,86	0,0051	0,5191	0,9938
2	500	41,42	54,27	54,04	12.62	0,0552		
3	1000	45,18	50,36	49,64	7,46	0,0628		
4	2000	39,24	46,47	45,56	6,32	0,1531		
5	4000	21,35	44,96	44,91	23,59	0,2429		
КТ 2в								
1	250	43,73	51,34	50,51	6,783	0,0054	0,6157	0,9968
2	500	33,81	47,72	47,54	13,72	0,0591		
3	1000	30,52	45,28	45,13	14,61	0,1352		
4	2000	31,75	43,14	42,81	11,06	0,1979		
5	4000	25,26	42,51	42,43	17,16	0,2181		

Аналогично приведенному способу при расчетах значений для КТ 1а произведены расчеты для КТ 3, КТ 4 (на стенах, граничащих с соседними кабинетами). На рассматриваемых инженерных конструкциях выбрано по одной контрольной точки на стену из-за однородности материала стен и отсутствии в них трещин и отверстий. Рассчитанные значения для КТ 3, КТ 4 приведены в таблице 3.8.

На рис. 3.9 показана типовая схема измерения показателей перекрытия пола. Расположение акустического излучателя должно быть на месте источника звука (рабочий стол руководителя, трибуна для выступлений и т.д.) [21].

Аналогично измерениям, проводимым для КТ 5 (пол), проводились измерения и для КТ 6 (потолок). В свою очередь, методика расчета использована такая же, как для КТ 1а. Полученные данные приведены в таблице 3.9.

Таблица 3.8.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 3, КТ 4

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень акустического шума в контрольной точке $L_{ш i}$, дБ	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(с+ш) i}$, дБ	Уровень акустического сигнала, L_{C_i}, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия АРР, W
КТ 3								
1	250	38,29	44,21	42,92	4,63	0,0041	0,6332	0,9971
2	500	33,45	43,83	43,41	9,96	0,0446		
3	1000	29,24	42,59	42,38	13,14	0,1259		
4	2000	23,17	40,95	40,87	17,71	0,2487		
5	4000	21,78	37,48	37,36	15,57	0,2086		
КТ 4								
1	250	35,74	46,21	45,8	10,06	0,0077	0,5963	0,9964
2	500	32,57	44,15	43,84	11,26	0,0495		
3	1000	25,26	42,78	42,69	17,44	0,1508		
4	2000	28,41	39,84	39,52	11,10	0,1979		
5	4000	23,33	36,17	35,94	12,61	0,1904		

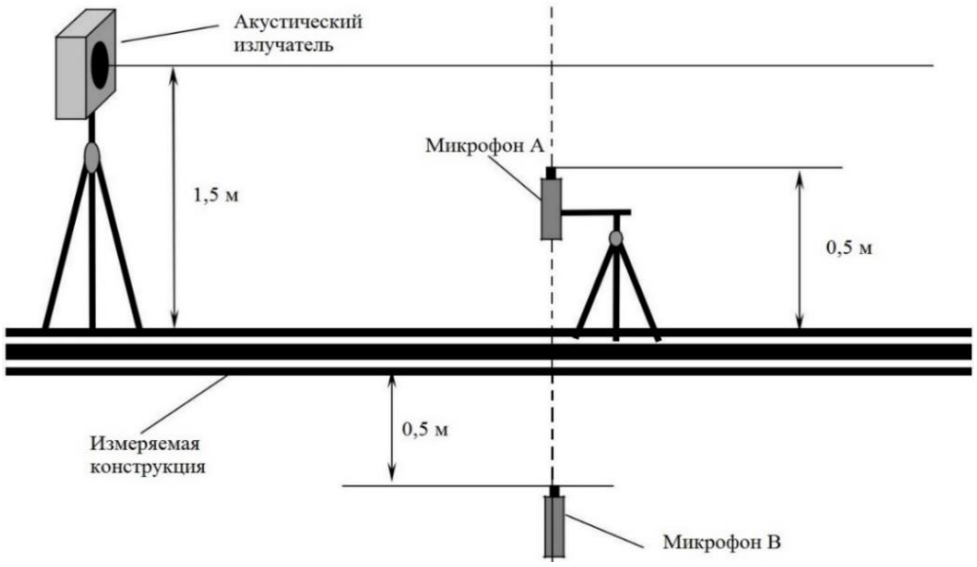

Рис. 3.9. Схема измерения акустических характеристик перекрытия пола

Таблица 3.9.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 5, КТ 6

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень акустического шума в контрольной точке $L_{ш i}$, дБ	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(с+ш) i}$, дБ	Уровень акустического сигнала, $L_{С_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, R	Показателя противодействия АРР, W
КТ 5								
1	250	40,81	49,24	48,57	7,76	0,0061	0,5423	0,9951
2	500	35,04	46,18	45,83	10,79	0,0477		
3	1000	33,76	42,74	42,15	8,39	0,0962		
4	2000	27,53	40,51	40,29	12,76	0,2127		
5	4000	26,19	37,62	37,29	11,11	0,5424		
КТ 6								
1	250	46,74	53,82	52,87	6,13	0,0051	0,6536	0,9974
2	500	43,11	55,27	54,99	11,88	0,0519		
3	1000	36,43	51,92	51,79	15,36	0,1396		
4	2000	31,27	48,46	48,38	17,11	0,2449		
5	4000	30,14	46,31	46,21	16,06	0,2121		

На рис. 3.10 показана схема измерения акустических характеристик дверного проема.

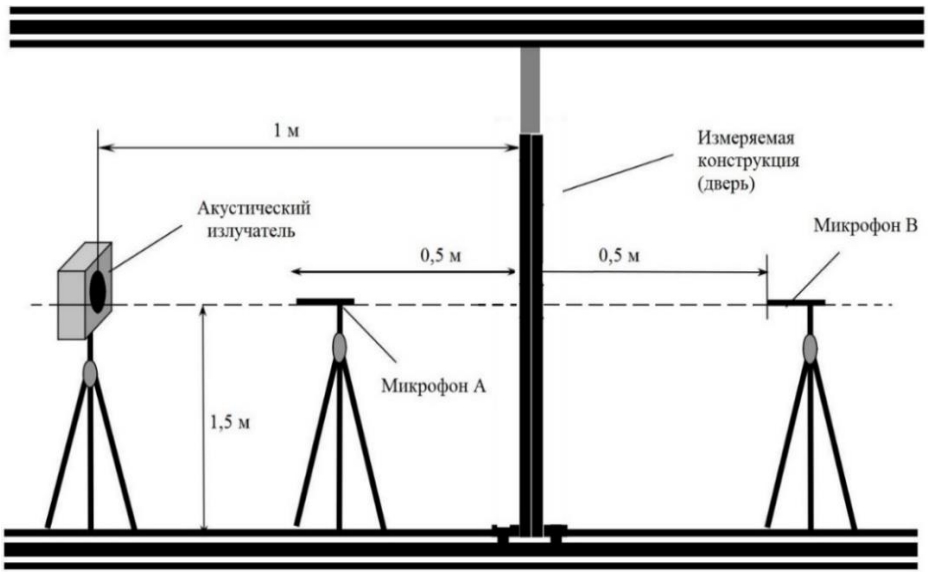

Рис. 3.10. Схема измерения акустических характеристик дверного проема

В результате инструментального контроля с использованием комплекса «Спрут 7М» получены следующие данные по акустическому сигналу для контрольной точки 7 (дверь). Также приведены значения, рассчитанные для КТ 7 по методике, примененной для КТ 1а, в таблице 3.10.

Таблица 3.10.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 7

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень акустического сигнала, L_{C_i}	Уровень акустического шума в контрольной точке $L_{ш_i}$, дБ	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(с+ш)i}$,	Отношение сигнал/шум в октавных полосах, E_i	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, R	Показателя противодействия APP, W
КТ 7								
1	250	51,78	50,53	54,21	1,25	0,0025	0,5022	0,994
2	500	48,11	42,47	49,16	5,64	0,0297		
3	1000	46,54	40,16	47,44	6,38	0,0832		
КТ 7								
4	2000	44,59	37,03	45,29	7,56	0,1654	0,5022	0,994
5	4000	46,11	28,29	46,17	17,81	0,2214		

Сравнив полученные в результате расчетов значения показателя противодействия APP с нормированными значениями, можно сделать вывод о невыполнении норм по защите информации от утечки по акустическому каналу. Поэтому необходимо применение мер по защите информации и предотвращения утечки информации по акустическому каналу.

3.3. Оценка эффективности защиты информации от утечки информации по виброакустическому каналу

Для оценки защищенности применен комплекс «Спрут-7М» [37] и установлен режим измерения виброакустических сигналов, в качестве датчика использован акселерометр. Примеры крепления вибродатчика приведены на рис. 3.11.

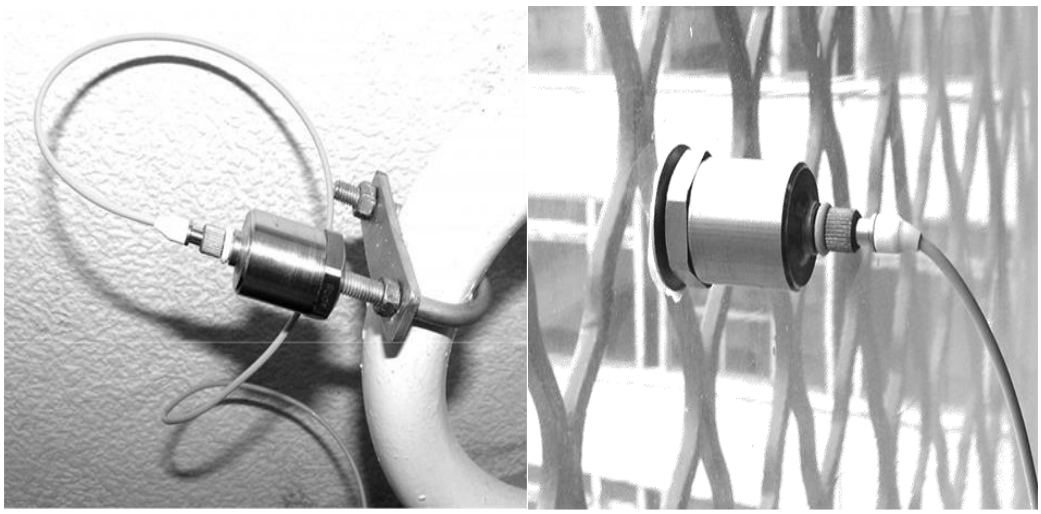

Рис. 3.11. Пример крепления вибродатчика на трубе и стеклянной поверхности

Необходимо выбрать контрольные точки на внешних поверхностях ограждающих конструкций:

КТ 1–дверь;

КТ 2 – на стене со стороны коридора;

КТ 3 – на стене со стороны окна;

КТ 4, КТ 5 – на стенах, граничащих с соседними кабинетами;

КТ 6 – на потолке;

КТ 7 – на полу;

КТ 8а, КТ 8б – на выходах за пределы помещения труб отопления;

КТ 9а, КТ 9б – на окне.

По виброакустическому каналу измерения проводятся аналогично измерениям по акустическому каналу, только в качестве приемника сигнала выступит акселерометр. Следует отметить, что крепление акселерометра к мягким поверхностям таким, как штукатура, не допускается. Это вызвано ослаблением виброколебаний данными веществами.

В результате инструментального контроля получены следующие данные по виброакустическому сигналу для контрольной точки № 1 (дверь) представлены в таблице 3.11.

Таблица 3.11.

