Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

сборник учебно-методических материалов для направления подготовки
09.03.02 Информационные системы и технологии

Благовещенск, 2017

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
Университета

Составитель: Пашенцев А.И.

Технические средства защиты информации: сборник учебно-методических материалов для направления подготовки 09.03.02 Информационные системы и технологии – Благовещенск: Амурский гос. ун-т, 2017.

Содержание

Краткое изложение лекционного материала.

Тема 1. Современные угрозы и модели каналов утечки информации.

Цель лекции. Рассмотреть основные определения и понятия по дисциплине.

План

1. Источники, носители, методы и средства разведки, защищаемой информации.
2. Физические основы и особенности образования технических каналов утечки информации.

Краткое содержание

Значение информации в жизни любого цивилизованного общества непрерывно возрастает. С незапамятных времен сведения, имеющие важное военно-стратегическое значение для государства, тщательно скрывались и защищались. В настоящее время информация, относящаяся к технологии производства и сбыта продукции, стала рыночным товаром, имеющим большой спрос как на внутреннем так и на внешнем рынках. Информационные технологии постоянно совершенствуются в направлении их автоматизации и способов защиты информации. Развитие новых информационных технологий сопровождаются такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к секретной и конфиденциальной информации. Поэтому защита информации является важнейшей государственной задачей в любой стране. Острая необходимость в защите информации в России нашла выражение в создании Государственной системы защиты информации (ГСЗИ) и в развитии правовой базы информационной безопасности. Приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных», «Доктрина информационной безопасности Российской Федерации» и др.

Для определения способов пресечения утечки информации необходимо рассмотреть известные **технические средства негласного съема информации** и принципы их действия.

У злоумышленников есть достаточно большой выбор средств для несанкционированного получения конфиденциальной информации. Одни удобны благодаря простоте установки, но, соответственно, также легко могут быть обнаружены. Другие очень сложно разыскать, но их непросто и установить. Они различаются по технологии применения, по схемам и способам использования энергии, по видам каналов передачи информации. Важно подчеркнуть, что на каждый метод получения информации по техническим каналам ее утечки существует метод противодействия, часто не один, который может свести такую угрозу к минимуму.

В зависимости от схемы и способа использования энергии спецсредства негласного получения информации можно подразделить на пассивные (переизлучающие) и активные (излучающие). Обязательными элементами всех **активных спецсредств** является датчик или сенсор контролируемой информации, преобразующий информацию в электрический сигнал. Усилитель-преобразователь, который усиливает сигнал и преобразует его в ту или иную форму для последующей передачи информации. Форма сигнала может быть аналоговой или цифровой. Обязательным элементом активных спецсредств съема информации является оконечный излучающий модуль.

Пассивные устройства не излучают вовне дополнительную энергию. Для получения информации от подобных устройств с удаленного контрольного пункта в направлении

контролируемого объекта направляется мощный сигнал. Достигая объекта, сигнал отражается от него и окружающих предметов и частично возвращается на контрольный пункт. Отраженный сигнал несет в себе информацию о свойствах объекта контроля. К пассивным спецсредствам формально можно отнести практически все средства перехвата информации на естественных или искусственных каналах связи. Все они энергетически и физически скрытны.

Самым распространенным и относительно недорогим способом негласного съема информации до сих пор остается установка разнообразных закладок (жучков). **Закладное устройство** – скрытно устанавливаемое техническое средство негласного съема информации. Одни из них предназначены для получения акустической информации, другие – для получения видовых изображений, цифровых или аналоговых данных от использующихся вычислительных средств и средств оргтехники, средств связи, телекоммуникации и др.

Сегодня на рынке присутствует огромное количество подобных устройств. Они различаются исполнением и способом передачи информации – автономные или сетевые, они могут быть изготовлены в виде стандартных элементов существующих силовых и слаботочных линий (вилок, разъемов и т. п.), радиозакладки в виде авторучек, пепельниц, картона, «забытых» личных вещей, стандартных элементов телефонных аппаратов и т. п. К этой же категории средств относятся различные варианты миниатюрных диктофонов, микрокамер, телекамер и проч.

Более дорогие и предназначенные для продолжительного контроля технические средства заранее устанавливаются на объектах контроля (например, в период капитального или косметического ремонта). Это могут быть проводные средства с микрофонами, глубоко замаскированные закладки (например, в вычислительной технике), средства акустического или видеоконтроля, автономные радиомикрофоны или оптоэлектронные микрофоны с вынесенными излучающими элементами и др.

Наиболее сложные и соответственно самые дорогие – **специальные технические средства,** позволяющие перехватывать информацию на некотором удалении от ее источника. Это разнообразные регистраторы виброакустических колебаний стен и систем коммуникаций, возникающих при разговоре в помещении; регистраторы ослабленных акустических полей, проникающих через естественные звуководы (например, системы вентиляции); регистраторы побочных излучений от работающей оргтехники; направленные и высокочувствительные микрофоны для контроля речевой информации от удаленных источников; средства дистанционного визуального или видеоконтроля; лазерные средства контроля вибраций оконных стекол и др.

Регистрация разговоров (переговоров) является одним из самых распространенных способов и достаточно информативным каналом негласного получения информации. Прослушивание может осуществляться путем как непосредственного подслушивания (через дверь, вентиляционные каналы, стены, и т. п.), так и с использованием технических средств. Это могут быть разнообразные микрофоны, диктофоны (аналоговые с записью на магнитную ленту, цифровые с записью на флеш-память, в т. ч. оборудованные акустоматом), направленные микрофоны и т. п. Тактика применения этих устройств довольно проста, но эффективна.

Акустические микрофоны. Самыми распространенными устройствами являются различные микрофоны. Микрофоны могут быть встроены в стены, электро– и телефонные розетки, различную аппаратуру и др. Они могут быть закамуфлированы под что угодно, например, могут иметь вид обычного конденсатора, который стоит в схеме принтера и подключен к его системе питания. Чаще всего используются **проводные микрофоны** с передачей информации по специально проложенным проводам, по сети электроснабжения, по проводам сигнализации, радиотрансляции и т. п. Дальность передачи информации от таких устройств практически не ограничена. Они, как правило, появляются после различных ремонтов, после аренды помещений, визитов различных проверяющих и т. п. Обнаруживаются с трудом, но зато легко ликвидируются.

Радиомикрофоны – это микропередатчики УКВ-диапазона, которые могут быть и стационарными, и временными. Сами разговоры перехватываются на расстоянии до нескольких десятков метров. Дальность передачи информации составляет от десятков до сотен метров, причем для увеличения дальности применяют промежуточные ретрансляторы, а «жучки» устанавливают на металлические предметы – трубы водоснабжения, бытовые электроприборы (служащие дополнительной передающей антенной).

Любые радиомикрофоны и телефонные передатчики выдают себя излучением в радиодиапазоне (20–1500 МГц), поэтому так или иначе они могут быть обнаружены с помощью пассивных средств. Атмосферные и промышленные помехи, которые постоянно присутствуют в среде распространения носителя информации, оказывают наибольшее влияние на амплитуду сигнала, и в меньшей степени – на его частоту. В функциональных каналах, допускающих передачу более широкополосных сигналов, например, в УКВ-диапазоне, передачу информации осуществляют, как правило, частотно-модулированными сигналами как более помехоустойчивыми, а в узкополосных ДВ-, СВ– и КВ-диапазонах – амплитудно-модулированными сигналами. Для повышения скрытности работы мощность передатчиков проектируется небольшой. Высокая скрытность передачи сигнала от радиомикрофонов нередко достигается выбором рабочей частоты, близкой к несущей частоте мощной радиостанции, и маскируется ее сигналами.

Подведенные микрофоны могут иметь самую разнообразную конструкцию, соответствующую акустическим «щелям». «Игольчатый» микрофон, звук к которому подводится через тонкую трубку длиной около 30 см, может быть просунут в любую щель. Динамический тяжелый капсюль, например, можно опустить в вентиляционную трубу с крыши. А плоский кристаллический микрофон можно подвести под дверь снизу.

Оптический микрофон-передатчик передает сигнал от выносного микрофона невидимым глазу инфракрасным излучением. В качестве приемника используется специальная оптоэлектронная аппаратура с кремниевым фотоприемником.

По времени работы передатчиков спецсредства подразделяют на непрерывно излучающие, с включением на передачу при появлении в контролируемом помещении разговоров или шумов и дистанционно управляемые. Сегодня появились «жучки» с возможностью накопления информации и последующей ее передачи в эфир (сигналы со сверхкороткой передачей), с псевдослучайной скачкообразной перестройкой несущей частоты радиосигнала, с непосредственным расширением спектра исходного сигнала и модуляцией несущей частоты псевдослучайной М-последовательностью (шумоподобные сигналы).

Недостатком всех описанных выше средств акустической разведки является необходимость проникновения на интересующий объект в целях скрытной установки спецаппаратуры. Этих недостатков лишены **направленные микрофоны** для прослушивания разговоров. Они могут иметь различное конструктивное исполнение.

Используется **микрофон с параболическим отражателем** диаметром от 30 см до 2 м, в фокусе которого находится чувствительный обычный микрофон. **Микрофон-трубка**может камуфлироваться под трость или зонтик. Не так давно появились так называемые **плоские направленные микрофоны**, которые могут встраиваться в стенку дипломата или вообще носиться в виде жилета под рубашкой или пиджаком. Самыми современными и эффективными считаются **лазерные** и **инфракрасные микрофоны**, которые позволяют воспроизводить речь, любые другие звуки и акустические шумы при светолокационном зондировании оконных стекол и других отражающих поверхностей. При этом дистанция прослушивания в зависимости от реальной обстановки может достигать сотен метров. Это очень дорогие и сложные устройства.

Несанкционированный доступ к акустической информации может быть также осуществлен с помощью **стетоскопов** и **гидроакустических датчиков**. Звуковые волны, несущие речевую информацию, хорошо распространяются по воздуховодам, водопроводным трубам, железобетонным конструкциям и регистрируются специальными датчиками, установленными за пределами охраняемого объекта. Эти устройства засекают микроколе-

бания контактных перегородок с помощью прикрепленного к обратной стороне преграды миниатюрного вибродатчика с последующим преобразованием сигнала. С помощью стетоскопов возможно прослушивание переговоров через стены толщиной более метра (в зависимости от материала). Иногда используются гидроакустические датчики, позволяющие прослушивать разговоры в помещениях, используя трубы водоснабжения и отопления.

Утечка акустической информации возможна также из-за воздействия звуковых колебаний на элементы электрической схемы некоторых технических приборов за счет электроакустического преобразования и гетеродинного оборудования. К числу технических устройств, способных образовывать *электрические каналы утечки,* относятся телефоны (особенно кнопочные), датчики охранной и пожарной сигнализации, их линии, сеть электропроводки и т. д.

Например, в случае с телефонными аппаратами и электрическими часами утечка информации происходит за счет преобразования звуковых колебаний в электрический сигнал, который затем распространяется по проводным линиям. Доступ к конфиденциальной информации может осуществляться путем подключения к этим проводным линиям.

В телевизорах и радиоприемниках утечка информации происходит за счет имеющихся в этих приборах гетеродинов (генераторов частоты). Из-за модуляции звуковым колебанием несущей частоты гетеродина в систему «просачивается» звуковая информация и излучается в виде электромагнитного поля.

Чтобы обнаружить наличие таких каналов утечки в охраняемом помещении, включают мощный источник звуковых колебаний и проверяют наличие сигналов на выходящих линиях.

Для обнаружения закладок с передачей акустической информации по естественным проводным каналам (телефонная линия, электросеть, цепи охранно-пожарной сигнализации и пр.) используется метод обнаружения известного звукового сигнала. При такой технологии поиск закладных устройств осуществляется прослушиванием сигналов в проводной коммуникации с целью идентификации известного звука «на слух».

Чтобы свести возможные потери от утечки информации к минимуму, нет необходимости стараться обеспечить защиту всего здания. Главное – необходимо ограничить доступ в те места и к той технике, где сконцентрирована конфиденциальная информация (с учетом возможностей и методов ее дистанционного получения).

Особо важен выбор места для переговорной комнаты. Ее целесообразно размещать на верхних этажах. Желательно, чтобы комната для переговоров не имела окон или же они выходили бы во двор. Использование средств сигнализации, хорошая звукоизоляция, звуковая защита отверстий и труб, проходящих через эти помещения, демонтаж излишней проводки, применение других специальных устройств серьезно затруднят попытки внедрения спецтехники съема акустической информации. Также в комнате для переговоров не должно быть телевизоров, приемников, ксероксов, электрических часов, телефонных аппаратов и т. п.

Тема 2. Методы и средства защиты информации от утечки по техническимканалам.

Цель лекции. Рассмотреть основные определения и понятия по дисциплине.

План

1. Основные положения современной концепции защиты информации техническими средствами.
2. Методы и средства защиты информации обрабатываемой ТСПИ от утечки по техническим каналам.
3. Методы и средства защиты акустической информации от утечки по техническим каналам.

Краткое содержание

Для создания системы защиты объекта от утечки информации по техническим каналам необходимо осуществить ряд мероприятий. Прежде всего, надо проанализировать специфические особенности расположения зданий, помещений в зданиях, территорию вокруг них и подведенные коммуникации. Затем необходимо выделить те помещения, внутри которых циркулирует конфиденциальная информация и учесть используемые в них технические средства. Далее следует осуществить такие технические мероприятия:
- проверить используемую технику на соответствие величины побочных излучений допустимым уровням;
- экранировать помещения с техникой или эту технику в помещениях;
- перемонтировать отдельные цепи, линии, кабели;
- использовать специальные устройства и средства пассивной и активной защиты.

Важно подчеркнуть, что на каждый метод получения информации по техническим каналам ее утечки существует метод противодействия, часто не один, который может свести угрозу к минимуму. При этом успех зависит от двух факторов: - от вашей компетентности в вопросах защиты информации (либо от компетентности тех лиц, которым это дело поручено) и от наличия оборудования, необходимого для защитных мероприятий. Первый фактор важнее второго, так как самая совершенная аппаратура останется мертвым грузом в руках дилетанта.

В каких случаях целесообразно проводить меры защиты от технического проникновения? Прежде всего, такую работу необходимо осуществлять превентивно, не ожидая пока "грянет гром". Роль побудительного мотива могут сыграть сведения об утечке информации, обсуждавшейся в конкретном помещении узкой группой лиц, или обрабатывавшейся на конкретных технических средствах. Толчком к действию могут стать следы, свидетельствующие о проникновении в помещения вашей фирмы посторонних лиц, либо какие-то странные явления, связанные с используемой техникой (например, подозрительный шум в телефоне).

Осуществляя комплекс защитных мер, не стремитесь обеспечить защиту всего здания. Главное - ограничить доступ в те места и к той технике где сосредоточена конфиденциальная информация (не забывая, конечно, о возможностях и методах ее дистанционного получения). В частности, использование качественных замков, средств сигнализации, хорошая звукоизоляция стен, дверей, потолков и пола, звуковая защита вентиляционных каналов, отверстий и труб, проходящих через эти помещения, демонтаж излишней проводки, а также применение специальных устройств (генераторов шума, аппаратуры ЗАС и др.) серьезно затруднят или сделают бессмысленными попытки внедрения спецтехники.

Именно поэтому для разработки и реализации мероприятий по защите информации от утечки по техническим каналам надо приглашать квалифицированных специалистов, либо готовить собственные кадры по соответствующим программам в соответствующих учебных центрах. Для краткости условимся, что аббревиатура ТСПИ обозначает Технические Средства Передачи Информации.

Защита информации, обрабатываемой техническими средствами, осуществляется с применением пассивных и активных методов и средств.

Пассивные методы защиты информации направлены на:

• ослабление побочных электромагнитных излучений (информационных сигналов) ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

• ослабление наводок побочных электромагнитных излучений (информационных сигналов) ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, беспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

• исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Активные методы защиты информации направлены на:

• создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;

• создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ.

Ослабление побочных электромагнитных излучений ТСПИ и их наводок в посторонних проводниках осуществляется путем экранирования и заземления ТСПИ и их соединительных линий.

Исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания достигается путем фильтрации информационных сигналов.

Для создания маскирующих электромагнитных помех используются системы пространственного и линейного зашумления.

Экранирование технических средств

Функционирование любого технического средства информации связано с протеканием по его токоведущим элементам электрических токов различных частот и образованием разности потенциалов между различными точками его электрической схемы, которые порождают магнитные и электрические поля, называемые **побочными электромагнитными излучениями**.

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи, создают в ближней зоне электромагнитные поля с преобладанием электрической составляющей. Преимущественное влияние электрических полей на элементы электронной аппаратуры наблюдается и в тех случаях, когда эти элементы малочувствительны к магнитной составляющей электромагнитного поля.

Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения, создают в ближней зоне электромагнитные поля с преобладанием магнитной составляющей. Преимущественное влияние магнитных полей на аппаратуру наблюдается также в случае, если рассматриваемое устройство малочувствительно к электрической составляющей или последняя много меньше магнитной за счет свойств излучателя.

Переменные электрическое и магнитное поля создаются также в пространстве, окружающем соединительные линии (провода, кабели) ТСПИ.

Побочные электромагнитные излучения ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки информации, а также могут оказаться причиной возникновения наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня побочных электромагнитных излучений уделяется большое внимание.

Эффективным методом снижения уровня ПЭМИ является экранирование их источников.

Различают следующие способы экранирования:

• электростатическое;

• магнитостатическое;

• электромагнитное.

Электростатическое и магнитостатическое экранирование основаны на замыкании экраном (обладающим в первом случае высокой электропроводностью, а во втором - магнитопроводностью) соответственно электрического и магнитного полей.

Электростатическое экранирование по существу сводится к замыканию электроста-

тического поля на поверхность металлического экрана и отводу электрических зарядов на землю (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования. Применение металлических экранов позволяет полностью устранить влияние электростатического поля. При использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника наводки в ε раз, где ε - относительная диэлектрическая проницаемость материала экрана.

Основной задачей экранирования электрических полей является снижение емкости связи между экранируемыми элементами конструкции. Следовательно, эффективность экранирования определяется в основном отношением емкостей связи между источником и рецептором наводки до и после установки заземленного экрана. Поэтому любые действия, приводящие к снижению емкости связи, увеличивают эффективность экранирования.

Экранирующее действие металлического листа существенно зависит от качества соединения экрана с корпусом прибора и частей экрана друг с другом. Особенно важно не иметь соединительных проводов между частями экрана и корпусом.

В диапазонах метровых и более коротких длин волн соединительные проводники длиной в несколько сантиметров могут резко ухудшить эффективность экранирования. На еще более коротких волнах дециметрового и сантиметрового диапазонов соединительные проводники и шины между экранами недопустимы. Для получения высокой эффективности экранирования электрического поля здесь необходимо применять непосредственное сплошное соединение отдельных частей экрана друг с другом.

Узкие щели и отверстия в металлическом экране, размеры которых малы по сравнению с длиной волны, практически не ухудшают экранирование электрического поля.

С увеличением частоты эффективность экранирования снижается.

Основные требования, которые предъявляются к электрическим экранам, можно сформулировать следующим образом :

• конструкция экрана должна выбираться такой, чтобы силовые линии электрического поля замыкались на стенки экрана, не выходя за его пределы;

• в области низких частот (при глубине проникновения (δ) больше толщины (d), т.е. при δ>d) эффективность электростатического экранирования практически определяется качеством электрического контакта металлического экрана с корпусом устройства и мало зависит от материала экрана и его толщины;

• в области высоких частот (при d<δ) эффективность экрана, работающего в электромагнитном режиме, определяется его толщиной, проводимостью и магнитной проницаемостью.

Магнитостатическое экранирование используется при необходимости подавить наводки на низких частотах от 0 до 3 ... 10 кГц .

Основные требования, предъявляемые к магнитостатическим экранам, можно свести к следующим:

• магнитная проницаемость μ_a материала экрана должна быть возможно более высокой. Для изготовления экранов желательно применять магнитомягкие материалы с высокой магнитной проницаемостью (например, пермаллой);

• увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако при этом следует принимать во внимание возможные конструктивные ограничения по массе и габаритам экрана;

• стыки, разрезы и швы в экране должны размещаться параллельно линиям магнитной индукции магнитного поля. Их число должно быть минимальным;

• заземление экрана не влияет на эффективность магнитостатического экранирования.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов.

Экранирование высокочастотного магнитного поля основано на использовании магнитной индукции, создающей в экране переменные индукционные вихревые токи (токи

Фуко). Магнитное поле этих токов внутри экрана будет направлено навстречу возбуждающему полю, а за его пределами - в ту же сторону, что и возбуждающее поле. Результирующее поле оказывается ослабленным внутри экрана и усиленным вне его. Вихревые токи в экране распределяются неравномерно по его сечению (толщине). Это вызывается явлением поверхностного эффекта, сущность которого заключается в том, что переменное магнитное поле ослабевает по мере проникновения в глубь металла, так как внутренние слои экранируются вихревыми токами, циркулирующими в поверхностных слоях.

Благодаря поверхностному эффекту плотность вихревых токов и напряженность переменного магнитного поля по мере углубления в металл падает по экспоненциальному закону.