Результаты измерений в контрольной точке К1 (дверь)

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ
1	250	47,22	54,24
2	500	45,43	55,39
3	1000	48,29	53,31
4	2000	43,57	49,81
5	4000	42,17	50,65

1. Вычисляем уровень акустического сигнала в КТ1 для пяти октавных полос по формуле:

$$V_{C_i} = 10\lg\{10^{0,1V_{(с+ш)_i}} - 10^{0,1V_{ш_i}}\}$$

$$V_{C_1} = 10\lg\{10^{0,1*54,24} - 10^{0,1*47,22}\} = 53,28 \text{ дБ}$$
$$V_{C_2} = 10\lg\{10^{0,1*55,39} - 10^{0,1*45,43}\} = 54,93 \text{ дБ}$$
$$V_{C_3} = 10\lg\{10^{0,1*53,31} - 10^{0,1*48,29}\} = 51,67 \text{ дБ}$$
$$V_{C_4} = 10\lg\{10^{0,1*49,81} - 10^{0,1*43.57}\} = 48,63 \text{ дБ}$$
$$V_{C_5} = 10\lg\{10^{0,1*50,65} - 10^{0,1*42,17}\} = 49,99 \text{ дБ}$$

2. Рассчитаем отношение сигнал/шум в октавных полосах:

$$E_i = V_{c_i} - V_{ш_i}$$
$$E_1 = 53,28 - 47,22 = 6,06 \text{ дБ}$$
$$E_2 = 54,41 - 45,43 = 9,49 \text{ дБ}$$
$$E_3 = 51,67 - 48,29 = 3,38 \text{ дБ}$$
$$E_4 = 48,63 - 43,57 = 5,06 \text{ дБ}$$
$$E_5 = 49,99 - 42,17 = 7,82 \text{ дБ}$$

3. Вычисляются октавные индексы артикуляции речи:

$$r_i = K_i \left| z - \frac{0,78 + 5,46exp[-4,3 * 10^{-3}(27,3 - |E_i - A_i|)^2]}{1 + 10^{0,1|E_i - A_i|}} \right|$$

где $z = \begin{cases} 0, \text{если } E_i \le A_i \\ 1, \text{если } E_i > A_i \end{cases}$

$$r_1 = 0.03 \left| 0 - \frac{0,78 + 5,46exp[-4,3 * 10^{-3}(27,3 - |6,06 - 18|)^2]}{1 + 10^{0,1|6,06-18|}} \right|$$
$$r_1 = 0,04498$$

$$r_2 = 0.12 \left| 0 - \frac{0,78 + 5,46exp[-4,3 * 10^{-3}(27,3 - |9,49 - 14|)^2]}{1 + 10^{0,1|9,49-14|}} \right|$$
$$r_2 = 0,04286$$

$$r_3 = 0,2 \left| 0 - \frac{0,78 + 5,46exp[-4,3 * 10^{-3}(27,3 - |3,38 - 9|)^2]}{1 + 10^{0,1|3,38-9|}} \right|$$
$$r_3 = 0,06469$$

$$r_4 = 0,3 \left| 0 - \frac{0,78 + 5,46exp[-4,3 * 10^{-3}(27,3 - |5,06 - 6|)^2]}{1 + 10^{0,1|5,06-6|}} \right|$$
$$r_4 = 0,14122$$

$$r_5 = 0,26 \left| 1 - \frac{0,78 + 5,46exp[-4,3 * 10^{-3}(27,3 - |7,82 - 6|)^2]}{1 + 10^{0,1|7,82-6|}} \right|$$
$$r_5 = 0,15335$$

4. Рассчитывается интегральный индекс артикуляции речи:

$$R = \sum_{i=1}^{5} r_i$$

$$R = 0,04498 + 0,04286 + 0,06469 + 0,14122 + 0,15335 = 0,4471$$

5. Рассчитывается значение показателя противодействия АРР:

$$W = \begin{cases} 1{,}54R^{0{,}25}[1 - \exp(-11R)], & \text{если } R < 0{,}15 \\ 1 - exp\left(-\dfrac{11R}{1 + 0{,}7R}\right), & \text{если } R \geq 0{,}15 \end{cases}$$

Так как $R \geq 0{,}15$, то для расчета W применяется следующее выражение:

$$W = 1 - exp\left(-\frac{11 * 0{,}4471}{1 + 0{,}7 * 0{,}4471}\right) = 0{,}99131$$

Данная методика расчета значений показателя противодействия используется и для остальных контрольных точек. В таблице 3.12 приведены значения, полученные в КТ 2 и КТ 3.

Таблица 3.12.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 2, КТ 3

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, R	Показателя противодействия АРР, W
КТ 2								
1	250	23,17	35,87	35,63	12,46	0,0098	0,6811	0,9977
2	500	21,39	32,57	32,23	10,84	0,0479		
3	1000	19,74	37,54	37,47	17,73	0,1523		
4	2000	24,46	39,17	39,02	14,56	0,2272		
5	4000	17,15	40,99	40,97	23,82	0,2439		
КТ 3								
1	250	29,68	38,53	37,92	8,24	0,0064	0,6193	0,9968
2	500	26,14	37,39	37,05	10,91	0,0482		
3	1000	22,11	35,13	34,91	12,81	0,1242		
4	2000	17,95	34,84	34,75	16,79	0,2431		
5	4000	18,52	32,35	32,16	13,65	0,1974		

В таблице 3.13 приведены значения, полученные в результате инструментального контроля, в КТ 4 и КТ 5 (на стенах, граничащих с соседними кабинетами).

В таблице 3.14 приведены значения, полученные в результате инструментального контроля в КТ 6 и КТ 7 (на полу и потолке соответственно).

Таблица 3.13

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 4, КТ 5

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия APP, W
КТ 4								
1	250	38,35	45,06	44,02	5,69	0,0047	0,5611	0,9956
2	500	34,66	42,28	41,45	6,79	0,0334		
3	1000	27,14	40,63	40,43	13,29	0,1273		
4	2000	28,73	37,54	36,93	8,19	0,1709		
5	4000	20,57	39,18	39,12	18,55	0,2248		
КТ 5								
1	250	34,63	46,14	45,82	11,19	0,0087	0,6131	0,9967
2	500	33,89	44,75	44,38	10,49	0,0466		
3	1000	30,58	39,83	39,28	8,69	0,1018		
4	2000	19,74	38,72	38,67	18,93	0,2559		
5	4000	22,48	36,71	36,54	14,06	0,2001		

Таблица 3.14.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 6, КТ 7

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия APP, W
КТ 6								
1	250	31,46	43,17	42,87	11,41	0,0089	0,5734	0,9959
2	500	33,76	41,39	40,57	6,81	0,0334		
3	1000	26,31	39,74	39,54	13,23	0,1269		
4	2000	24,48	36,46	36,17	11,69	0,2036		
5	4000	20,85	35,15	34,99	14,14	0,2006		

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия APP, W
КТ 7								
1	250	30,27	39,62	39,08	8,81	0,0068	0,5959	0,9964
2	500	27,62	40,84	40,63	13,01	0,0563		
3	1000	23,31	37,92	37,79	15,48	0,1403		
4	2000	24,41	35,63	35,29	10,88	0,1963		
5	4000	20,48	34,13	33,94	13,46	0,1962		

Проведение измерения виброакустических характеристик системы отопления представлены на рис. 3.12.

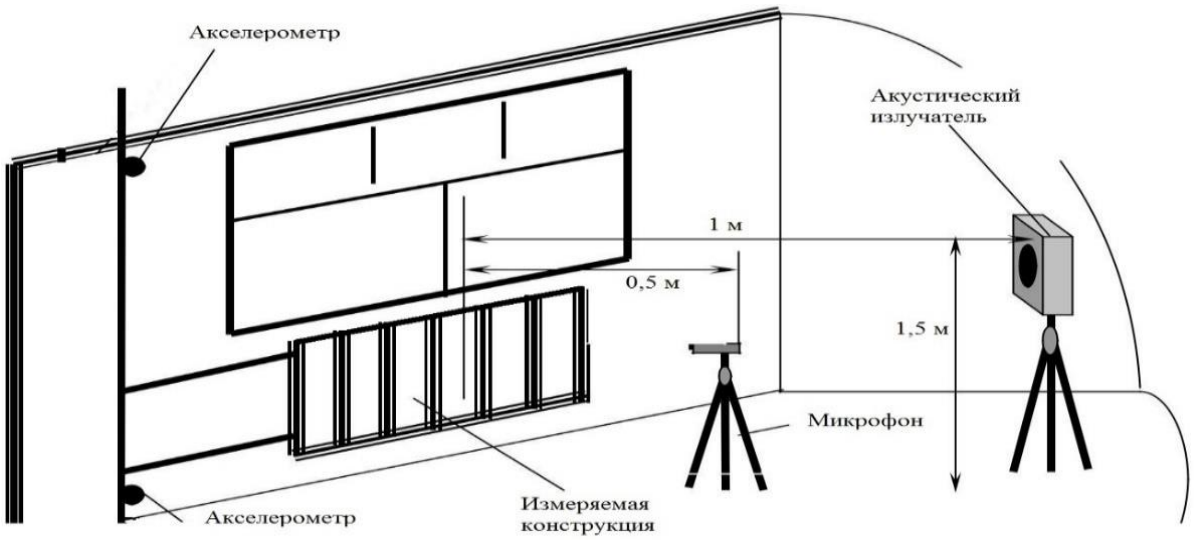

Рис. 3.12. Схема измерений системы отопления

В таблице 3.15 приведены значения, полученные в результате инструментального контроля, для КТ 8а, КТ 8б – на выходах за пределы помещения труб отопления.

Для оценки защищенности объекта информатизации от утечки информации по оптико-электронному каналу так же применен комплекс «Спрут 7» и установлен режим измерения виброакустических сигналов, в качестве датчика использован акселерометр [36]. Замер производится в верхней и нижней части односекторного окна, в КТ 9а и КТ 9б соответственно. Результаты измерений и расчет показателей приведен в таблице 3.16.

Таблица 3.15.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 8а, КТ 8б

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия APP, W
КТ 8а								
1	250	23,14	31,44	30,75	7,61	0,0059	0,7278	0,99817
2	500	22,87	33,95	33,59	10,73	0,0474		
3	1000	20,35	38,74	38,68	18,33	0,1552	0,7278	0,99817
4	2000	18,46	40,21	40,18	21,72	0,2699		
5	4000	16,41	42,62	42,61	26,2	0,2494		
КТ 8б								
1	250	25,51	32,46	31,48	5,97	0,0049	0,6286	0,99742
2	500	24,63	34,17	33,66	9,03	0,0411		
3	1000	23,82	41,24	41,16	17,34	0,1503		
4	2000	21,24	39,34	39,27	18,03	0,2508		
5	4000	24,11	40,18	40,07	15,96	0,2115		

Таблица 3.16.

Результаты определения отношений «сигнал/шум» в октавных полосах в КТ 9а, КТ 9б

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V_{(с+ш)_i}$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия APP, W
КТ 9а								
1	250	36,64	46,38	45,89	9,25	0,0071	0,7213	0,99811
2	500	34,02	50,27	50,16	16,15	0,0681		
3	1000	31,45	52,71	52,67	21,23	0,1679		
4	2000	29,36	49,37	49,33	19,97	0,2616		
5	4000	24,19	41,17	41,08	16,89	0,2166		

Номер октавной полосы, i	Среднегеометрическая частота октавной полосы, Гц	Уровень виброакустического шума, $V_{ш_i}$, дБ	Уровень суммарного виброакустического сигнала и шума, $V(с+ш)_i$, дБ	Уровень виброакустического сигнала, $V_{с_i}$, дБ	Отношение сигнал/шум в октавных полосах, E_i, дБ	Октавный индекс артикуляции речи, r_i	Интегральный индекс артикуляции речи, *R*	Показателя противодействия APP, W
КТ 9б								
1	250	33,24	45,81	45,56	12,32	0,0097		
2	500	34,16	50,11	49,99	15.84	0,0669		
3	1000	31,75	49,94	49,87	18,12	0,1542	0,6232	0,99689
4	2000	30,93	46,39	46,27	15,34	0,2329		
5	4000	26,14	35,27	34,69	8,56	0,1595		

Сравнив результаты расчетов значения показателя APP противодействия, полученные при измерениях с нормированными, можно сделать вывод о невыполнении норм и возможной утечки защищаемой информации.

Таким образом, в результате оценки защищенности объекта информатизации от утечки информации по виброакустическому каналу можно подвести итог: возможность утечки речевой информации через ограждающие конструкции существует.

Вопросы и задания для самоконтроля:

1. Что такое защита информации от несанкционированного доступа?
2. Что такое защищаемое помещение?
3. Дайте понятие контролируемой зоне.
4. Что такое основные технические средства и системы (ОТСС)?
5. Что такое вспомогательные технические средства и системы (ВТСС)?
6. Приведите примеры ОТСС.
7. Приведите примеры ВТСС.
8. Что такое канал связи.
9. Опишите электромагнитный ТКУИ.
10. Опишите электрический ТКУИ.
11. Опишите индукционный ТКУИ.
12. Как классифицируют технические каналы утечки информации, обрабатываемой основными техническими средствами и системами?
13. Как образуется параметрический ТКУИ?
14. Как образуются электрические каналы утечки?
15. Дайте понятие акустоэлектрическим преобразователям.
16. Какие случайные акустоэлектрические преобразователи относятся к наиболее распространенным?
17. Какие выделяют три вида паразитной связи?

18. Дайте определение термина «объект информатизации». Приведите примеры объектов информатизации, предназначенных для обработки информации в ОВД.

19. Поясните значение терминов «Основные технические средства обработки информации (ОТСС)». Вспомогательные технические средства обработки информации (ВТСС). Контролируемая зона.

20. Составьте описание Защищаемого помещения территориального органа МВД России (этаж, площадь, наличие окон, батарей и т.д.) и нарисуйте структурную схему.

21. Дайте определение термина «технический канал утечки информации». Нарисуйте схему образования ТКУИ.

22. Определите местоположение технических каналов утечки речевой информации (прямой акустический, виброакустический, акустоэлектрический, оптико-электронный) на составленной схеме.

23. Заполните таблицу, сопоставив технические каналы утечки информации и используемые технические средства.

Технические каналы утечки информации	**Специальные технические средства, используемые для перехвата информации**
1. Прямой акустический	
2. Виброакустический	
3. Акустоэлектрический	
4. Оптико-электронный	

а) лазерные акустические локационные системы, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны;

б) электронные стетоскопы, установленные в смежных помещениях, принадлежащих другим организациям;

в) направленные микрофоны, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны;

г) электронные устройства перехвата речевой информации с датчиками контактного типа, установленные на инженерно-технических коммуникациях (трубы водоснабжения, отопления, канализации, воздуховоды и т.п.) и внешних ограждающих конструкциях (стены, потолки, полы, двери, оконные рамы и т.п.) выделенного помещения, при условии неконтролируемого доступа к ним посторонних лиц;

д) специальные высокочувствительные микрофоны, установленные в воздуховодах или в смежных помещениях, принадлежащих другим организациям;

е) аппаратура «высокочастотного навязывания», подключаемая к соединительным линиям ВТСС, обладающим «микрофонным» эффектом, за пределами контролируемой зоны;

ж) электронные устройства перехвата речевой информации с датчиками микрофонного типа, установленные в воздуховодах, при условии неконтролируемого доступа к ним посторонних лиц;

з) специальные радиоприемные устройства, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, перехватывающие ПЭМИ на частотах работы высокочастотных генераторов, входящих в состав ВТСС, обладающих «микрофонным» эффектом;

и) аппаратура «высокочастотного облучения», установленная в ближайших строениях или смежных помещениях, находящихся за пределами контролируемой зоны;

к) прослушивание разговоров, ведущихся в выделенном помещении, без применения технических средств посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных с выделенным помещениях (непреднамеренное прослушивание);

л) специальные низкочастотные усилители, подключаемые к соединительным линиям ВТСС, обладающим «микрофонным» эффектом, за пределами контролируемой зоны.

24. Определить активные и пассивные методы защиты речевой информации, применительно к рассматриваемому объекту информатизации Защищаемому помещению.

25. Определить способы получения видовой информации по оптическим каналам утечки информации, применительно к рассматриваемому объекту информатизации Защищаемому помещению.

26. Определить методы защиты видовой информации по оптическим каналам утечки информации, применительно к рассматриваемому объекту информатизации Защищаемому помещению, и указать их на схеме.

27. Используя таблицу «Государственный реестр сертифицированных средств защиты информации», размещенную на официальном сайте ФСТЭК России, определить технические средства защиты речевой информации от утечки по техническим каналам (прямой акустический, виброакустический, акустоэлектрический, оптико-электронные), применительно к рассматриваемому объекту информатизации Защищаемому помещению и разместить их на схеме.

ГЛАВА 4. ОРГАНИЗАЦИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОМВД РОССИИ

4.1. Выбор средств защиты информации от утечки информации по электромагнитному каналу

Создавая систему защиты информации на стадии уже построенного и функционирующего здания отдела ОМВД России, применять инженерно-строительные конструкции для защиты информации не представляется выгодным и действенным решением, из-за трудоёмкости предстоящих работ, экономических затрат и результирующего эффекта. Возникает объективная необходимость применения активных средств защиты информации от утечки по электромагнитному каналу - генераторов шума (ГШ) [35].

Для выбора генератора шума, составим таблицу 4.1, в которой приведено наименование технических средств и их характеристики, в соответствие с которыми будет произведен выбор генератора шума.

Таблица 4.1

Характеристики генераторов шума

Наименование технического средства	Сертификат ФСТЭК (номер, срок действия)	Рабочий диапазон	Цена СЗИ (руб.)
ГШ -2500МС	№ 3545 до 14.04.2019	00,1 … 2000 МГц	17 700
ГШ-К-1800МС	№ 3631 до 30.09.2019	0,1 … 1800 МГц	15 500
ЛГШ-501	№ 753 до 16.05.2018	0,01 до 1800 МГц	19 800

Проанализировав представленные в таблице 4.1 данные, проведем сравнительный анализ с целью выбора подходящего генератора шума. Все представленные средства защиты имеют сертификат ФСТЭК, однако стоит обратить внимание на сроки и данные о продлении сертификатов: применение средств защиты информации может быть не рационально, в виду возможного скорого прекращения сертификата ФСТЭК. Рабочий диапазон имеет широкую полосу частот генератор шума ГШ-2500МС. Самым экономически выгодным решением является ГШ-К-1800МС. Однако, он подсоединяется ко входу материнской платы персонального компьютера, что осложняет его эксплуатацию. Решающим фактором при выборе генератора шума при схожести остальных параметров является широкий диапазон частот и приемлемая цена, а также понятный и удобный в эксплуатации интерфейс блока управления. Поэтому был выбран для обеспечения защиты информации от утечки по электромагнитному каналу утечки информации ГШ -2500МС (рис. 4.1).

Рис. 4.1. Внешний вид генератора шума ГШ -2500МС

Генератор шума ГШ-2500МС служит для маскировки информативных побочных электромагнитных излучений и наводок (ПЭМИН) средств ВТ путем формирования и излучения в окружающее пространство шума в широком спектре частот, что позволяет одному генератору обеспечивать защиту информации средств вычислительной техники, размещенной в помещении площадью ~ 40 м^2.

4.2. Выбор средств защиты информации от осуществления несанкционированного доступа к информации

Наиболее эффективное обеспечение защиты средств ВТ и АС от несанкционированного доступа может осуществляться системами разграничения доступа (СРД). Данные функции при различной их реализации представлены в средствах защиты информации от НСД. Для выбора конкретного средства защиты информации следует произвести сравнительный анализ, представленных на российском рынке средств защиты информации и имеющих сертификат ФСТЭК. Выделим используемые в ОВД средства защиты информации (СЗИ) от НСД и обозначим основные особенности:

1. Страж NT 4.0;
2. Secret Net 7;
3. Dallas Lock 8.0 (C).

СЗИ «Страж NT» может применяться на персональных компьютерах в настольном исполнении, портативных компьютерах, промышленных компьютерах, серверах, в том числе и в составе кластера. СЗИ «Страж NT» может устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена и серверах. Для этого СЗИ проблемы встречаются редко, что может говорить о дружелюбном к пользователю механизму защиты.

При осуществлении сравнения средств защиты информации учитываются характерные функциональные возможности и особенности технических средств, а также мнение привлеченных экспертов, задействованных из состава практических сотрудников ОВД.

Для решения задачи выбора средства защиты необходимо составить таблицу, в которой обозначим наличие у конкретной СЗИ основных функции защиты от НСД. В результате сравнения показателей будет определен приемлемый вариант.

Исследуется задача выбора средств защиты информации в АС. Для этого составлены следующие оценочные критерии эффективности средств защиты информации от НСД:

I. использование средств аппаратной поддержки;

II. шифрование пользовательской информации;

III. осуществление аудита событий;

IV. контроль целостности ресурсов;

V. возможность настройки замкнутой программной среды;

VI. стоимость средств защиты;

VII. личные предпочтения администратора безопасности;

VIII. поддержка аутентификации.

Результаты оценивания приведены в таблице 4.2.

Таблица 4.2

Выбор средства защиты информации

Средства защиты	Оценочные критерии								Итого
	I	II	III	IV	V	VI	VII	VIII	
Secret Net 7(без платы Secret net touch memory)	1	0	3	4	5	3	3	5	24
Secret Net 7 (с платой Соболь)	5	0	3	5	5	5	4	5	32
Dallas Lock 8C	1	5	5	5	5	4	4	5	34
Страж NT 3.0	1	1	5	5	5	3	4	5	29

Таким образом, применяя метод экспертной оценки, получили суммарные результаты, на основании которых можно сделать вывод, что подходящим средством защиты от НСД на ОИ ОМВД России является Dallas Lock версия 8C.

Помимо СЗИ от НСД необходимо применение средства антивирусной защиты. Руководствуясь анализом ситуации, сложившейся в практических органах системы МВД России, можно констатировать, что в МВД используется антивирусное программное средство «Антивирус Касперского». Поэтому для защиты АС от несанкционированного воздействия вредоносных программ необходимо установить Endpoint Security 10 [19].

Программное изделие «Kaspersky Endpoint Security 10» является средством антивирусной защиты и предназначено для защиты от вредоносных компьютерных программ, в том числе в системах обработки данных и

государственных информационных системах органов государственной власти Российской Федерации.

Функциональные возможности Kaspersky Endpoint Security 10:

- аудит безопасности;
- управление безопасностью;
- проверки объектов заражения;
- методы проверок объектов заражения;
- обработка объектов, подвергшихся воздействию;
- блокирование;
- сигнализация;
- восстановление объектов.

Перед установкой необходимо проанализировать аппаратные и программные требования, предъявляемые к рабочей станции, для корректной работы и реализации всех заявленных разработчиком функций.

4.3. Выбор средств защиты информации от утечки информации по акустическому каналу

Организационным мероприятием по защите объекта от утечки речевой информации по акустическому и виброакустическому каналам является создание инструкции по эксплуатации объекта информатизации [26]. В ней предусмотрено назначение ответственных лиц и закрепление за ними обязанностей по проведению переговоров, содержащих сведения ограниченного доступа, и работе с АС. Эти функциональные обязанности должны включать проверку включения и работоспособности средств активной защиты информации на ОИ, а также плотное закрытие форточки окна и двери во время проведения переговоров.

Технической мерой обеспечения защиты объекта является установка систем активного зашумления. На отечественном рынке представлен широкий спектр данных устройств, отличающихся техническими особенностями, ценой, частотным диапазоном и другими характеристиками. Для выбора системы защиты информации по акустическому и виброакустическому каналам проведем анализ следующих, представленных в таблице 4.3 технических средств.