Эффективность магнитного экранирования зависит от частоты и электрических свойств материала экрана. Чем ниже частота, тем слабее действует экран, тем большей толщины приходится его делать для достижения одного и того же экранирующего эффекта. Для высоких частот, начиная с диапазона средних волн, экран из любого металла толщиной 0,5 ... 1,5 мм действует весьма эффективно. При выборе толщины и материала экрана следует учитывать механическую прочность, жесткость, стойкость против коррозии, удобство стыковки отдельных деталей и осуществления между ними переходных контактов с малым сопротивлением, удобство пайки, сварки и пр..

Для частот выше 10 МГц медная и тем более серебряная пленка толщиной более 0,1 мм дает значительный экранирующий эффект. Поэтому на частотах выше 10 МГц вполне допустимо применение экранов из фольгированного гетинакса или другого изоляционного материала с нанесенным на него медным или серебряным покрытием.

При экранировании магнитного поля заземление экрана не изменяет величины возбуждаемых в экране токов и, следовательно, на эффективность магнитного экранирования не влияет.

На высоких частотах применяется исключительно **электромагнитное экранирование**. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления.

Теория и практика показывают, что с точки зрения стоимости материала и простоты изготовления преимущества на стороне экранированного помещения из листовой стали. Однако при применении сетчатого экрана могут значительно упроститься вопросы вентиляции и освещения помещения. В связи с этим сетчатые экраны также находят широкое применение.

Для изготовления экрана целесообразно использовать следующие материалы:

сталь листовая декапированная ГОСТ 1386-47 толщиной (мм)
0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм)
0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм)
0,51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;
сетка стальная тканая ГОСТ 3826-47 номер 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;
сетка стальная плетеная ГОСТ 5336-50 номер 3; 4; 5; 6;
сетка из латунной проволоки марки Л-80 ГОСТ 6613-53 0,25; 0,5; 1,0; 1,6; 2,0; 2,5; 2,6.

Металлические листы или полотнища сетки должны быть между собой электрически соединены по всему периметру. Для сплошных экранов это может быть осуществлено электросваркой или пайкой. Шов электросварки или пайки должен быть непрерывным с тем, чтобы получить цельносварную конструкцию экрана.

Для сетчатых экранов пригодна любая конструкция шва, обеспечивающая хороший электрический контакт между соседними полотнищами сетки не реже чем через 10 ... 15 мм. Для этой цели может применяться пайка или точечная сварка.

Экран, изготовленный из луженой низкоуглеродистой стальной сетки с ячейкой 2,5 ... 3

мм, дает ослабление порядка 55 ... 60 дБ, а из такой же двойной (с расстоянием между наружной и внутренней сетками 100 мм) - около 90 дБ. Экран, изготовленный из одинарной медной сетки с ячейкой 2,5 мм, имеет ослабление порядка 65 ... 70 дБ.

Необходимая эффективность экрана в зависимости от его назначения и величины уровня излучения ПЭМИН обычно находится в пределах 60 ... 120 дБ.

Наряду блоками аппаратуры экранированию подлежат и монтажные провода и соединительные линии.

Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Подключение оболочки должно осуществляться путем непосредственного контакта (лучше всего путем пайки или сварки) с корпусом.

Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим попроводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплетку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путем для протекания обратного тока.

Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой.

На низких частотах приходится использовать более сложные схемы экранирования - коаксиальные кабели с двойной оплеткой (триаксиальные кабели).

На более высоких частотах, когда толщина экрана значительно превышает глубину проникновения поля, необходимость в двойном экранировании отпадает. В этом случае внешняя поверхность играет роль электрического экрана, а по внутренней поверхности протекают обратные токи.

Применение экранирующей оболочки существенно увеличивает емкость между проводом и корпусом, что в большинстве случаев нежелательно. Экранированные провода более громоздки и неудобны при монтаже, требуют предохранения от случайных соединений с посторонними элементами и конструкциями.

Длина экранированного монтажного провода должна быть меньше четверти длины самой короткой волны передаваемого по проводу спектра сигнала. При использовании более длинных участков экранированных проводов необходимо иметь в виду, что в этом случае экранированный провод следует рассматривать как длинную линию, которая во избежании искажений формы передаваемого сигнала должна быть нагружена на сопротивление, равное волновому.

Для уменьшения взаимного влияния монтажных цепей следует выбирать длину монтажных высокочастотных проводов наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а неэкранированные провода высокочастотных цепей - при пересечении под прямым углом. При параллельном расположении такие провода должны быть максимально удалены друг от друга или разделены экранами, в качестве которых могут быть использованы несущие конструкции электронной аппаратуры (кожух, панель и т.д.).

Экранированные провода и кабели следует применять в основном для соединения отдельных блоков и узлов друг с другом.

Кабельные экраны выполняются в форме цилиндра из сплошных оболочек, в виде спирально намотанной на кабель плоской ленты или в виде оплетки из тонкой проволоки. Экраны при этом могут быть однослойными и многослойными комбинированными, изготовленными из свинца, меди, стали, алюминия и их сочетаний (алюминий-свинец, алюминий-сталь, медь-сталь-медь и т.д.).

В кабелях с наружными пластмассовыми оболочками применяют экраны ленточного типа в основном из алюминиевых, медных и стальных лент, накладываемых спирально

или продольно вдоль кабеля.

В области низких частот корпуса применяемых многоштырьковых низкочастотных разъемов являются экранами и должны иметь надежный электрический контакт с общей шиной или землей прибора, а зазоры между разъемом и корпусом должны быть закрыты электромагнитными уплотняющими прокладками.

В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению с используемыми высокочастотными разъемами. При заделке коаксиального кабеля в высокочастотные разъемы жила кабеля не должна иметь натяжения в месте соединения с контактом разъема, а сам кабель должен быть жестко прикреплен к шасси аппаратуры вблизи разъема.

Для эффективного экранирования низкочастотных полей применяются экраны, изготовленные из ферромагнитных материалов с большой относительной магнитной проницаемостью. При наличии такого экрана линии магнитной индукции проходят в основном по его стенкам, которые обладают малым сопротивлением по сравнению с воздушным пространством внутри экрана [128].

Качество экранирования таких полей зависит от магнитной проницаемости экрана и сопротивления магнитопровода, которое будет тем меньше, чем толще экран и меньше в нем стыков и швов, идущих поперек направления линий магнитной индукции.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их информационных кабелей в экранирующий распределительный короб. Когда такого короба не имеется, то приходится экранировать отдельные линии связи.

Для защиты линий связи от наводок необходимо разместить линию в экранирующую оплетку или фольгу, заземленную в одном месте, чтобы избежать протекания по экрану токов, вызванных неэквипотенциальностью точек заземления.

Для защиты линии связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводами линии. Если линия представляет собой одиночный провод, а возвратный ток течет по некоторой заземляющей поверхности, то необходимо максимально приблизить провод к поверхности. Если линия образована двумя проводами, то их необходимо скрутить, образовав бифиляр (витую пару). Линии, выполненные из экранированного провода или коаксиального кабеля, в которых по оплетке протекает возвратный ток, также отвечают требованию минимизации площади контура линии.

Наилучшую защиту как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, из которых один используется в качестве электрического экрана), триаксильного кабеля (изолированного коаксильального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского многопроводного кабеля, покрытого с одной или обеих сторон медной фольгой).

Приведем несколько схем, используемых на частотах порядка 100 кГц. Цепь, показанная на рис. 2.1, а, имеет большую площадь петли, образованной «прямым» проводом и «землей». Эта цепь подвержена прежде всего магнитному влиянию. Экран заземлен на одном конце и не защищает от магнитного влияния. Переходное затухание для этой схемы примем равным 0 дБ для сравнения с затуханием схем на рис. 2.1, б - и.

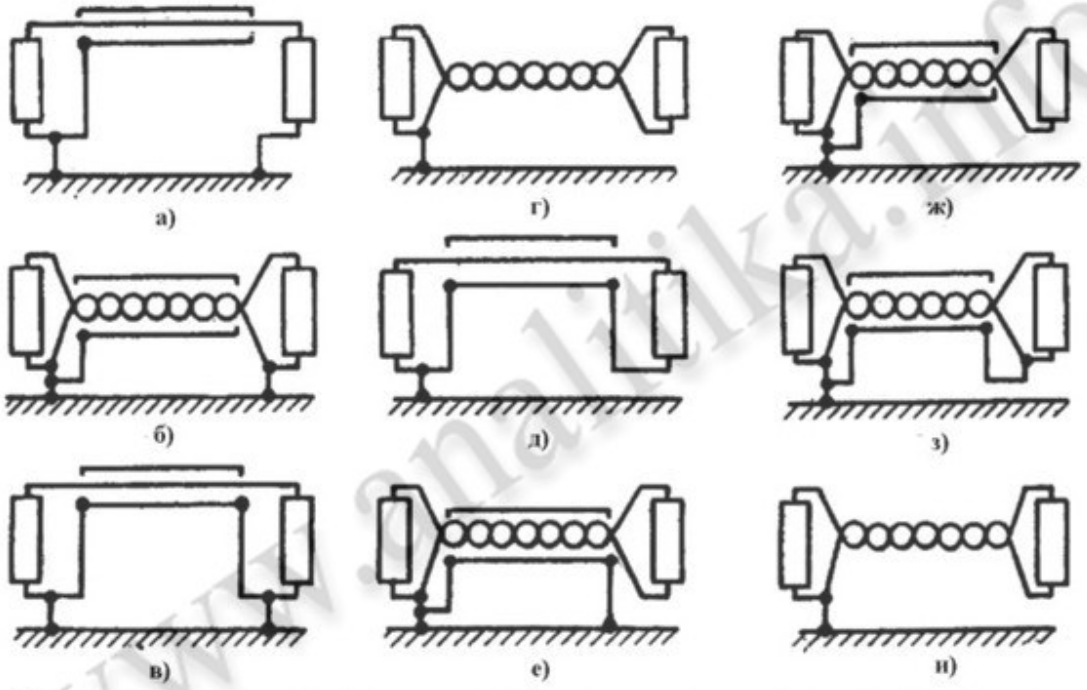

Рис. 2.1. Сравнение защищенности различных цепей от влияния внешних магнитных и электрических полей: а) 0 дБ; б) – 2 дБ; в) – 5 дБ; г) – 49 дБ, скрученная пара, 18 витков на метр; д) –57 дБ; е) – 64 дБ, схема предпочтительна на высоких частотах; ж) –64 дБ; з) – 71 дБ; и) –79 дБ, скрученная пара (54 витка на метр)

Схема на рис. 2.1, б практически не уменьшает магнитную связь, так как обратный провод заземлен с обоих концов, и этом смысле она аналогична схеме на рис. 2.1, а. Степень улучшения соизмерима с погрешностью расчета (измерения).

Схема на рис. 2.1, в отличается от схемы на рис. 2.1, а наличием обратного провода - коаксиального экрана, однако экранирование магнитного поля ухудшено, так как цепь заземлена на обоих концах, в результате чего с «землей» образуется петля большой площади.

Схема на рис. 2.1, г позволяет существенно повысить защищенность цепи (- 49 дБ) благодаря скрутке проводов. В этом случае (по сравнению со схемой на рис. 2.1, б) петли нет, поскольку правый конец цепи не заземлен.

Дальнейшее повышение защищенности цепи достигается применением схемы на рис. 2.1, с, коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара на рис. 2.1, г.

Площадь петли в схеме на рис. 3.1, д не больше, чем в схеме на рис. 2.1, г, так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом.

Схема на рис. 2.1, е позволяет повысить защищенность цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Кроме того, в этой схеме используется независимый экран.

Схема на рис. 2.1, ж имеет ту же защищенность, что и схема на рис. 2.1, е: эффект тот же, что и при заземлении на обоих концах, поскольку длина цепи и экрана существенно меньше рабочей длины волны.

Причины улучшения защищенности схемы на рис. 2.1, з по сравнению с рис. 2.1, ж объяснить трудно. Возможной причиной может быть уменьшение площади эквивалентной петли.

Более плотная скрутка проводов (схема рис. 2.1, и) позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь (в обоих проводах токи наводятся одинаково).

Для уменьшения магнитной и электрической связи между проводами необходи-

мо уменьшить площадь петли, максимально разнести цепи и максимально уменьшить длину параллельного пробега линий ТСПИ и посторонними проводниками.

При нулевых уровнях сигналов (0 dB) в соединительных линиях ТСПИ между ними и посторонними проводниками должно обеспечиваться переходное затухание не менее 114 dB (13 Нп). Данное переходное затухание обеспечивается, как правило, при прокладке кабелей ТСПИ на расстоянии не менее 0,1 м от посторонних проводников. При этом допускается прокладка кабелей ТСПИ вплотную с посторонними проводниками при суммарной длине их совместного пробега не более 70 м.

Экранироваться могут не только отдельные блоки (узлы) аппаратуры и их соединительные линии, но и помещения в целом.

В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующие свойства дверей и окон хуже. Для повышения экранирующих свойств стен применяются дополнительные средства, в том числе:

• токопроводящие лакокрасочные покрытия или токопроводящие обои;

• шторы из металлизированной ткани;

• металлизированные стекла (например, из двуокиси олова), устанавливаемые в металлические или металлизированные рамы.

В помещении экранируются стены, двери и окна.

При закрытии двери должен обеспечиваться надежный электрический контакт со стенками помещения (с дверной рамой) по всему периметру не реже чем через 10 ... 15 мм. Для этого может быть применена применена пружинная гребенка из фосфористой бронзы, которую укрепляют по всему внутреннему периметру дверной рамы.

Окна должны быть затянуты одним или двумя слоями медной сетки с ячейкой не более 2х2 мм, причем расстояние между слоями сетки должно быть не менее 50 мм. Оба слоя сетки должны иметь хороший электрический контакт со стенками помещения (с рамой) по всему периметру. Сетки удобнее делать съемными и металлическое обрамление съемной части также должно иметь пружинящие контакты в виде гребенки из фосфористой бронзы.

При проведении работ по тщательному экранированию подобных помещений необходимо одновременно обеспечить нормальные условия для работающего в нем человека, прежде всего вентиляцию воздуха и освещение.

Конструкция экрана для вентиляционных отверстий зависит от диапазона частот. Для частот менее 1000 МГц применяются сотовые конструкции, закрывающие вентиляционное отверстие, с прямоугольными, круглыми, шестигранными ячейками. Для достижения эффективного экранирования размеры ячеек должны быть менее одной десятой от длины волны. При повышении частоты необходимые размеры ячеек могут быть столь малыми, что ухудшается вентиляция.

Экранировку электромагнитных волн более 100 дБ можно обеспечить только в специальных экранированных камерах (см. табл. 2.2.), в которых электромагнитный экран выполнен в виде электрогерметичного стального корпуса, а для ввода электрических коммуникаций используются специальные фильтры.

Размеры экранированного помещения выбирают исходя из его назначения и стоимости. Обычно экранированные помещения строят площадью 6 ... 8 м^2 при высоте 2,5 ... 3 м.

Защита телефонных каналов может быть осуществлена с помощью криптографических систем защиты (скремблеров), анализаторов телефонных линий, односторонних маскираторов речи, средств пассивной защиты, постановщиков активной заградительной помехи. Защита информации может осуществляться на семантическом (смысловом) уровне с применением криптографических методов и энергетическом уровне.

Существующая аппаратура, противодействующая возможности прослушивания телефонных переговоров, по степени надежности подразделяется на три класса:

I класс – простейшие преобразователи, искажающие сигнал, сравнительно дешевые, но не очень надежные – это различные шумогенераторы, кнопочные сигнализаторы и т. п;

II класс – скемблеры, при работе которых обязательно используется сменный ключ-пароль, сравнительно надежный способ защиты, но специалисты-профессионалы с помощью хорошего компьютера могут восстановить смысл записанного разговор;

III класс – аппаратура кодирования речи, преобразующая речь в цифровые коды, представляющая собой мощные вычислители, более сложные, чем персональные ЭВМ. Не зная ключа, восстановить разговор практически невозможно.

Установка на телефоне *средства кодирования речевого сигнала* (скремблера) обеспечивает защиту сигнала на всем протяжении телефонной линии. Речевое сообщение абонента обрабатывается по какому-либо алгоритму (кодируется), обработанный сигнал направляется в канал связи (телефонную линию), затем полученный другим абонентом сигнал преобразуется по обратному алгоритму (декодируется) в речевой сигнал.

Этот метод, однако, является очень сложным и дорогим, требует установки совместимого оборудования у всех абонентов, участвующих в закрытых сеансах связи, и вызывает временные задержки на синхронизацию аппаратуры и обмен ключами с начала передачи и до момента приема речевого сообщения. Скремблеры могут обеспечивать также закрытие передачи факсовых сообщений. Портативные скремблеры имеют слабый порог защиты – с помощью компьютера его код можно разгадать за несколько минут.

Анализаторы телефонных линий сигнализируют о возможном подключении на основе измерения электрических параметров телефонной линии или обнаружения в ней посторонних сигналов.

Анализ параметров линий связи и проводных коммуникаций заключается в измерении электрических параметров этих коммуникаций и позволяет обнаруживать закладные устройства, считывающие информацию с линий связи или передающих информацию по проводным линиям. Они устанавливаются на предварительно проверенной телефонной линии и настраивются с учетом ее параметров. При наличии любых несанкционированных подключений устройств, питающихся от телефонной линии, выдается сигнал тревоги. Некоторые типы анализаторов способны имитировать работу телефонного аппарата и тем самым выявлять подслушивающие устройства, приводимые в действие сигналом вызова. Однако такие устройства характеризуются высокой частотой ложного срабатывания (т. к. существующие телефонные линии весьма далеки от совершенства) и не могут обнаруживать некоторые виды подключений.

Для защиты от «микрофонного эффекта» следует просто включить последовательно со звонком два запараллеленных во встречном направлении кремниевых диода. Для защиты от «высокочастотной накачки» необходимо включить параллельно микрофону соответствующий (емкостью 0,01–0,05 мкФ) конденсатор, закорачивающий высокочастотные колебания.

Метод *«синфазной» маскирующей низкочастотной помехи* применяется для подавления устройств съема речевой информации, подключенных к телефонной линии последовательно в разрыв одного из проводов или через индукционный датчик к одному из проводов. При разговоре в каждый провод телефонной линии подаются согласованные по амплитуде и фазе маскирующие помеховые сигналы речевого диапазона частот (дискретные псевдослучайные сигналы импульсов М-последовательности в диапазоне частот от 100 до 10000 Гц). Так как телефон подключен параллельно телефонной линии, согласованные по амплитуде и фазе помеховые сигналы компенсируют друг друга и не приводят к искажению полезного сигнала. В закладных устройствах, подключенных к одному телефонному проводу, помеховый сигнал не компенсируется и «накладывается» на полезный сигнал. А так как его уровень значительно превосходит полезный сигнал, то перехват передаваемой информации становится невозможным.

Метод *высокочастотной маскирующей помехи.* В телефонную линию подается помеховый сигнал высокой частоты (обычно от 6–8 кГц до 12–16 кГц). В качестве маскирующего шума используются широкополосные аналоговые сигналы типа «белого» шума или дискретные сигналы типа псевдослучайной последовательности импульсов с шириной спектра не менее 3–4 кГц. В устройстве защиты, подключенному параллельно в разрыв телефонной линии, устанавливается специальный фильтр нижних частот с граничной частотой выше 3–4 кГц, который подавляет (шунтирует) помеховые сигналы высокой частоты и не оказывает существенного влияния на прохождение низкочастотных речевых сигналов.

Метод *повышения* или *понижения напряжения.* Метод изменения напряжения применяется для нарушения функционирования всех типов электронных устройств перехвата информации с контактным (как последовательным, так и параллельным) подключением к линии, с использованием ее в качестве источника питания. Изменение напряжения в линии вызывает у телефонных закладок с последовательным подключением и параметрической стабилизацией частоты передатчика «уход» несущей частоты и ухудшение разборчивости речи. Передатчики телефонных закладок с параллельным подключением к линии при таких скачках напряжениях в ряде случаев просто отключаются. Эти методы обеспечивают подавление устройств съема информации, подключаемых к линии только на участке от защищаемого телефонного аппарата до АТС.

Компенсационный метод. На принимающую сторону подается «цифровой» маскирующий шумовой сигнал речевого диапазона частот. Этот же сигнал («чистый» шум) подается на один из входов двухканального адаптивного фильтра, на другой вход которого поступает смесь получаемого речевого сигнала и маскирующего шума. Фильтр компенсирует шумовую составляющую и выделяет скрываемый речевой сигнал. Этот способ очень эффективно подавляет все известные средства негласного съема информации, подключаемых к линии на всем участке телефонной линии от одного абонента до другого.

Так называемое *«выжигание»* осуществляется подачей высоковольтных (более 1500 В) импульсов мощностью 15–50 Вт с их излучением в телефонную линию. У гальванически подсоединенных к линии электронных устройств съема информации «выгорают» входные каскады и блоки питания. Результатом работы является выход из строя полупроводниковых элементов (транзисторов, диодов, микросхем) средств съема информации. Подача высоковольтных импульсов осуществляется при отключении телефонного аппарата от линии. При этом для уничтожения параллельно подключенных устройств подача высоковольтных импульсов осуществляется при разомкнутой, а последовательно подключенных устройств – при «закороченной» (как правило, в телефонной коробке или щите) телефонной линии.

Тема 3. Организация работ по защите информации от утечки по техническим каналам.

Цель лекции. Рассмотреть способы организации работ по защите информации от утечки по техническим каналам..