Таблица 4.3.

Сравнительные характеристики средств акустической защиты

Характеристика \ СЗИ	Камертон-3	«Соната-АВ» модель 3М	«Шорох-3»
Сертификат ФСТЭК	+	+	+
Диапазон частот (Гц)	90 – 11200	90 – 11 200	180 – 11200
Цена (руб.)	28200	21 240	29 500

Для защиты информации от утечки по акустическому и виброакустическому каналам из рассмотренных в таблице средств наиболее подходит «Соната АВ». Данное средство защиты имеет сертификат ФСТЭК рассчитан на более длительное время использования по сравнению с остальными техническими средствами. Также «Соната» является простой в установке и настройке, а также у действующих сотрудников по технической защите ОМВД России имеется значительной опыт в эксплуатации данного технического средства. Учитывая приемлемую цену при прочих равных технических характеристик, предлагается использовать систему акустической и виброакустической защиты «Соната-АВ» модель 3М в составе:

- аудиоизлучатель АИ – 3М;
- «тяжёлый» виброизлучатель ВИ – 3М;
- «лёгкий» виброизлучатель (пьезоизлучатель) ПИ – 3М;
- генераторный блок: Соната АВ, модель 3М.

Состав изделия Соната АВ, модель 3М представлен на рисунке 4.2.

аудиоизлучатель АИ-3М

«Тяжелый» виброизлучатель ВИ- 3М

«Легкий» виброизлучатель ПИ-3М

Генераторный блок: Соната АВ, модель 3М

Рис. 4.2. Состав системы «Соната АВ»

Типовая модель подключения компонентов системы «Соната АВ» продемонстрирована на рис. 4.3.

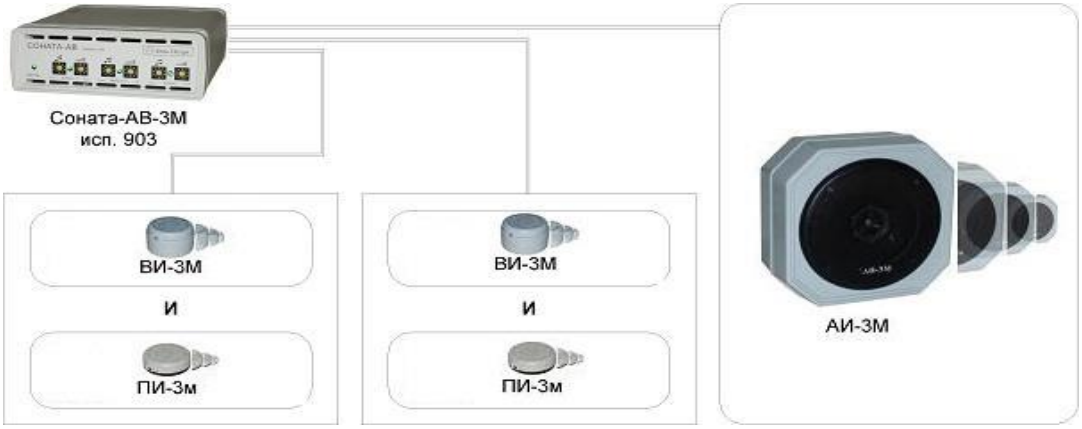

Рис. 4.3. Модель подключения изделий Соната АВ, модель 3М

Виды креплений, используемые при установке излучателей системы «Соната АВ», представлены в таблице 4.4.

Таблица 4.4.

Виды фиксаторов виброизлучателей системы «Соната АВ»

		
Тип 1	Тип 2	Тип 3
		
Тип 4	Тип 4м	Крепление фиксатора тип 4м на стекле (склейка)

Итак, в таблице 4.5 указано количество виброизлучателей и аудиоизлучателей для ОИ ОМВД России в соответствии с представленными нормами.

Таблица 4.5

Потребность в компонентах системы «Соната»

Ограждающая конструкция	Излучатели			Крепления	
	Кол-во ВИ	Кол-во АИ	Кол-во ПИ	Тип	Кол-во
Стена №1	1	-	-	Тип 1	1
Стена №2	1	-	-	Тип 1	1
Стена №3	1	-	-	Тип 1	1
Стена №4	1	-	-	Тип 1	1
Верхнее перекрытие	1	-	-	Тип 1	1
Нижнее перекрытие	1	-	-	Тип 1	1
Окна	-	-	1	Тип 4м	1
Дверь	-	1	-	-	-
Трубы	2	-	-	Тип 3	2

Для защиты информации от утечки по оптико-электронному каналу утечки информации применили возможности, рассмотренного средства защиты информации – Соната АВ, модель 3М. В составе данного СЗИ входит пьезоизлучатель ПИ-3М.

Пьезоизлучатели ПИ-3М используются для активной виброакустической защиты ограждающих остеклений и легких межкомнатных перегородок.

4.4. Выбор средств защиты информации от утечки информации по виброакустическому каналу

На основании полученного результата необходимо принять меры для защиты объекта информатизации. Технической мерой обеспечения защиты объекта может быть установка систем активного зашумления или использование, например, сертифицированного ФСТЭК комплекса виброакустической защиты помещения «Соната АВ-4Б», состоящего из устройств СВ-4Б, СА-4Б, Соната ИП-4.3, Соната-ДУ-4.3 и набора креплений для установки.

«Соната СА-4Б» - акустический генератор излучатель нового поколения для установки в запотолочном пространстве, дверных тамбурах, системах вентиляции. Является составной частью системы виброакустической защиты для выделенных помещений и защиты от прослушивания кабинетов первых лиц и переговорных комнат.

Электропитание и управление подключаемыми к выходу «Нагрузка» элементами системы активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б (Системы) в ходе ее эксплуатации осуществляется с помощью источника питания «Соната ИП-4.3» [37].

В качестве активного средства (генератор шума) виброакустической защиты 1 класса комбинированного типа может быть использован комплекс SEL SP-157 «Шагрень» [56]. Для защиты объектов информатизации 1

категории и противодействия техническим средствам перехвата речевой информации по виброакустическим каналам применяется комплекс виброакустической защиты «Барон» [35].

Организационным мероприятием по защите объекта от утечки речевой информации по акустическому и виброакустическому каналам является создание инструкции по эксплуатации объекта информатизации. В ней необходимо предусмотреть назначение ответственных лиц и закрепление за ними обязанностей по проведению переговоров, содержащих сведения ограниченного доступа, и работе с автоматизированными средствами (АС). Эти функциональные обязанности должны включать проверку включения и работоспособности средств активной защиты информации на объекте информатизации, а также плотное закрытие форточки окна и двери во время проведения переговоров.

4.5. Средства защиты баз данных

Средства защиты БД в различных СУБД несколько отличаются друг от друга. На основе анализа современных СУБД можно утверждать, что средства защиты БД условно делятся на две группы: основные и дополнительные.

К *основным средствам защиты* информации можно отнести следующие средства:

- парольной защиты;
- шифрования данных и программ;
- установления прав доступа к объектам БД;
- защиты полей и записей таблиц БД.

Парольная защита представляет простой и эффективный способ защиты БД от несанкционированного доступа. Пароли устанавливаются конечными пользователями или администраторами БД. Учет и хранение паролей производится самой СУБД. Обычно пароли хранятся в определенных системных файлах СУБД в зашифрованном виде. Поэтому просто найти и определить пароль невозможно. После ввода пароля пользователю СУБД предоставляются все возможности по работе с защищенной БД. Саму СУБД защищать паролем большого смысла нет.

Шифрование данных (всей базы или отдельных таблиц) применяют для того, чтобы другие программы, «знающие формат БД этой СУБД», не могли прочитать данные. Такое шифрование (применяемое в Microsoft Access), по-видимому, дает немного, поскольку расшифровать БД может любой с помощью «родной» СУБД. Если шифрация и дешифрация требуют задания пароля, то дешифрация становится возможной при верном вводе пароля.

Шифрование исходных текстов программ позволяет скрыть от несанкционированного пользователя описание соответствующих алгоритмов [11].

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления *прав доступа* к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта

(пользователь, создавший объект), а также администратор БД имеют все права. Остальные пользователи к разным объектам могут иметь различные уровни доступа.

По отношению к таблицам в общем случае могут предусматриваться следующие права доступа:

– просмотр (чтение) данных;
– изменение (редактирование) данных;
– добавление новых записей;
– добавление и удаление данных;
– все операции, в том числе изменение структуры таблицы.

К данным, имеющимся в таблице, могут применяться меры защиты по отношению к отдельным полям и отдельным записям. В известных нам реляционных СУБД, отдельные записи специально не защищаются, хотя, можно привести примеры из практики, когда это требуется. Контроль прав доступа, по-видимому, должен быть в объектно-ориентированных СУ БД, в которых есть идентификация отдельных записей (одно из отличий объектно-ориентированной модели от реляционной) [50].

Применительно к защите данных в полях таблиц можно выделить следующие уровни прав доступа:

– полный запрет доступа;
– только чтение;
– разрешение всех операций (просмотр, ввод новых значений, удаление и изменение).

По отношению к формам могут предусматриваться две основные операции: вызов для работы и разработка (вызов Конструктора). Запрет вызова Конструктора целесообразно делать для экранных форм готовых приложений, чтобы конечный пользователь случайно не испортил приложение. В самих экранных формах отдельные элементы могут быть тоже защищены. Например, некоторые поля исходной таблицы вообще могут отсутствовать или скрыты от пользователя, а некоторые поля - доступны для просмотра [58].

Отчеты во многом похожи на экранные формы, за исключением следующего. Во-первых, они не позволяют изменять данные в таблицах, а во-вторых, основное их назначение - вывод информации на печать. На отчеты, также, как и на экранные формы, может накладываться запрет на вызов средств их разработки.

Для исключения просмотра и модификации (случайной и преднамеренной) текстов программ, используемых в приложениях СУБД, помимо шифрации, может применяться их парольная защита.

К *дополнительным средствам защиты* БД можно отнести такие, которые нельзя прямо отнести к средствам защиты, но которые непосредственно влияют на безопасность данных. Их составляют следующие средства:

– встроенные средства контроля значений данных в соответствии с типами;

– повышения достоверности вводимых данных;

– обеспечения целостности связей таблиц;

– организации совместного использования объектов БД в сети.

Редактируя БД, пользователь может случайно ввести такие значения, которые не соответствуют типу поля, в которое это значение вводится. Например, в числовое поле пытаться занести текстовую информацию. В этом случае СУБД с помощью *средств контроля значений* блокирует ввод и сообщает пользователю об ошибке звуковым сигналом, изменением цвета вводимых символов или другим способом.

Средства повышения достоверности вводимых значений в СУБД служат для более глубокого контроля, связанного с семантикой обрабатываемых данных. Они обычно обеспечивают возможность при создании таблицы указывать следующие ограничения на значения: минимальное и максимальное значения; значение; принимаемое по умолчанию (если нет ввода), требование обязательного ввода; задание маски (шаблона) ввода; указание дополнительной сверочной таблицы, по которой ведется контроль вводимых значений и т.д.

Более совершенной формой организации контроля достоверности информации в БД является разработка хранимых процедур. Механизм хранимых процедур применяется в БД, размещенных на сервере. Сами хранимые процедуры представляют собой программы, алгоритмы которых предусматривают выполнение некоторых функций (в том числе контрольных) над данными. Процедуры хранятся вместе с данными и при необходимости вызываются из приложений, либо при наступлении некоторых событий в БД [67].

Решение прикладной задачи, как правило, требует информации из нескольких таблиц. Сами таблицы для удобства обработки и исключения дублирования информации некоторым образом связываются. Функции поддержания *логической целостности связанных таблиц* берет на себя СУБД. К сожалению, далеко не все СУБД в полной мере реализуют эти функции, в этом случае ответственность за корректность связей возлагается на приложение.

Приведем пример возможных действий СУБД по контролю целостности связей таблиц. Пусть между двумя таблицами существует связь вида 1:М и, следовательно, одной записи основной таблицы может соответствовать несколько записей вспомогательной таблицы.

При вставке записей во вспомогательную таблицу система контролирует наличие соответствующих значений в поле связи основной таблицы. Если вводимое значение отсутствует в основной таблице, СУБД временно блокирует работу с новой записью и предлагает изменить значение или удалить запись целиком.

Удаление записей дополнительных таблиц проходит «безболезненно», чего не скажешь о записях основной таблицы. В случае, когда запись основной

таблицы связана с несколькими записями дополнительной таблицы, возможны два варианта поведения: не удалять основной записи, пока имеется хотя бы одна подчиненная запись (записи должен удалять пользователь), либо удалить основную запись и все подчиненные записи (каскадное удаление).

В многооконных системах (почти все современные программы) и, тем более, в распределенных информационных системах, работающих с базами данных, возникает проблема разрешения конфликтов между различными действиями над *одними и теми же объектами (совместного использования объектов БД)*. Например, что делать в случае, когда один из пользователей локальной сети редактирует БД, а другой хочет изменить се структуру? Для таких ситуаций в СУБД должны быть предусмотрены механизмы разрешения конфликтов.

Обычно при одновременной работе нескольких пользователей сети, а также работе нескольких приложений на одном компьютере или работе в нескольких окнах СУБД используются блокировки.

Блокировки могут действовать на различные объекты БД и на отдельные элементы объектов. Очевидной ситуацией блокировки объектов БД является случай одновременного использования объекта и попытки входа в режим разработки этого же объекта. Применительно к таблицам баз данных дополнительные блокировки могут возникать при работе с отдельными записями или полями.

Блокировки бывают явные и неявные. Явные блокировки накладываются пользователем или приложением с помощью команд. Неявные блокировки организует сама система, чтобы избежать возможных конфликтов. Например, в случае попытки изменения структуры БД во время редактирования информации устанавливается запрет реструктурирования БД до завершения редактирования данных [68].

Управление распределенными данными. С управлением данными в распределенных системах связаны следующие две группы проблем: поддержка соответствия БД вносимым изменениям и обеспечение совместного доступа нескольких пользователей к общим данным.

Поддержка соответствия БД вносимым изменениям. В современных распределенных системах информация может храниться *централизовано* или *децентрализовано.* В первом случае проблемы идентичности представления информации для всех пользователей не существует, так как все последние изменения хранятся в одном месте. На практике чаще информация изменяется одновременно в нескольких узлах распределенной вычислительной системы. В этом случае возникает проблема контроля за всеми изменениями информации и предоставления ее в достоверном виде всем пользователям.

Существуют две основные технологии децентрализованного управления БД: *распределенных БД* (Distributed Database) и *тиражирования, или репликации, БД* (Data Replication).

Распределенная БД состоит из нескольких фрагментов, размещенных на разных узлах сети и, возможно, управляемых разными СУБД. С точки

зрения программ и пользователей, обращающихся к распределенной БД, последняя воспринимается как единая локальная БД (рис. 4.4).

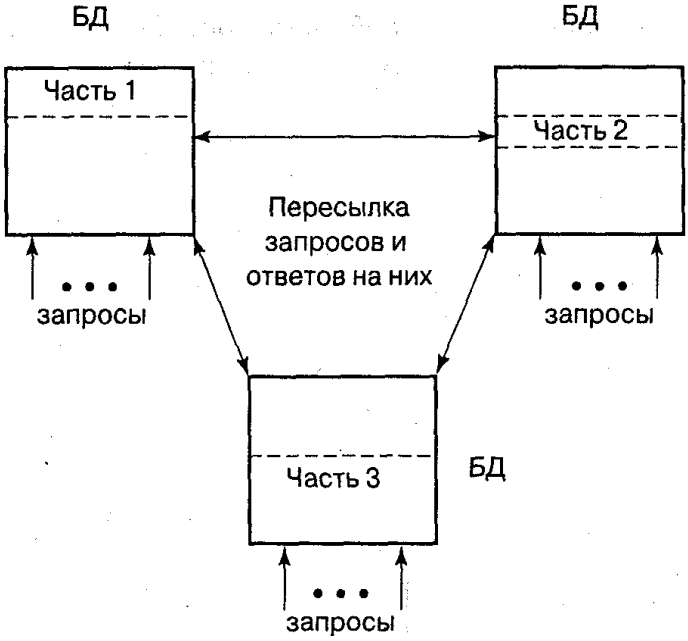

Рис. 4.4. Модель распределенной БД

Информация о местоположении каждой из частей распределенной БД и другая служебная информация хранится в так называемом *глобальном словаре данных.* В общем случае этот словарь может храниться на одном из узлов или тоже быть распределенным.

Для обеспечения корректного доступа к распределенной БД в современных системах чаще всего применяется протокол (метод) *двухфазной фиксации транзакций* (two-phase commit). Суть этого метода состоит в двухэтапной синхронизации выполняемых изменений на всех задействованных узлах. На первом этапе в узлах сети производятся изменения (пока обратимые) в их БД, о чем посылаются уведомления компоненту системы, управляющему обработкой распределенных транзакций.

На втором этапе, получив от всех узлов сообщения о правильности выполнения операций (что свидетельствует об отсутствии сбоев и отказов аппаратно-программного обеспечения), управляющий компонент выдает всем узлам команду фиксации изменений. После этого транзакция считается завершенной, а ее результат необратимым.

Основным *достоинством* модели распределенной БД является то, что пользователи всех узлов (при исправных коммуникационных средствах) получают информацию с учетом всех последних изменений. Второе достоинство состоит в экономном использовании внешней памяти компьютеров, что позволяет организовывать БД больших объемов.

К *недостаткам* модели распределенной БД относится следующее: жесткие требования к производительности и надежности каналов связи, а также большие затраты коммуникационных и вычислительных ресурсов из-за их связывания на все время выполнения транзакций. При интенсивных обращениях к распределенной БД, большом числе взаимодействующих узлов,

низкоскоростных и ненадежных каналах связи обработка запросов по этой схеме становится практически невозможной [43].

Модель ***тиражирования данных,*** в отличие от технологии распределенных БД, предполагает дублирование данных (создание точных копий) в узлах сети (рис. 4.5).

Данные всегда обрабатываются как обычные локальные. Поддержку идентичности копий друг другу в асинхронном режиме обеспечивает компонент системы, называемый *репликатором* (replicator). При этом между узлами сети могут передаваться как отдельные изменения, так и группы изменений. В течение некоторого времени копии БД могут отличаться друг от друга.

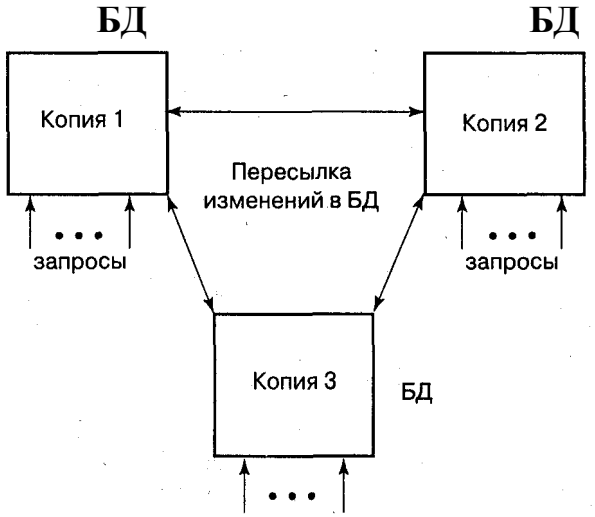

Рис. 4.5. Модель тиражирования БД

К основным *достоинствам* модели тиражирования БД (в сравнении с предыдущей моделью) относятся: более высокая скорость доступа к данным, так как они всегда есть в узле; существенное уменьшение передаваемого по каналам связи потока информации, поскольку происходит передача не всех операций доступа к данным, а только изменений в БД; повышение надежности механизмов доступа к распределенным данным, поскольку нарушение связи не приводит к потере работоспособности системы (предполагается буферизация потока изменений, позволяющая корректно возобновить работу после восстановления связи).

Основной *недостаток* модели тиражирования БД заключается в том, что на некотором интервале времени возможно «расхождение» копий БД. Если отмеченный недостаток некритичен для прикладных задач, то предпочтительно иметь схему с тиражированием БД.

Доступ к общим данным. При обслуживании обращений к общим данным средства управления БД должны обеспечивать по крайней мере два основных метода доступа: монопольный и коллективный. Основными объектами доступа в различных системах могут быть целиком БД, отдельные таблицы, записи, поля записей. В СУБД, предоставляющих возможность

разработки, объектами доступа также могут выступать спецификации отчетов и экранных форм, запросы и программы.

Монопольный доступ обычно используется в двух случаях:

– во-первых, когда требуется исключить доступ к объектам со стороны других пользователей (например, при работе с конфиденциальной информацией);

– во-вторых, когда производятся *ответственные* операции с БД, не допускающие других действий, например, изменение структуры БД.

В первом случае пользователь с помощью диалоговых средств СУБД или прикладной программы устанавливает явную *блокировку.* Во втором случае пользователь тоже может установить явную блокировку, либо положиться на СУБД. Последняя обычно автоматически устанавливает неявную (без ведома пользователя или приложения) блокировку, если это необходимо.

В режиме ***коллективного доступа*** полная блокировка на используемые объекты, как правило, не устанавливается. Коллективный доступ возможен, например, при одновременном просмотре таблиц. Попытки получить монопольный доступ к объектам коллективного доступа должны быть пресечены. Например, в ситуации, когда один или несколько пользователей просматривают таблицу, а другой пользователь собирается удалить эту же таблицу.

Для организации коллективного доступа в СУБД применяется ***механизм блокировок.*** Суть блокировки состоит в том, что на время выполнения какой-либо операции в БД доступ к используемому объекту со стороны других потребителей временно запрещается или ограничивается. Например, при копировании таблицы она блокируется от изменения, хотя и разрешено просматривать ее содержимое.

Рассмотрим некоторый типичный набор блокировок. В конкретных программах схемы блокирования объектов могут отличаться от описываемой. Выделим четыре вида блокировок, перечисленные в порядке убывания строгости ограничений на возможные действия:

– полная блокировка;

– блокировка от записи;

– предохраняющая блокировка от записи;

– предохраняющая полная блокировка.

Полная блокировка. Означает полное запрещение всяких операций над основными объектами (таблицами, отчетами и экранными формами). Этот вид блокировки обычно применяется при изменении структуры таблицы.

Блокировка от записи. Накладывается в случаях, когда можно использовать таблицу, но без изменения ее структуры или содержимого. Такая блокировка применяется, например, при выполнении операции слияния данных из двух таблиц.

Предохраняющая блокировка от записи. Предохраняет объект от наложения на него со стороны других операций полной блокировки, либо

блокировки от записи. Этот вид блокировки позволяет тому, кто раньше «захватил» объект, успешно завершить модификацию объекта. Предохраняющая блокировка от записи совместима с аналогичной блокировкой (предохраняющей блокировкой от записи), а также с предохраняющей полной блокировкой Примером необходимости использования этой блокировки является режим совместного редактирования таблицы несколькими пользователями.

Предохраняющая полная блокировка. Предохраняет объект от наложения на него со стороны других операций только полной блокировки. Обеспечивает максимальный уровень совместного использования объектов. Такая блокировка может использоваться, например, для обеспечения одновременного просмотра несколькими пользователями одной таблицы. В группе пользователей, работающих с одной таблицей, эта блокировка не позволит никому изменить структуру общей таблицы.

При незавершенной операции с некоторым объектом и запросе на выполнение новой операции с этим же объектом производится попытка эти операции совместить. Совмещение возможно тогда, когда совместимыми оказываются блокировки, накладываемые конкурирующими операциями.