План

4. Основные положения современной концепции защиты информации техническими средствами.
5. Методы и средства защиты информации обрабатываемой ТСПИ от утечки по техническим каналам.
6. Методы и средства защиты акустической информации от утечки по техническим каналам.

Краткое содержание

К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [3]. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Защита информации ограниченного доступа (далее - защищаемой информации) от утечки по техническим каналам осуществляется на основе Конституции Российской Федерации, требований законов Российской Федерации “Об информации, информатизации и защите информации”, “О государственной тайне”, “О коммерческой тайне”, других законодательных актов Российской Федерации, “Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам”, утвержденного Постановлением Правительства РФ от 15.09.93 № 912-51, “Положения о лицензировании деятельности предприятий, организаций и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны”, утвержденного Постановлением Правительства РФ от 15 апреля 1995 г. № 333, “Положения о государственном лицензировании деятельности в области защиты информации”, утвержденного Постановлением Правительства РФ от 27 апреля 1994 г. № 10, “Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации” утвержденного Постановлением Правительства РФ от 27 мая 2002 г. № 348, с изменениями и дополнениями от 3 октября 2002 г. № 731, “Положения о сертификации средств защиты информации”, утвержденного Постановлением Правительства РФ от 26 июня 1995 г. № 608, Постановлений Правительства Российской Федерации “О лицензировании деятельности по технической защите конфиденциальной информации” (от 30 апреля 2002 г. № 290, с изменениями и дополнениями от 23 сентября 2002 г. № 689 и от 6 февраля 2003 г. № 64), “О лицензировании отдельных видов деятельности” (от 11 февраля 2002 г. № 135), а также “Положения по аттестации объектов информатизации по требованиям безопасности информации”, утвержденного Председателем Гостехкомиссии России 25 ноября 1994 г., и других нормативных документов.

Требования и рекомендации нормативных документов распространяются на защиту государственных информационных ресурсов. При проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну и т.д., требования нормативных документов носят рекомендательный характер.

Режим защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (далее - конфиденциальной информации), устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством Российской Федерации.

В дальнейшем рассмотрим методические рекомендации по организации защиты конфиденциальной информации, собственником которой являются негосударственные предприятия (организации, фирмы).

Мероприятия по защите конфиденциальной информации от утечки по техническим каналам (далее - технической защите информации) являются составной частью деятельности предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению их информационной безопасности.

Защита конфиденциальной информации от утечки по техническим каналам должна осуществляться посредством выполнения комплекса организационных и технических мероприятий, составляющих систему технической защиты информации на защищаемом объекте (СТЗИ), и должна быть дифференцированной в зависимости от установленной

категории объекта информатизации или выделенного (защищаемого) помещения (далее – объекта защиты).

Организационные мероприятия по защите информации от утечки по техническим каналам в основном основываются на учете ряда рекомендаций при выборе помещений для установки технических средств обработки конфиденциальной информации (ТСОИ) и ведения конфиденциальных переговоров, введении ограничений на используемые ТСОИ, вспомогательные технические средства и системы (ВТСС) и их размещение, а также введении определенного режима доступа сотрудников предприятия (организации, фирмы) на объекты информатизации и в выделенные помещения.

Технические мероприятия по защите информации от утечки по техническим каналам основываются на применении технических средств защиты и реализации специальных проектных и конструкторских решений.

Техническая защита информации осуществляется подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководителями организаций для проведения таких работ. Для разработки мер по защите информации могут привлекаться сторонние организации, имеющие лицензии ФСТЭК или ФСБ России на право проведения соответствующих работ.

Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства защиты. Порядок сертификации определяется законодательством Российской Федерации.

Перечень необходимых мер защиты информации определяется по результатам специального обследования объекта защиты, сертификационных испытаний и специальных исследований технических средств, предназначенных для обработки конфиденциальной информации.

Уровень технической защиты информации должен соответствовать соотношению затрат на организацию защиты информации и величины ущерба, который может быть нанесен собственнику информационных ресурсов.

Защищаемые объекты должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России на соответствие установленным нормам и требованиям по защите информации. По результатам аттестации дается разрешение (аттестат соответствия) на обработку конфиденциальной информации на данном объекте.

Ответственность за обеспечение требований по технической защите информации возлагается на руководителей организаций, эксплуатирующих защищаемые объекты.

В целях своевременного выявления и предотвращения утечки информации по техническим каналам должен осуществляться контроль состояния и эффективности защиты информации. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Защита информации считается эффективной, если принятые меры соответствуют установленным требованиям и нормам. Организация работ по защите информации возлагается на руководителей подразделений, эксплуатирующих защищаемые объекты, а контроль за обеспечением защиты информации - на руководителей подразделений по защите информации (служб безопасности).

Установка технических средств обработки конфиденциальной информации, а также средств защиты информации должна выполняться в соответствии с техническим проектом или техническим решением. Разработка технических решений и технических проектов на установку и монтаж ТСОИ, а также средств защиты информации производится подразделениями по защите информации (службами безопасности предприятий) или проектными организациями, имеющими лицензию ФСТЭК, на основании технических заданий на проектирование, выдаваемых заказчиками.

Технические решения по защите информации от утечки по техническим каналам являются составной частью технологических, планировочных, архитектурных и конструк-

тивных решений и составляют основу системы технической защиты конфиденциальной информации.

Непосредственную организацию работ по созданию СТЗИ осуществляет должностное лицо, обеспечивающее научно-техническое руководство проектированием объекта защиты.

Разработка и внедрение СТЗИ может осуществляться как силами предприятий (организаций, фирм), так и другими специализированными организациями, имеющими лицензии ФСТЭК и (или) ФСБ России на соответствующий вид деятельности.

В случае разработки СТЗИ или ее отдельных компонентов специализированными организациями в организации - заказчике определяются подразделения или отдельные специалисты, ответственные за организацию и проведение мероприятий по защите информации, которые должны осуществлять методическое руководство и участвовать в специальном обследовании защищаемых объектов, аналитическом обосновании необходимости создания СТЗИ, согласовании выбора ТСОИ, технических и программных средств защиты, разработке технического задания на создание СТЗИ, организации работ по внедрению СТЗИ и аттестации объектов защиты.

Порядок организации на предприятии работ по созданию и эксплуатации объектов информатизации и выделенных (защищаемых) помещений определяется в специальном “Положении о порядке организации и проведения на предприятии работ по защите информации от ее утечки по техническим каналам” с учетом конкретных условий, которое должно определять:

- порядок определения защищаемой информации;
- порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СТЗИ, их задачи и функции на различных стадиях создания и эксплуатации защищаемого объекта;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию защищаемых объектов;
- ответственность должностных лиц за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СТЗИ.

На предприятии (учреждении, фирме) должен быть документально оформлен перечень сведений, подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

При организации работ по защите утечки по техническим каналам информации на защищаемом объекте можно выделить три этапа [6, 9]:

- первый этап (подготовительный, предпроектный);
- второй этап (проектирование СТЗИ);
- третий этап (этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации).

Подготовительный этап создания системы технической защиты информации

На первом этапе осуществляется подготовка к созданию системы технической защиты информации на защищаемых объектах, в процессе которой проводится специальное обследование защищаемых объектов, разрабатывается аналитическое обоснование необходимости создания СТЗИ и техническое (частное техническое) задание на ее создание.

При проведении специального обследования защищаемых объектов с привлечением соответствующих специалистов проводится оценка потенциальных технических каналов утечки информации.

Для анализа возможных технических каналов утечки на объекте изучаются [1, 6 - 9]:

- план (в масштабе) прилегающей к зданию местности в радиусе до 150 - 300 м с указанием (по возможности) принадлежности зданий и границы контролируемой зоны;
- поэтажные планы здания с указанием всех помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
- план-схема инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схема системы заземления объекта с указанием места расположения заземлителя;
- план-схема системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схема прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схема систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок.

Устанавливается: когда был построен объект (здание), какие организации привлекались для строительства, какие организации в нем ранее располагались.

При анализе условий расположения объекта определяются граница контролируемой зоны, места стоянки автомашин, а также здания, находящиеся в прямой видимости из окон защищаемых помещений за пределами контролируемой зоны. Определяются (по возможности) принадлежность этих зданий и режим доступа в них.

Путем визуального наблюдения или фотографирования из окон защищаемых помещений устанавливаются окна близлежащих зданий, а также места стоянки автомашин, находящиеся в прямой видимости. Проводится оценка возможности ведения из них разведки с использованием направленных микрофонов и лазерных акустических систем разведки, а также средств визуального наблюдения и съемки.

Устанавливается месторасположение трансформаторной подстанции, электрощитовой, распределительных щитов. Определяются здания и помещения, находящиеся за пределами контролируемой зоны, которые запитываются от той же низковольтной шины трансформаторной подстанции, что и защищаемые объекты. Измеряется длина линий электропитания от защищаемых объектов до возможных мест подключения средств перехвата информации (распределительных щитов, помещений и т.п.), находящихся за пределами контролируемой зоны. Проводится оценка возможности приема информации, передаваемой сетевыми закладками (при их установке в защищаемых помещениях), за пределами контролируемой зоны.

Определяются помещения, смежные с защищаемыми и находящиеся за пределами контролируемой зоны. Устанавливаются их принадлежность и режим доступа в них. Определяется возможность доступа с внешней стороны к окнам защищаемых помещений. Проводится оценка возможности утечки речевой информации из защищаемых помещений по акустовибрационным каналам.

Определяются соединительные линии вспомогательных технических средств и систем (линии телефонной связи, оповещения, систем охранной и пожарной сигнализации, часофикации и т.п.), выходящие за пределы контролируемой зоны, места расположения их распределительных коробок. Измеряется длина линий от защищаемых объектов до мест возможного подключения средств перехвата информации за пределами контролируемой зоны. Проводится оценка возможности утечки речевой информации из защищаемых помещений по акустоэлектрическим каналам.

Определяются инженерные коммуникации и посторонние проводники, выходящие за пределы контролируемой зоны, измеряется их длина от защищаемых объектов до мест возможного подключения средств перехвата информации.

Устанавливается месторасположение заземлителя, к которому подключен контур заземления защищаемого объекта. Определяются помещения, расположенные за пределами контролируемой зоны, которые подключены к тому же заземлителю.

Определяются места установки на объектах информатизации ТСОИ и прокладки их соединительных линий.

Проводится оценка возможности перехвата информации, обрабатываемой ТСОИ, специальными техническими средствами по электромагнитным и электрическим каналам утечки информации.

В современных условиях целесообразно провести технический контроль по оценке реальных экранирующих свойств конструкций здания звуко- и виброизоляции помещений в целях учета их результатов при выработке мер защиты ТСОИ и выделенных помещений.

Предпроектное обследование может быть поручено специализированной организации, имеющей соответствующую лицензию, но и в этом случае анализ информационного обеспечения в части защищаемой информации целесообразно выполнять представителям организации - заказчика при методической помощи специализированной организации.

Ознакомление специалистов этой организации с защищаемыми сведениями осуществляется в установленном в организации - заказчике порядке.

После проведения предпроектного специального обследования защищаемого объекта группой (комиссией), назначенной руководителем предприятия (организации, фирмы), проводится аналитическое обоснование необходимости создания СТЗИ, в процессе которого:

- определяется перечень сведений, подлежащих защите (перечень сведений конфиденциального характера утверждается руководителем организации);
- проводится категорирование сведений конфиденциального характера, подлежащих защите;
- определяется перечень лиц, допущенных до сведений конфиденциального характера, подлежащих защите;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении и т.п.) информации, характер их взаимодействия между собой и со службой безопасности;
- разрабатывается матрица допуска персонала к сведениям конфиденциального характера, подлежащих защите;
- определяется (уточняется) модель вероятного противника (злоумышленника, нарушителя);
- проводятся классификация и категорирование объектов информатизации и выделенных помещений;
- проводится обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования и внедрения СТЗИ;
- проводится оценка материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;
- определяются ориентировочные сроки разработки и внедрения СТЗИ.

Основным признаком конфиденциальной информации является ее ценность для потенциального противника (конкурентов). Поэтому, определяя перечень сведений конфиденциального характера, их обладатель должен определить эту ценность через меру ущерба, который может быть нанесен предприятию при их утечке (разглашении). В зависимости от величины ущерба (или негативных последствий), который может быть нанесен при утечке (разглашении) информации, вводятся следующие категории важности информации:

- **1 категория** – информация, утечка которой может привести к потере экономической или финансовой самостоятельности предприятия или потери ее репутации (потери доверия потребителей, смежников, поставщиков и т.п.);

- **2 категория** – информация, утечка которой может привести к существенному экономическому ущербу или снижению ее репутации;
- **3 категория** – информация, утечка разглашение которой может нанести экономический ущерб предприятию.

С точки зрения распространения информации ее можно разделить на две группы:

- **первая группа (1)** – конфиденциальная информация, которая циркулирует только на предприятии и не предназначенная для передачи другой стороне;
- **вторая группа (2)** – конфиденциальная информация, которая предполагается к передаче другой стороне или получаемая от другой стороны.

Следовательно, целесообразно установить шесть уровней конфиденциальности информации (табл. 1).

Таблица 1. Уровни конфиденциальности информации

Величина ущерба (негативных последствий), который может быть нанесен при разглашении конкретной информации	**Уровень конфиденциальности информации**	
	информация, не подлежащая передаче другим предприятиям (организациям)	**информация, предназначенная для передачи другим предприятиям (организациям) или полученная от них**
Утечка информации может привести к потере экономической или финансовой самостоятельности предприятия или потери ее репутации	1.1	1.2
Утечка информации может привести к существенному экономическому ущербу или снижению репутации предприятия	2.1	2.2
Утечка информации может нанести экономический ущерб предприятию	3.1	3.2

Введение категорий конфиденциальности информации необходимо для определения объема и содержания комплекса мер по ее защите.

При установлении режима доступа к конфиденциальной информации необходимо руководствоваться принципом - чем больше ущерб от разглашения информации, тем меньше круг лиц, которые к ней допущены.

Режимы доступа к конфиденциальной информации должны быть увязаны с должностными обязанностями сотрудников.

В целях ограничения круга лиц, допущенных к сведениям, составляющим коммерческую тайну, целесообразно введение следующих режимов доступа к ней:

- **режим 1** – обеспечивает доступ ко всему перечню сведений конфиденциального характера. Устанавливается руководящему составу предприятия;
- **режим 2** – обеспечивает доступ к сведениям при выполнении конкретных видов деятельности (финансовая, производственная, кадры, безопасность и т.п.). Устанавливается для руководящего состава отделов и служб;
- **режим 3** – обеспечивает доступ к определенному перечню сведений при выполнении конкретных видов деятельности. Устанавливается для сотрудников - специалистов конкретного отдела (службы) в соответствии с должностными обязанностями.

Таким образом, после составления перечня сведений конфиденциального характера необходимо установить уровень их конфиденциальности, а также режим доступа к ним сотрудников.

Разграничение доступа сотрудников предприятия (фирмы) к сведениям конфиденциального характера целесообразно осуществлять или по уровням (кольцам) конфиденциальности в соответствии с режимами доступа, или по так называемым матрицам полномочий, в которых в строках перечислены должности сотрудников предприятия (фирмы), а столбцах - сведения, включенные в перечень сведений, составляющих коммерческую тайну. Элементы матрицы содержат информацию об уровне полномочий соответствующих должностных лиц (например, “+” – доступ к сведениям разрешен, “-” – доступ к сведениям запрещен).

Далее определяется (уточняется) модель вероятного противника (злоумышленника, нарушителя), которая включает определение уровня оснащения противника, заинтересованного в получении информации, и его возможностей по использованию тех или иных технических средств разведки для перехвата информации.

В зависимости от финансового обеспечения, а также возможностей доступа к тем или иным средствам разведки, противник имеет различные возможности по перехвату информации. Например, средства разведки побочных электромагнитных излучений и наводок, электронные устройства перехвата информации, внедряемые в технические средства, лазерные акустические системы разведки могут использовать, как правило, разведывательные и специальные службы государств.

Для обеспечения дифференцированного подхода к организации защиты информации от утечки по техническим каналам защищаемые объекты должны быть отнесены к соответствующим категориям и классам.

Классификация объектов проводится по задачам технической защиты информации и устанавливает требования к объему и характеру комплекса мероприятий, направленных на защиту конфиденциальной информации от утечки по техническим каналам в процессе эксплуатации защищаемого объекта.

Защищаемые объекты целесообразно разделить на два класса защиты (табл. 2).

К классу защиты А относятся объекты, на которых осуществляется полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте).

К классу защиты Б относятся объекты, на которых осуществляется скрытие параметров информационных сигналов, возникающих при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте).

Таблица 2. Классы защиты объектов информатизации и выделенных помещений

Задача технической защиты информации	**Установленный класс защиты**
Полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте)	А
Скрытие параметров информационных сигналов, которые возникают при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	Б

При установлении категории защищаемого объекта учитываются класс его защиты, а также финансовые возможности предприятия по закрытию потенциальных технических каналов утечки информации. Защищаемые объекты целесообразно разделить на три категории.

Категорирование защищаемых объектов информатизации и выделенных помещений проводится комиссиями, назначенными руководителями предприятий, в ведении ко-

торых они находятся. В состав комиссий, как правило, включаются представители подразделений, ответственных за обеспечение безопасности информации, и представители подразделений, эксплуатирующих защищаемые объекты.

Категорирование защищаемых объектов проводится в следующем порядке:

- определяются объекты информатизации и выделенные помещения, подлежащие защите;
- определяется уровень конфиденциальности информации, обрабатываемой ТСОИ или обсуждаемой в выделенном помещении, и производится оценка стоимости ущерба, который может быть нанесен предприятию (организации, фирме) вследствие ее утечки;
- для каждого объекта защиты устанавливается класс защиты (А или Б) и определяются потенциальные технические каналы утечки информации и специальные технические средства, которые могут использоваться для перехвата информации (табл. 3, 4);
- определяется рациональный состав средств защиты, а также разрабатываются организационные мероприятия по закрытию конкретного технического канала утечки информации для каждого объекта защиты;
- для информации, отнесенной к конфиденциальной и предоставленной другой стороной, определяется достаточность мер, принятых по ее защите (меры или нормы по защите информации определяются соответствующим договором);
- проводится оценка стоимости мероприятий (организационных и технических) по закрытию конкретного технического канала утечки информации для каждого объекта защиты;
- с учетом оценки возможностей вероятного противника (конкурента, злоумышленника) по использованию для перехвата информации тех или иных технических средств разведки, а также с учетом стоимости закрытия каждого канала утечки информации и стоимости ущерба, который может быть нанесен предприятию вследствие ее утечки, определяется целесообразность закрытия тех или иных технических каналов утечки информации;
- после принятия решения о том, какие технические каналы утечки информации необходимо закрывать, устанавливается категория объекта информатизации или выделенного помещения (табл. 5).

Результаты работы комиссии оформляются актом, который утверждается должностным лицом, назначившим комиссию.

Таблица 3. Потенциальные технические каналы утечки информации, обрабатываемой ПЭВМ

Технические каналы утечки информации	**Специальные технические средства, используемые для перехвата информации**
Электромагнитный (перехват побочных электромагнитных излучений ТСОИ)	Средства разведки побочных электромагнитных излучений и наводок (ПЭМИН), установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны
Электрический (перехват наведенных электрических сигналов)	Средства разведки ПЭМИН, подключаемые к линиям электропитания ТСОИ, соединительным линиям ВТСС, посторонним проводникам, цепям заземления ТСОИ за пределами контролируемой зоны
Высокочастотное облучение ТСОИ	Аппаратура “высокочастотного облучения”, установленная в ближайших строениях или смежных помещениях, находящихся за пределами контролируемой зоны

Внедрение в ТСОИ электронных устройств перехвата информации	Аппаратные закладки модульного типа, устанавливаемые в системный блок или периферийные устройства в процессе сборки, эксплуатации и ремонта ПЭВМ: • аппаратные закладки для перехвата изображений, выводимых на экран монитора, устанавливаемые в мониторы ПЭВМ; • аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ, устанавливаемые в клавиатуру; • аппаратные закладки для перехвата информации, выводимой на печать, устанавливаемые в принтер; • аппаратные закладки для перехвата информации, записываемой на жесткий диск ПЭВМ, устанавливаемые в системный блок. Аппаратные закладки, скрытно внедряемые в блоки, узлы, платы и отдельные элементы схем ПЭВМ на стадии их изготовления

Таблица 4. Потенциальные технические каналы утечки речевой информации

Технические каналы утечки информации	**Специальные технические средства, используемые для перехвата информации**
Прямой акустический (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.)	• направленные микрофоны, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны; • специальные высокочувствительные микрофоны, установленные в воздуховодах или в смежных помещениях, принадлежащих другим организациям; • электронные устройства перехвата речевой информации с датчиками микрофонного типа, установленные в воздуховодах, при условии неконтролируемого доступа к ним посторонних лиц; • 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)
Акустовибрационный (через ограждающие конструкции, трубы инженерных коммуникаций и т.д.)	• электронные стетоскопы, установленные в смежных помещениях, принадлежащих другим организациям; • 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
Акустооптический	лазерные акустические локационные системы,

(через оконные стекла)	установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны
Акустоэлектрический (через соединительные линии ВТСС)	• специальные низкочастотные усилители, подключаемые к соединительным линиям ВТСС, обладающим “микрофонным” эффектом, за пределами контролируемой зоны; • аппаратура “высокочастотного навязывания”, подключаемая к соединительным линиям ВТСС, обладающим “микрофонным” эффектом, за пределами контролируемой зоны
Акустоэлектромагнитный (параметрический)	• 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; • аппаратура “высокочастотного облучения”, установленная в ближайших строениях или смежных помещениях, находящихся за пределами контролируемой зоны

Таблица 5. Категории объектов информатизации и выделенных помещений

Задача технической защиты информации	**Закрываемые технические каналы утечки информации**	**Установленная категория объекта защиты**
Полное скрытие информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте)	все потенциальные технические каналы утечки информации	1
Скрытие параметров информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	все потенциальные технические каналы утечки информации	2
Скрытие параметров информационных сигналов**,** возникающих при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	наиболее опасные технические каналы утечки информации	3

После установления категории объекта защиты оцениваются возможности по созданию и внедрению СТЗИ силами предприятия (организации, фирмы) или проводится обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования и внедрения СТЗИ. Проводится оценка материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ, определяются ориентировочные сроки разработки и внедрения СТЗИ.