В отношении перечисленных выше четырех блокировок действуют следующие правила совмещения:

– при наличии полной блокировки над объектом нельзя производить операции, приводящие хотя бы к одному из видов блокировок (полная блокировка несовместима ни с какой другой блокировкой);

– блокировка от записи совместима с аналогичной блокировкой и предохраняющей полной блокировкой;

– предохраняющая блокировка от записи совместима с обеими видами предохраняющих блокировок;

– предохраняющая полная блокировка совместима со всеми блокировками, кроме полной.

Обычно в СУБД каждой из выполняемых с БД операций соответствует определенный вид блокировки, которую эта операция накладывает на объект. Пользователям современных СУБД, работающим в интерактивном режиме, не нужно помнить все тонкости механизма блокировки, поскольку система достаточно «разумно» осуществляет автоматическое блокирование во всех случаях, когда это требуется. При этом система сама стремится предоставить всем пользователям наиболее свободный доступ к объектам. При необходимости пользователь и программист может воспользоваться командными или языковыми средствами явного определения блокировок. Например, в СУБД Paradox для явного блокирования отдельной записи во время редактирования таблицы используется команда Record | Lock.

Тупики. Если не управлять доступом к совместно используемым объектам, то между потребителями ресурсов могут возникать тупиковые ситуации (клинчи, «смертельные объятия» или блокировки). Следует отличать понятие блокировки в смысле контроля доступа к объектам (мы

придерживаемся такого термина) от блокировки в смысле тупикового события.

Существует два основных вида тупиков: *взаимные* (deadlock) и *односторонние* (livelock)!

Простейшим случаем ***взаимного тупика*** является ситуация, когда каждый из двух пользователей стремится захватить данные, уже захваченные другим пользователем (рис. 4.6а). В этой ситуации пользователь-1 ждет освобождения ресурса N, в то время как пользователь-2 ожидает освобождения от захвата ресурса M. Следовательно, никто из них не может продолжить работу.

В действительности могут возникать и более сложные ситуации, когда выполняются обращения трех и более пользователей к нескольким ресурсам. Пример одной из таких ситуаций приведен на рис. 4.6б

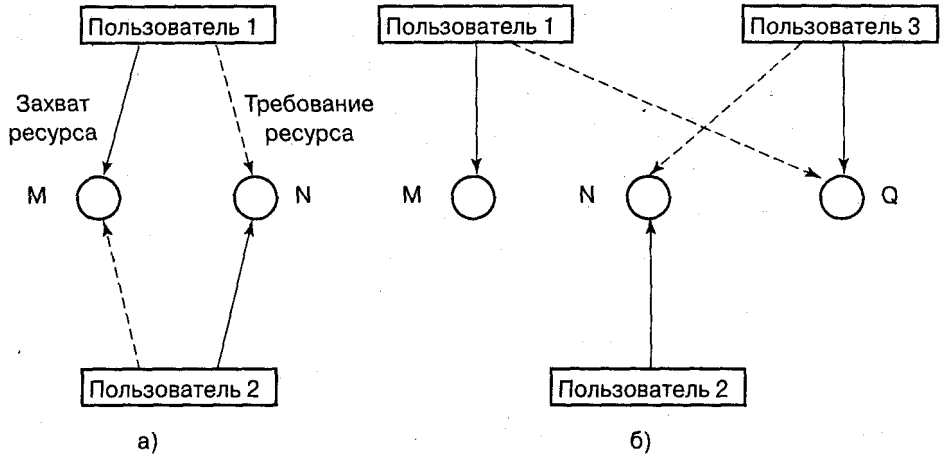

Рис. 4.6. Примеры взаимных тупиков в распределенных БД

Односторонний тупик возникает в случае требования получить монопольный доступ к некоторому ресурсу, как только он станет доступным и невозможности удовлетворить это требование.

Системы управления распределенными БД, очевидно, должны иметь соответствующие средства обнаружения или предотвращения конфликтов, а также разрешения возникающих конфликтов. Одной из наиболее сложных является задача устранения конфликтов в неоднородных системах в случае, если некоторая программа не обрабатывает или обрабатывает некорректно сигналы (уведомления) о наличии конфликтов. При этом важно не только сохранить целостность и достоверность данных в распределенных БД, но и восстановить вычислительный процесс, иногда парализующий пользователей и программы ожиданием чего-то [33].

Пользователи и разработчики приложений в распределенной среде должны предусматривать обработку сигналов о тупиках.

Вопросы и задания для самоконтроля:

1. Каким образом осуществляется выбор средств защиты информации от утечки информации по электромагнитному каналу?

2. По каким критериям производится выбор средств защиты информации от утечки информации по электромагнитному каналу

3. По каким характеристикам осуществить выбор генератора шума?

4. По каким критериям осуществляется выбор средств защиты информации от осуществления несанкционированного доступа к информации?

5. Дайте характеристику СЗИ «Страж NT».

6. Как можно решить задачу выбора средства защиты?

7. По каким оценочным критериям эффективности средств защиты информации от НСД решается задача выбора средств защиты информации в АС?

8. В чем заключается метод экспертной оценки?

9. Каким образом осуществляется выбор средств защиты информации от утечки информации по акустическому каналу?

10. Что включает в себя организационное мероприятие по защите объекта от утечки речевой информации по акустическому и виброакустическому каналам?

11. Что является технической мерой обеспечения акустической защиты объекта?

12. По каким характеристикам осуществляется выбор средств акустической защиты?

13. Дайте характеристику системе акустической и виброакустической защиты «Соната-АВ».

14. Каким образом осуществляется выбор средств защиты информации от утечки информации по виброакустическому каналу?

15. Дайте характеристику комплексу SEL SP-157 «Шагрень».

16. Дайте характеристику комплексу виброакустической защиты «Барон».

17. Что можно отнести к основным средствам защиты информации?

18. Что представляет собой парольная защита?

19. Что представляет собой шифрование данных?

20. Укажите права доступа к таблицам в общем случае.

21. Какие уровни прав доступа можно выделить применительно к защите данных в полях таблиц?

22. Какие операции предусматриваются к по отношению к формам БД?

23. Какие средства защиты можно отнести к дополнительным средствам защиты БД?

24. Для чего служат средства повышения достоверности вводимых значений в СУБД?

25. Что представляет собой разработка хранимых процедур?

26. Каковы вида отношений в реляционной СУБД?

27. Опишите проблему разрешения конфликтов в распределенных информационных системах, работающих с базами данных, между различными действиями над одними и теми же объектами.

28. Опишите содержание управления распределенными данными.

29. В чем заключается поддержка соответствия БД вносимым изменениям?

30. Какова структура распределенной БД?

31. В чем заключается сущность модели тиражирования данных?

ЗАКЛЮЧЕНИЕ

Основой для построения надежной системы информационной безопасности служит тщательный анализ угроз. Если пренебречь этим этапом, защита рискует превратиться в неэффективный набор разрозненных мер и технических решений.

Специфика этой сферы заключается в огромном и постоянно меняющемся перечне угроз: одни из них становятся актуальными, тогда как другие утрачивают свою значимость. Для систематизации этого многообразия требуется упорядочить существующие риски по определенным критериям.

Рассматриваемый объект информатизации - это служебное помещение, где работают с данными ограниченного доступа. В его оснащение входят основные технические средства и системы (ОТСС), представленные автоматизированной системой, а также вспомогательные технические средства и системы (ВТСС), такие как охранная и пожарная сигнализация и система кондиционирования.

В ходе оценки рисков были изучены опасности, связанные с возможной установкой закладочных устройств, формированием технических каналов утечки данных, а также несанкционированным доступом (НСД) к информации.

Несмотря на разную природу этих угроз, подход к созданию системы защиты должен быть единым и всесторонним. Для эффективного противодействия необходима комбинация технических и организационных мер, направленных на предотвращение получения злоумышленником сведений об объекте информатизации (ОИ) ОМВД России. Все применяемые меры должны быть скоординированы между собой по целям, месту и времени их применения.

В число дополнительных организационных мер для ОИ ОМВД России могут входить следующие мероприятия:

- регламентация доступа сотрудников к конфиденциальным сведениям;
- разработка инструкций по обращению с служебными документами и подготовка материалов для аттестации объекта;
- оборудование дверного проема тамбуром и установка на окно жалюзи;
- управление доступом пользователей к ОИ и его техническим средствам на основе разрешительной системы;
- регулирование процедур смены и ввода паролей, а также контроль действий пользователей при работе с ними;
- проведение специальных проверок на предмет выявления внедренных устройств для перехвата информации.

Внедрение указанных организационных мер в комплексе с техническими решениями создаст эффективную систему защиты данных на объектах информатизации ОМВД России.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Акапьев В.Л. Объекты защиты в области информационной безопасности по российскому законодательству / С.Е. Савотченко // Алтайский юридический вестник. 2023. № 3 (43). С. 27-35.
2. Акапьев В.Л. Оценка защищенности объекта информатизации ОМВД России / Е.Г. Ковалева, А.В. Борисенко // Вестник Воронежского института ФСИН России. 2025. № 2. С. 20-30.
3. Акапьев В.Л. Оценка защищенности объекта информатизации от утечки информации по виброакустическому каналу / Е.Г. Ковалева, А.В. Борисенко // Вестник Воронежского института ФСИН России. 2025. № 3. С. 42-50.
4. Акапьев В.Л. Проблемы информационного обеспечения деятельности правоохранительных органов // Сборник статей XII Всероссийской научно-практической конференции. - Белгород, 2025.
5. Акапьев В.Л. Проблемы реализации регуляторной политики государства в области информационной безопасности хозяйствующих субъектов / С.Е. Савотченко // Вестник владимирского юридического института. 2024. № 1 (70). С. 95-102.
6. Акапьев В.Л. Публично-правовое регулирование обеспечения безопасности объектов критической информационной инфраструктуры / С.Е. Савотченко // Вестник Удмуртского университета. Серия Экономика и право. 2024. Т. 34. № 3. С. 494-503.
7. Аудит информационной безопасности: учебное пособие / С.И. Козьминых, С.А. Борисов. – М.: КНОРУС, 2026. – 336 с.
8. Баланов А.Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. - М.: Инфра-Инженерия. 2024. - 156 с.
9. Баранова Е.К. Информационная безопасность: лабораторный практикум / Е.К. Баранова, А.В. Бабаш, Ю.Н. Мельников. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2024. – 336 с.
10. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 2-е изд., стер. – Москва: КНОРУС, 2025. – 132 с.
11. Баранова Е.К. Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. – Москва: РИОР: ИНФРА-М, 2024. – 236 с.
12. Белоус А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А.И. Белоус. – Москва; Вологда: Инфра-Инженерия, 2020. – 644 с.
13. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. - М.: МГТУ им. Н. Э. Баумана. 2024. - 252 с.
14. Борисенко А.В. Оценка защищенности объекта информатизации от утечки информации по акустическому каналу / Е.Г. Ковалева, В.Л. Акапьев // Вестник Воронежского института ФСИН России. 2025. № 2. С. 31-45.

15. Бурлаков М.Е. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум: учебное пособие / М.Е. Бурлаков, М.Н. Осипов. – Самара: Издательство Самарского университета, 2021 – 96 с. ил.

16. Васильев Р.А., Ротков Л.Ю. Обнаружение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «Легенда»: учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2018 – 45 с.

17. Васильева Т.Ю., Куприянов А.И., Мельников В.П. Информационная безопасность. Учебник. - М.: КноРус. 2023. - 372 с.

18. Вехен Джульен Безопасный DevOps. Эффективная эксплуатация систем. – СПб.: Питер, 2020. - 432 с.: ил.

19. Владстон Феррейра Фило, Мото Пиктет Теоретический минимум по Computer Science. Сети, криптография и data science/ - СПб.: Питер, 2022. – 288 с.: ил.

20. Внуков А.А. Основы информационной безопасности: защита информации. – М.: ЮРАЙТ, 2024. – 162.

21. Вострецова Е.В. Основы информационной безопасности: учебное пособие. – Екатеринбург, 2019. – 204.

22. Галатенко В.А. Информационная безопасность // Открытые системы. 2015. № 1. С. 38-43.

23. Грибунин В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский: учебное пособие рек. УМО вузов РФ. – Москва: Академия, 2013. – 416 с.

24. Гродзенский Я.С. Информационная безопасность: учебное пособие. - М.: РГ-Пресс. 2024. - 144 с.

25. Еремин А.Л. Информационная и цифровая гигиена. - М.: Лань. 2023. - 92 с.

26. Зайцев А.П. Технические средства и методы защиты информации: учебное пособие: рек. УМО вузов по образованию / А.П. Зайцев [и др.] – Москва: 2012. – 614 с.

27. Запечников С.В. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.] – Москва, 2011. – 536 с.

28. Защита информации в компьютерных системах: учеб. пособие / А.А. Симаков, А.В. Кургузов. - Омск: Омская академия МВД России, 2022. -108 с.

29. Зенков А.В. Основы информационной безопасности: учебное пособие / А.В. Зенков. – Москва; Вологда: Инфра-Инженерия, 2022. – 104 с.: ил., табл.

30. Зенков А.В. Информационная безопасность и защита информации. - М.: Юрайт. 2023. - 108 с.

31. Иванова С.В. Защита информации // СПС КонсультантПлюс. 2024.

32. Использование особенностей системного программного обеспечения для противодействия преступности в сфере информационно-телекоммуникационных технологий: учебное пособие / А.А. Дрога,

С.Е. Савотченко, В.Л. Акапьев. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2023. – 76 с.

33. Казарин О.В., Шубинский И.Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. - М.: Юрайт. 2023. - 343 с.

34. Ковалева Е.Г. Системный подход к обеспечению информационной и экономической безопасности хозяйствующего субъекта / С.Е. Савотченко, В.Л. Акапьев // В сборнике: Проблемы информационного обеспечения деятельности правоохранительных органов. сборник статей IX Всероссийской научно-практической конференции. 2022. С. 142-146.

35. Комплекс виброакустической защиты «БАРОН» - URL: https://bezar.ru/zaschita-informacii-poiskovaya-tehnika/generatory-radioshuma-i-pomeh?product_id=898 (дата обращения 16.11.2025).

36. Комплексы для проведения акустических и виброакустических измерений СПРУТ-7М. – М.: ЗАО НПЦ фирма «НЕЛК», 2025.

37. Комплектация устройства Соната-Р2. Основные и дополнительные элементы: сертификат. – URL: // https://sertifikatru1.ru/sonata-r2-sertfstek-generator-radioshuma-i-pemin-td-videoglaz-moskva/ (дата обращения 16.11.2025).

38. Корабельников С.М. Преступления в сфере информационной безопасности. – М.: Юрайт, 2024. – 112 с.

39. Куприянов А.И., Мельников В.П. Информационная безопасность. Учебник. - М.: КноРус, 2022. - 268 с.

40. Левушкин А.Н. Обеспечение баланса интересов граждан, предпринимателей и публично-правовых образований как участников имущественных правоотношений в цифровом пространстве и защите информации // Вестник Тверского государственного университета. Серия: Право. 2022. № 4 (72). С. 81 – 90.

41. Лукацкий А. Законодательные требования РФ по информационной безопасности // URL: https://www.youtube.com/watch?v=qfxj-vHr5lU&t=1368s (дата обращения: 04.03.2025).

42. Максуров А.А. Обеспечение информационной безопасности в сети Интернет. Монография. - М.: Инфра-М. 2023. - 226 с.

43. Малькольм М. Грокаем безопасность веб-приложений. – СПб.: Питер, 2025. – 336 с.: ил.

44. Нестеров С.А. Основы информационной безопасности. - М.: Лань. 2023. - 324 с.

45. Николаева М.О. Информационная безопасность: современная картина, проблемы информационной безопасности и защиты информации // Мониторинг. Образование. Безопасность. 2023. Т. 1. № 1. С. 51-57.

46. Новиков А.А. Уязвимость и информационная безопасность телекоммуникационных технологий / А.А. Новиков, Г.Н. Устинов: учебное пособие для вузов. – Москва: Радио и связь, 2012. – 296 с.

47. Организационная защита информации. Часть 1. Методологические основы организационной защиты информации: учебное пособие. - СПб.: Изд-во СПб ун-та МВД России, 2019. - 156 с.

48. Пестунова Т.М. Информационная безопасность и защита информации: краткое введение и практикум: учебное пособие / Т.М. Пестунова, А.А. Перов. – М.: РУСАЙНС, 2025. – 134 с.

49. Проблемы безопасности умного дома: учебное пособие / Е.А. Верещагина, А.Л. Золкин, А.С. Ярмонов. – М.: РУСАЙНС, 2025. – 104 с.

50. Прохорова О.В. Информационная безопасность и защита информации. – М.: Лань, 2025. – 124 с.

51. Рыженко С., Василенко В., Сидак А. Методы и средства защиты акустической речевой информации от утечки по техническим каналам: лабораторный практикум. – М.: Директ-Медиа, 2023. – 92 с.

52. Савотченко С.Е. Информатизация правоохранительной деятельности в условиях цифровой трансформации общества / В.Л. Акапьев // В сборнике: Развитие информационных технологий органов внутренних дел Российской Федерации. Сборник научных трудов Всероссийская научно-практическая конференция. Москва, 2025. С. 82-91.

53. Савотченко С.Е. Нормативно-правовое регулирование защиты конфиденциальной геологической информации // В.А. Захаров, В.Л. Акапьев // В сборнике: Проблемы информационного обеспечения деятельности правоохранительных органов. Сборник статей 11-й Всероссийской научно-практической конференции. Белгород, 2024. С. 235-239.

54. Савотченко С.Е. Проблемы правового регулирования защиты конфиденциальной геологической информации / В.А. Захаров, В.Л. Акапьев // В сборнике: «Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел». Сборник научных трудов по итогам Всероссийской научно-практической конференции. Ростов-на-Дону, 2025. С. 5-12.

55. Савотченко С.Е. Терминологическо-образовательные аспекты реализации мер информационной безопасности детей в современном обществе / В.Л. Акапьев // Право и образование. 2023. № 12. С. 67-79.

56. Система виброакустической защиты SEL SP-157 Шагрень. – URL: https://detsys.ru/catalog/vibroakusticheskaya_zashchita/sel_sp_157/ (дата обращения 17.11.2025).

57. Скабцов Н. Kali Linux в действии. Аудит безопасности информационных систем. 2-е изд. – СПб.: Питер, 2024. – 384 с.: ил.

58. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. – Москва: ИНФРА-М, 2023. – 201 с.

59. Физические основы защиты информации: учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. – М.: РИОР: ИНФРА-М, 2026. – 204 с.

60. Ховард Рик Кибербезопасность: главные принципы. – СПб.: Питер, 2024. – 320 с.: ил.

61. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов: в 3 т. – Т. 1. Технические каналы утечки информации / А.А. Хорев; под ред. Ю.Н. Лаврухина. – М.: НПЦ «Аналитика», 2008. – 436 с.

62. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие рекомендовано УМО по образованию. – Москва: Академия, 2013. – 256 с.

63. Чернова Е.В. Информационная безопасность человека: учебное пособие для вузов / Е.В. Чернова. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2024. – 327 с.

64. Швечкова О.Г., Бабаев С.И. Информационная безопасность. Часть 1. Теоретические основы. Учебник. – М.: КУРС, 2022. – 144 с.

65. Швечкова О.Г., Бабаев С.И. Информационная безопасность. Часть 2. Теоретические основы. Учебник. – М.: КУРС, 2022. – 144 с.

66. Шевцов В.Ю. Программно-аппаратная защита локальных АРМ с использованием ПО Secret Net: учебно-методическое пособие / В.Ю. Шевцов, Е.В. Булгакова. – Москва; Вологда: Инфра-Инженерия, 2024. – 80 с.

67. Шостак Адам Защита систем. Чему «Звездные войны» учат инженера ПО. – М.: Эксмо, 2025. – 444 с.

68. Ярочкин В.И. Информационная безопасность: учебник для вузов. – Москва: Академический Проект, 2014. – 544 с.

69. Why information protection is important. - URL: https://data.uq.edu.au/data-and-information-essentials/why-information-protection-important (дата обращения 18.11.2025).

ПРИЛОЖЕНИЕ 1

Тестовые задания

1. Утечка информации по техническому каналу– это:

а) неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

б) процесс раскрытия секретной информации;

в) процесс уничтожения информации;

г) непреднамеренная утрата носителя информации.

2. Технический канал утечки информации - это:

а) совокупность технических средств, при взаимодействии которых происходит передача информации

б) передача информации от источника к получателю

в) канал, образованный воздушной средой

г) совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

3. Технические каналы утечки информации делятся на:

а) акустические и виброакустические;

б) радиоэлектронные;

в) визуально-оптические;

г) материально-вещественные;

д) все перечисленное.

4. Какие технические каналы утечки отвечают за распространение звуковых колебаний в любом звукопроводящем материале или среде?

а) Акустические и виброакустические.

б) Электрические

в) Визуально-оптические.

г) Радиоканалы.

5. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?

а) Визуально-оптический.

б) Радиоэлектронный.

в) Акустический.

г) Материально-вещественный.

6. В каком техническом канале утечки информации в качестве носителей используются фотоны?

а) Визуально-оптический.

б) Радиоэлектронный.
в) Акустический.
г) Материально-вещественный.

7. В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?
а) Визуально-оптический.
б) Радиоэлектронный.
в) Акустический.
г) Материально-вещественный.

8. Какие ТКУИ бывают воздушными, вибрационными, параметрическими и оптико-электронными?
а) Визуально-оптический.
б) Радиоэлектронный.
в) Акустический.
г) Материально-вещественный.

9. Какой прибор используется для снятия информации по виброакустическому каналу?
а) Стетоскоп.
б) Эндоскоп.
в) Фильмоскоп.
г) Микрофон.

10. Как называется сигнал, который передает защищаемую информацию и может быть перехвачен злоумышленником с дальнейшим извлечением этой информации?
а) Демаскирующий.
б) Опасный.
в) Информационный.
г) Функциональный.

11. Как называются опасные сигналы, которые создаются техническим средством обработки информации для выполнения заданных функций?
а) Случайные.
б) Намеренные.
в) Функциональные.
г) Демаскирующие.

12. Что называется «контролируемой зоной»?
а) Это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

б) Это место или участок местности, где все под контролем технических средств охраны.

в) Участок местности, здание, помещение, где осуществляется контроль присутствия.

г) Зона, охраняемая спецслужбой.

13. Какие элементы конструкции из перечисленных в здании являются наиболее уязвимыми с точки зрения акустической разведки?

а) Плиты перекрытия.

б) Окна.

в) Кирпичные стены.

г) Полы.

14. Что такое электрический ТКУИ?

а) Съём информации с электрических проводов, находящихся под напряжением.

б) Съём информации посредством электрического тока.

в) Съем информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи.

г) Бесконтактный съем информации с кабельных линий связи.

15. Что такое индукционный ТКУИ?

а) Съём информации с электрических проводов, находящихся под напряжением.

б) Съём информации посредством электрического тока.

в) Съем информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи.

г) Бесконтактный съем информации с кабельных линий связи.

16. Основными техническими средствами и системами называются:

а) технические средства, которые в основном используются для обработки информации;

б) технические средства, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации;

в) технические средства, способные хранить передаваемую информацию;

г) технические средства, которые в обработке конфиденциальной информации занимают основное место.