Результаты аналитического обоснования необходимости создания СТЗИ оформляются пояснительной запиской, которая должна содержать [6, 8, 9]:

- перечень сведений конфиденциального характера с указанием их уровня конфиденциальности;
- перечень сотрудников предприятия, допущенных до конфиденциальной информации, с указанием их режима доступа, а при необходимости и матрицы доступа;
- информационную характеристику и организационную структуру объектов защиты;
- перечень объектов информатизации, подлежащих защите, с указанием их категорий;
- перечень выделенных помещений, подлежащих защите, с указанием их категорий;
- перечень и характеристику технических средств обработки конфиденциальной информации с указанием их места установки;
- перечень и характеристику вспомогательных технических средств и систем с указанием их места установки;
- предполагаемый уровень оснащения вероятного противника (конкурента, злоумышленника);
- технические каналы утечки информации, подлежащие закрытию (устранению);
- организационные мероприятия по закрытию технических каналов утечки информации;
- перечень и характеристику предлагаемых к использованию технических средств защиты информации с указанием их места установки;
- методы и порядок контроля эффективности защиты информации;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;
- ориентировочные сроки разработки и внедрения СТЗИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования СТЗИ.

Пояснительная записка подписывается руководителем группы (комиссии), проводившей аналитическое обоснование, согласовывается с руководителем службы безопасности и утверждается руководителем предприятия.

На основе аналитического обоснования и действующих нормативно-методических документов по защите информации от утечки по техническим каналам, с учетом установленного класса и категории защищаемого объекта задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СТЗИ.

Техническое задание (ТЗ) на разработку СТЗИ должно содержать:

- обоснование разработки;
- исходные данные объекта защиты в техническом, программном, информационном и организационном аспектах;
- ссылку на нормативно-методические документы, с учетом которых будет разрабатываться и приниматься в эксплуатацию СТЗИ;
- конкретные требования к СТЗИ;
- перечень предполагаемых к использованию технических средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;

- перечень подрядных организаций - исполнителей различных видов работ;
- перечень предъявляемой заказчику научно-технической продукции и документации.

Техническое задание на проектирование СТЗИ защищаемого объекта оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности организации-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Стадия проектирования системы технической защиты информации

Для разработки технического проекта на создание системы технической защиты информации должны привлекаться организации, имеющие лицензию ФСТЭК РФ.

Технический проект СТЗИ должен содержать:

- титульный лист;
- пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
- перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
- перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
- схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границ контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
- технологические поэтажные планы здания (в масштабе) с указанием мест расположения объектов информатизации и выделенных помещений, характеристик их стен, перекрытий, материалов отделки, типов дверей и окон;
- планы объектов информатизации (в масштабе) с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
- план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схему системы заземления объекта, с указанием места расположения заземлителя;
- план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
- схемы систем активной защиты (если они предусмотрены техническими заданием на проектирование);
- инструкции и руководства по эксплуатации технических средств защиты для пользователей и ответственных за обеспечение безопасности информации на объекте информатизации.

Технический проект, рабочие чертежи, смета и другая проектная документация должны быть учтены в установленном порядке.

Технический проект согласовывается со службой (специалистом) безопасности заказчика, органа по защите информации проектной организации, представителями подрядных организаций - исполнителей видов работ и утверждается руководителем проектной организации.

При разработке технического проекта необходимо учитывать следующие рекомендации :

– в выделенных помещениях необходимо устанавливать сертифицированные технические средства обработки информации и вспомогательные технические средства;

– для размещения ТСОИ целесообразно выбирать подвальные и полуподвальные помещения (они обладают экранирующими свойствами);

– кабинеты руководителей организации, а также особо важные выделенные помещения рекомендуется располагать на верхних этажах (за исключением последнего) со стороны, менее опасной с точки зрения ведения разведки;

– необходимо предусмотреть подвод всех коммуникаций (водоснабжение, отопление, канализация, телефония, электросеть и т.д.) к зданию в одном месте. Вводы коммуникаций в здание целесообразно сразу ввести в щитовое помещение и обеспечить закрытие его входа и установку сигнализации или охраны;

– в случае если разделительный трансформатор (трансформаторная подстанция), от которой осуществляется электропитание защищаемых технических средств и выделенных помещений, расположен за пределами контролируемой зоны, необходимо предусмотреть отключение от низковольтных шин подстанции, от которых осуществляется питание защищаемых объектов, потребителей, находящихся за контролируемой зоной;

– электросиловые кабели рекомендуется прокладывать от общего силового щита по принципу вертикальной разводки на этажи с горизонтальной поэтажной разводкой и с установкой на каждом этаже своего силового щитка. Аналогичным образом должны прокладываться соединительные кабели вспомогательных технических средств, в том числе кабели систем связи;

– число вводов коммуникаций в зону защищаемых помещений должно быть минимальным и соответствовать числу коммуникаций. Незадействованные посторонние проводники, проходящие через защищаемые помещения, а также кабели (линии) незадействованных вспомогательных технических средств должны быть демонтированы;

– прокладка информационных цепей, а также цепей питания и заземления защищаемых технических средств должна планироваться таким образом, чтобы был исключен или уменьшен до допустимых пределов их параллельный пробег с различными посторонними проводниками, имеющими выход за пределы контролируемой зоны;

– для заземления технических средств (в том числе вспомогательных), установленных в выделенных помещениях, необходимо предусмотреть отдельный собственный контур заземления, расположенный в пределах контролируемой зоны. Если это невозможно, необходимо предусмотреть линейное зашумление системы заземления объекта;

– необходимо исключить выходы посторонних проводников (различных трубопроводов, воздухопроводов, металлоконструкций здания и т.п.), в которых присутствуют наведенные информативные сигналы, за пределы контролируемой зоны. Если это невозможно, необходимо предусмотреть линейное зашумление посторонних проводников;

– прокладку трубопроводов и коммуникаций горизонтальной разводки рекомендуется осуществлять открытым способом или за фальшпанелями, допускающими их демонтаж и осмотр;

– в местах выхода трубопроводов технических коммуникаций за пределы выделенных помещений рекомендуется устанавливать гибкие виброизолирующие вставки с заполнением пространства между ними и строительной конструкцией раствором на всю

толщину конструкции. В случае невозможности установки вставок потребуется оборудование трубопроводов системой вибрационного зашумления;

– необходимо предусматривать прокладку вертикальных стояков коммуникаций различного назначения вне пределов зоны выделенных помещений;

– ограждающие конструкции выделенных помещений, смежные с другими помещениями организации, не должны иметь проемы, ниши, а также сквозные каналы для прокладки коммуникаций;

– систему приточно-вытяжной вентиляции и воздухообмена зоны выделенных помещений целесообразно сделать отдельной, она не должна быть связана с системой вентиляции других помещений организации и иметь свой отдельный забор и выброс воздуха;

– короба системы вентиляции рекомендуется выполнять из неметаллических материалов. Внешняя поверхность коробов вентиляционной системы, выходящих из выделенной зоны или отдельных важных помещений, должна предусматривать их отделку звукопоглощающим материалом. В местах выхода коробов вентиляционных систем из выделенных помещений рекомендуется установить мягкие виброизолирующие вставки из гибкого материала, например брезента или плотной ткани. Выходы вентиляционных каналов за пределами зоны выделенных помещений должны быть закрыты металлической сеткой;

– в помещениях, оборудованных системой звукоусиления, целесообразно применять облицовку внутренних поверхностей ограждающих конструкций звукопоглощающими материалами;

– дверные проемы в особо важных помещениях необходимо оборудовать тамбурами;

– декоративные панели отопительных батарей должны быть съемными для осмотра;

– в особо важных выделенных помещениях не рекомендуется использование подвесных потолков, особенно неразборной конструкции;

– для остекления особо важных выделенных помещений рекомендуется применение солнцезащитных и теплозащитных стеклопакетов;

– полы особо важных выделенных помещений целесообразно делать без плинтусов;

– в выделенных помещениях не рекомендуется применять светильники люминесцентного освещения. Светильники с лампами накаливания следует выбирать на полное сетевое напряжение без применения трансформаторов и выпрямителей.

Ввод в эксплуатацию системы технической защиты информации

На **третьем этапе** силами монтажных и строительных организаций осуществляется выполнение мероприятий по защите информации, предусмотренных техническим проектом. К работам по монтажу технических средств обработки информации, вспомогательных технических средств, а также проведения технических мероприятий по защите информации должны привлекаться организации, имеющие лицензию ФСТЭК РФ.

Монтажной организацией или заказчиком проводятся закупка сертифицированных ТСОИ и специальная проверка несертифицированных ТСОИ на предмет обнаружения возможно внедренных в них электронных устройств перехвата информации (“закладок”) и их специальные исследования.

По результатам специальных исследований ТСОИ уточняются мероприятия по защите информации. В случае необходимости вносятся соответствующие изменения в технический проект, которые согласовываются с проектной организацией и заказчиком.

Проводятся закупка сертифицированных технических, программных и программно-технических средств защиты информации и их установка в соответствии с техническим проектом.

Службой (специалистом) безопасности организуется контроль проведения всех мероприятий по защите информации, предусмотренных техническим проектом.

В период установки и монтажа ТСОИ и средств защиты информации особое внимание должно уделяться обеспечению режима и охране защищаемого объекта.