17. Какой способ защиты не относится к защите от утечки акустической (речевой) информации?

а) Использование звукопоглощающих материалов для покрытия стен помещения.

б) Применение генераторов шума в акустическом диапазоне.

в) Применение устройств виброакустической защиты.

г) Уменьшить отражательные свойства объекта защиты.

18. Какой способ защиты не относится к защите от утечки визуально-оптической информации?

а) Уменьшить освещенность объекта защиты.

б) Уменьшить отражательные свойства объекта защиты.

в) Использовать средства, преграждающие или значительно ослабляющие отражение света (ширмы, экраны, шторы).

г) Шифрование информации для передачи ее по кабельным линиям за пределы контролируемой зоны.

19. Какой способ защиты не относится к защите от утечки информации по радиоэлектронным каналам?

а) Контроль подключения закладных устройств к кабельным линиям связи с помощью специальных приборов.

б) Шифрование информации для передачи ее по кабельным линиям за пределы контролируемой зоны.

в) Увеличение контролируемой зоны.

г) Технические средства ультразвуковой защиты помещений.

21. Что такое «побочные электромагнитные излучения»?

а) Излучения технических средств, возникающие под действием электромагнита.

б) излучения, возникающие в технических средствах специального назначения, используемых для подавления опасных сигналов.

в) электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях.

г) одностороннее излучение электромагнитной энергии техническими средствами, при их работе в штатном режиме.

22. Какое из перечисленных средств не является устройством перехвата радиосигналов при их утечке:

а) сканирующий приемник;

б) анализатор спектра;

г) рефлектометр;

д) радиочастотомер.

23. Как называется паразитная связь, возникающая в результате воздействия электрического поля?

а) Емкостная.

б) Магнитострикционная.

в) Гальваническая.

г) Индуктивная.

24. Как называется паразитная связь, возникающая в результате воздействия магнитного поля?

а) Емкостная.

б) Магнитострикционная.

в) Гальваническая.

г) Индуктивная.

25. Брандмауэром (межсетевым экраном) называется:

а) программа для рассылки поддельных писем электронной почты;

б) вид сетевых сервисов, связанных с «ботированием», т.е. с преобразованием данных операционной системы в код ботов;

в) программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил;

г) компьютерная программа для разблокировки сети.

26. Что не является одной из основных целей регулярного обновления программ на компьютере?

а) Устранение уязвимостей приложений для вредоносных программ.

б) Совершенствование программных продуктов и добавление в них новых функций.

в) Исправление ошибок программного обеспечения.

г) Показать, что организация-разработчик приложения продолжает его совершенствовать.

27. Под информационной безопасностью понимается:

а) состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;

в) процесс разработки структуры базы данных в соответствии с требованиями;

г) нет правильного ответа.

28. Можно выделить следующие направления мер информационной безопасности:

а) правовые;

б) организационные;

в) технические;

г) все ответы верны.

29. Социальная инженерия - это:

а) эксплуатации человеческих слабостей, с целью несанкционированного доступа к конфиденциальной информации;

б) защита людей от несанкционированного доступа к конфиденциальной информации;

в) помощь людям в защите от любых киберугроз;

г) нет правильного ответа.

30. Большая группа угроз, источником которых являются собственные сотрудники - это:

а) инсайдерские угрозы;

б) вредоносное ПО;

в) фишинг;

г) антивирусное ПО.

31. Компьютерный инцидент на объекте КИИ - это:

а) целенаправленное вредоносное воздействие на объекты КИИ для нарушения или прекращения их функционирования;

б) факт нарушения или прекращения функционирования объекта КИИ и/или нарушения безопасности обрабатываемой объектом информации;

в) попытка нанесения вреда компьютеру, или компьютерной сети;

г) нет правильных ответов.

32. Что такое система ГосСОПКА?

а) Система возвышенностей на участке местности.

б) Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

в) Государственная система защиты информации в органах власти.

г) Нет правильных ответов.

33. Какие органы исполнительной власти являются ключевыми в области технической защиты информации?

а) ФСТЭК России.

б) ФСБ России.

в) СВР России.

г) МВД России.

д) Роскомнадзор.

34. Как называется документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров?

а) Аттестат.

б) Удостоверение.

в) Сертификат.

г) Лицензия.

35. Сертификация средств защиты информации производится в соответствии с:

а) Положением о системе сертификации средств защиты информации.

б) ФЗ «О государственной тайне».

в) Указом Президента «О сертификация средств защиты информации».

г) ФЗ «О техническом регулировании».

36. Срок действия сертификата соответствия ограничивается сроком:

а) 1 год;

б) до 5 лет;

в) 3 года;

г) более 5 лет.

37. На соответствие каким документам осуществляется сертификация технических средств защиты информации?

а) Региональный стандарт.

б) Руководящие документы ФСТЭК и ФСБ.

в) Межгосударственный стандарт.

г) Национальный стандарт.

38. Различают следующие виды сертификации продукции:

а) законодательную и исполнительную;

б) обязательную и добровольную;

в) точную и приблизительную;

г) корректную и поверхностную.

39. Какой закон регулирует отношения в области безопасности персональных данных?

а) №149-ФЗ от 27.07.2006.

б) № 152-ФЗ от 27.07.2006.

в) № 5485-1-ФЗ от 21.07.1993.

г) № 98-ФЗ от 29.07.2004.

40. Какой закон является основным в области информационных технологий и защиты информации?

а) 149-ФЗ от 27.07.2006.

б) 152-ФЗ от 27.07.2006.

в) 5485-1-ФЗ от 21.07.1993.

г) 98-ФЗ от 29.07.2004.

41 Какой закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне в РФ?

а) 149-ФЗ от 27.07.2006.

б) 152-ФЗ от 27.07.2006.

в) 5485-1-ФЗ от 21.07.1993.

г) 98-ФЗ от 29.07.2004.

42. Что называют угрозой информационной безопасности?

а) Произошедший компьютерный инцидент.

б) Потенциально возможное происшествие, которое может оказать нежелательное воздействие на компьютерную систему.

в) Любой инцидент информационной безопасности.

г) Возможное происшествие, которое оказало нежелательное воздействие на компьютерную систему.

43. На сайте какого регулятора в свободном доступе размещен банк данных угроз информационной безопасности?

а) ФСТЭК.

б) ФСБ.

в) Роскомнадзор.

г) Роспотребнадзор.

44. Выберите наиболее подходящее определение информации:

а) сведения о лицах, предметах;

б) сведения о лицах, предметах, фактах, событиях;

в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

г) сведения о лицах независимо от формы их представления.

45. Информационная система - это ...

а) набор программных и технических средств;

б) упорядоченную совокупность документов, информационных технологий и программно-аппаратных средств, реализующих информационные процессы;

в) упорядоченная совокупность документов, относящихся к определенной области;

г) набор программных средств, относящихся к одной задаче.

46. К информации ограниченного доступа относятся:

а) государственная тайна;

б) конфиденциальная информация;

в) персональные данные;

г) все ответы верны

47. Информационная безопасность являются переводом на русский язык английского термина:

а) information security;

б) information system;

в) information currency;

г) information crypto.

48. Защитой информации называют:

а) деятельность по предотвращению утечки любой информации;

б) деятельность по предотвращению утечки защищаемой информации;

в) деятельность по предотвращению утечки доступной информации;

г) все ответы верны.

49. Под утечкой понимают:

а) неконтролируемое распространение защищаемой информации путём её разглашения или несанкционированного доступа к ней;

б) неконтролируемое распространение скрытой информации путём её разглашения или несанкционированного доступа к ней;

в) неконтролируемое распространение конфиденциальной информации путём её разглашения или несанкционированного доступа к ней;

г) все верно.

50. Под непреднамеренным воздействием на защищаемую информацию понимают:

а) воздействие на неё из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;

б) воздействие на неё из-за ошибок пользователя, сбоя технических средств;

в) воздействие на неё из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;

г) все ответы верны.

51. Что не относится к задачам информационной безопасности:

а) целостность и секретность;

б) электронная подпись и датирование;

в) устойчивость связи и определение трафика;

г) неотказуемость и анонимность.

52. К методам обеспечения информационной безопасности не относятся:

а) корпоративные;

б) административные;

в) правовые;

г) технические.

53. Какие методы не относятся к обеспечению информационной безопасности:

а) принуждение и побуждение;

б) управление доступом и регламентация;

в) маскировка и препятствие;

г) скрытый доступ и копирование сообщений.

54. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:

а) уполномочивание;

б) контроль доступа;

в) сертификация;

г) нет верного ответа.

55. Основными характеристиками защищаемой информации являются:

а) конфиденциальность, целостность и статичность;

б) конфиденциальность, целостность и доступность;

в) аутентификация, целостность и доступность;

г) аутентификация, статичность и время создания.

56. Известность содержания информации только имеющим соответствующие полномочия субъектам - это:

а) целостность;

б) статичность;

в) конфиденциальность;

г) аутентификация.

57. Неизменность информации в условиях её случайного и (или) преднамеренного искажения и разрушения - это:

а) целостность;

b) конфиденциальность;

c) доступность;

d) идентификация.

58. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:

а) уязвимость;

б) атака;

в) угроза;

г) нет верного ответа.

59. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации - это:

а) статичность;

б) атака;

в) угроза;

г) изъян.

60. Классификацию угроз ИБ можно выполнить по нескольким критериям:

а) по аспекту информационной безопасности;

b) по компонентам информационной системы;
c) по способу осуществления;
d) все ответы верны.

61. Конфиденциальная информация может быть разделена на:
а) предметную и служебную;
б) служебную и закрытую;
в) предметную и открытую;
г) открытую и закрытую.

62. Высококвалифицированный специалист, стремящейся обойти защиту компьютерной системы:
а) крякер;
b) хаб;
c) хакер;
d) юзер.

63. Наибольшую угрозу ИС составляет:
а) юзер;
б) агент;
в) хакер;
г) крякер.

64. Что не относится к косвенным каналам утечки информации:
а) дистанционное видеонаблюдение;
б) использование полущивающих устройств;
в) перехват побочных электромагнитных излучений и наводок;
г) хищение носителей информации.

65. К каналам, предполагающим изменение элементов информационной структуры относится:
а) намеренное копирование файлов и носителей информации;
b) маскировка под других пользователей, путём похищение идентифицирующей их информации;
c) хищение носителей информации;
d) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.

66. АИС - это:
а) автоматизированная информационная среда;
б) автоматизированная информационная схема;
в) автоматизированная информационная система;
г) автоматизированная информационная структура.

67. Принципы обеспечения информационной безопасности:

а) системность, комплексность, непрерывность;

б) статичность, комплексность, доступность;

в) комплексность, целостность, доступность;

г) целостность, системность, открытость.

68. Центральный элемент системы защиты, который идентифицирует субъекты, объекты и параметры запрашиваемого доступа субъектов к объектам:

а) монитор безопасности

б) сканер;

в) модем безопасности;

г) шина безопасности.

69. К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые:

а) руководством организации;

б) персоналом организации;

в) пользователями;

г) нет верного ответа.

70. Из скольких уровней состоит правовое обеспечение информационной безопасности:

а) двух уровней;

b) трех уровней;

c) четырех уровней;

d) пяти уровней.

Учебное издание

Акапьев Виктор Львович
Борисенко Александр Васильевич
Ковалева Екатерина Геннадьевна
Новикова Екатерина Анатольевна
Пироженко Юрий Анатольевич

Методы анализа угроз нарушения информационной безопасности ведомственного объекта информатизации

Учебное пособие

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел Групп»
https://publishing.intelgr.com
E-mail: publishing@intelgr.com
Тел.: +7 (812) 945-50-63
Интернет-магазин издательства
https://shop.intelgr.com/

Подписано в печать 01.01.2026.
Формат 60×84/16
Объем 6,5 п.л.
Тираж 500 экз.

ISBN 978-5-00271-053-9