К основным рекомендациям на этот период можно отнести следующие [1, 2, 4 – 9]:

– организацию охраны и физической защиты помещений объекта информатизации и выделенных помещений, исключающих несанкционированный доступ к ТСОИ, их хищение и нарушение работоспособности, хищение носителей информации;

– при проведении реконструкции объекта должен быть организован контроль и учет лиц и транспортных средств, прибывших и покинувших территорию проводимых работ;

– рекомендуется организовать допуск строителей на территорию и в здание по временным пропускам или ежедневным спискам;

– копии строительных чертежей, особенно поэтажных планов помещений, схем линий электропитания, связи, систем охранной и пожарной сигнализации и т.п. должны быть учтены, а их число ограничено. По окончании монтажных работ копии чертежей, планов, схем и т.п. подлежат уничтожению установленным порядком;

– необходимо обеспечить хранение комплектующих и строительных материалов на складе под охраной;

– не рекомендуется допускать случаев проведения монтажных операций и отделочных работ, выполняемых одиночными рабочими, особенно в ночное время;

– на этапе отделочных работ необходимо обеспечить ночную охрану здания.

К некоторым мероприятиям по организации контроля в этот период можно отнести:

– перед монтажом необходимо обеспечить скрытную проверку всех монтируемых конструкций, особенно установочного оборудования, на наличие разного рода меток и отличий их друг от друга, а также закладных устройств;

– необходимо организовать периодический осмотр зон выделенных помещений в вечернее или в нерабочее время при отсутствии в нем строителей в цельях выявления подозрительных участков и мест;

– организовать контроль за ходом всех видов строительных работ на территории и в здании. Основная функция контроля заключается в подтверждении правильности технологии строительно-монтажных работ и соответствия их техническому проекту;

– организовать осмотр мест и участков конструкций, которые по технологии подлежат закрытию другими конструкциями. Такой контроль может быть организован легально под легендой необходимости проверки качества монтажа и материалов или скрытно;

– необходимо тщательно проверять соответствие монтажных схем и количество прокладываемых проводов техническому проекту. Особое внимание необходимо уделять этапу ввода проводных коммуникаций и кабелей в зону выделенных помещений. Все прокладываемые резервные провода и кабели необходимо нанести на план-схему с указанием мест их начала и окончания.

При проведении контроля особое внимание необходимо обращать на следующие моменты:

– несогласованное с заказчиком изменение количественного состава бригад, изменение их персонального состава, особенно в период длительных по времени однотипных процессов;

– наличие отклонений от согласованной или стандартной технологии строительно-монтажных работ;

– недопустимы большие задержки по времени выполнения стандартных монтажных операций;

– неожиданная замена типов строительных материалов и элементов конструкций;

– изменение схем и порядка монтажа конструкций;
– проведение работ в обеденное или в нерабочее время, особенно ночью;
– психологические факторы поведения отдельных строителей в присутствии контролирующих и т.п.

Перед установкой в выделенные помещения и на объекты информатизации мебели и предметов интерьера технические устройства и средства оргтехники должны проверяться на отсутствие закладных устройств. Одновременно целесообразно провести проверку технических средств на уровни побочных электромагнитных излучений. Такую проверку целесообразно проводить в специально оборудованном помещении или на промежуточном складе.

После отделки рекомендуется провести всесторонний анализ здания на возможность утечки информации по акустическим и вибрационным каналам. По результатам измерений с учетом реальной ситуации по режиму охраны должны быть разработаны дополнительные рекомендации по усилению мер защиты, если имеет место невыполнение требований по защите.

До начала монтажа ТСОИ и средств защиты информации заказчиком определяются подразделения и лица, планируемые к назначению ответственными за эксплуатацию СТЗИ. В процессе монтажа средств защиты и их опытной эксплуатации происходит обучение назначенных лиц специфике работ по защите информации.

Совместно с представителями проектной и монтажной организаций ответственными за эксплуатацию СТЗИ осуществляется разработка эксплуатационной документации на объект информатизации и выделенные помещения (технических паспортов объектов, инструкций, приказов и других документов).

Технический паспорт на объект защиты разрабатывается лицом, назначенным ответственным за эксплуатацию и безопасность информации на данном объекте, и включает:

– пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
– перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
– перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
– перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
– перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
– перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
– схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границ контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
– технологические поэтажные планы здания (в масштабе) с указанием мест расположения объектов информатизации и выделенных помещений, характеристик их стен, перекрытий, материалов отделки, типов дверей и окон;
– планы объектов информатизации (в масштабе) с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
– план-схему инженерных коммуникаций всего здания, включая систему вентиляции;

– план-схему системы заземления объекта, с указанием места расположения заземлителя;

– план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;

– план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;

– план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;

– схемы систем активной защиты (если они предусмотрены).

К техническому паспорту прилагаются:

– предписания на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;

– сертификаты соответствия требованиям безопасности информации на ВТСС;

– сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;

– акты на проведенные скрытые работы;

– протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин;

– протоколы измерения величины сопротивления заземления;

– протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки.

После установки и монтажа технических средств защиты информации проводится их опытная эксплуатация в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации.

По результатам опытной эксплуатации проводятся приемо-сдаточные испытания средств защиты информации с оформлением соответствующего акта.

По завершении ввода в эксплуатацию СТЗИ проводится аттестация объектов информатизации и выделенных помещений по требованиям безопасности. Она является процедурой официального подтверждения эффективности комплекса реализованных на объекте мер и средств защиты информации.

При необходимости по решению руководителя организации могут быть проведены работы по поиску электронных устройств съема информации (“закладных устройств”), возможно внедренных в выделенные помещения, осуществляемые организациями, имеющими соответствующие лицензии ФСБ России.

В период эксплуатации периодически должны проводиться специальные обследования и проверки выделенных помещений и объектов информатизации. Специальные обследования должны проводиться под легендой для сотрудников организации или в их отсутствие (допускается присутствие ограниченного круга лиц из числа руководителей организации и сотрудников службы безопасности).

Методические указания к лабораторным занятиям

Лабораторная работа 1. Современные угрозы и модели каналов утечки информации

Задание

Разработать модели каналов утечки информации для экономического объекта.

Обнаружение и распознавание технических каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков или индикаторов каналов утечки информации могут служить указанные в табл.

Таблица

Вид канала	Индикаторы
Оптический	Просматриваемость помещений из окон противоположных домов. Близость к окнам деревьев.Отсутствие на окнах занавесок, штор, жалюзей. Просматриваемость содержания документов на столах со сторон окон, дверей, шкафов в помещении.Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении. Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Складирование продукции во дворе без навесов. Малая высота забора и дырки в нем. Переноска и перевозка образцов продукции в открытом виде. Появление возле территории организации (предприятия)посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино- и видеокамерами.
Радиоэлектронный	Наличие в помещении радиоэлектронных средств, ПЭВМ, ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Близость к жилым домам и зданиям иных организаций. Использование в помещении средств радиосвязи. Параллельная прокладка кабелей в одном жгуте при разводке их внутри здания и на территории организации. Отсутствие заземления радио- и электрических приборов. Длительная и частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми.
Акустический	Малая толщина дверей и стен помещения Наличие в помещении открытых вентиляционных отверстий Отсутствие экранов на отопительных батареях Близость окон к улице и ее домам.Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле организации чужих автомобилей.
Вещественный	Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками конфиденциальной информации нанеучтенных листах бумаги.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации — руководителя фирмы, работающего в своем кабинете, утечка информации возможна по следующим каналам:

- через дверь в приемную или коридор;
- через окно на улицу или во двор;
- через вентиляционное отверстие в соседние помещения;
- с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения;
- по трубам отопления в другие помещения здания;
- через стены, потолок и пол в соседние помещения;
- с помощью закладных устройств за территорию фирмы.

Моделирование технических каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации. В основном применяются вербальные и математические модели. Физическое моделирование каналов утечки затруднено и часто невозможно по следующим причинам:

- приемник сигнала канала является средством злоумышленника, его точное месторасположение и характеристики службе безопасности неизвестны;
- канал утечки включает разнообразные инженерные конструкции (бетонные ограждения, здания, заборы и др.) и условия распространения носителя (переотражения, помехи и т. д.), воссоздать которые на макетах невозможно или требуются огромные расходы.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют **структурная** и**пространственная** модели. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве: места расположения источника и приемника сигналов, удаленность их от границ территории организации, ориентация вектора распространения носителя информации в канале утечки информации и ее протяженность. Структурную модель канала целесообразно представлять в табличной форме, пространственную —в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Структурная и пространственная модели не являются автономными, а взаимно дополняют друг друга.

Динамику канала утечки информации описывают **функциональная** и **информационная** модели. Функциональная модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а информационная содержат характеристики информации, утечка которойвозможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Указанные модели объединяются и увязываются между собой в рамках **комплексной модели** канала утечки. В ней указываются интегральные параметры канала утечки информации: источник информации и ее вид, источник сигнала, среда распространения и ее протяженность, место размещения приемника сигнала, риск канала и величина потенциального ущерба. Каждый вид канала содержит свой набор показателей источника и приемника сигналов в канале, позволяющих оценить длину технического канала утечки информации и показатели возможностей органов государственнойи коммерческой разведки.

Так как приемник сигнала является принадлежностью злоумышленника и точное место его размещения и характеристики не известны, то моделирование канала проводит-

ся применительно к гипотетическому приемнику. В качестве приемника целесообразно рассматривать приемник, параметры которого соответствуют современному уровню, а место размещения выбрано рационально. Уважительное отношение к интеллекту и техническим возможностям противника гарантирует от крупных ошибок в значительно большей степени, чем пренебрежительное.

При описании приемника сигнала необходимо учитывать реальные возможности злоумышленника. Очевидно, что приемникисигналов коммерческой разведки не могут, например, размещаться на космических аппаратах. Что касается технических характеристик средств добывания, то они для государственной и коммерческой разведки существенно не отличаются. Расположение приемника злоумышленника можно приблизительно определить исходя из условий обеспечения значения отношения сигнал/помеха на входе приемника, необходимого для съема информации с допустимым качеством, и безопасности злоумышленника или его аппаратуры.

Если возможное место размещения приемника сигналов выбрано, то в ходе моделирования канала рассчитывается энергетика носителя на входе приемника с учетом мощности носителя на выходе источника, затухания его в среде распространения, уровня помех, характеристик сигнала и его приемника.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в табл.

Таблица

Источникинформации	Путь утечки информации	Вид канала	Длина канала	Риск утечки	Величинаущерба	Ранг угрозы
1	2	3	4	5	6	7
...	...	...	...	...	...	...

В графе 2 указываются основные элементы канала утечки информации (источника сигналов, среды распространения и возможные места размещения приемника сигналов). По физической природе носителя определяется вид канала утечки информации, который указывается в столбце 3. По расстоянию между источником сигнала (информации) и приемником сигнала (получателя) определяется длина канала, значение которой вписывается в графу столбца 4. Риск утечки информации (столбец 5) по рассматриваемому каналу оценивается близостью параметров канала и сигнала на входе его приемника к нормативным значениям, при которых риск (вероятность) утечки ниже допустимого значения. Он зависит от совокупности факторов, влияющих на характеристики канала утечки: разрешающей способности приемника сигналов, их энергетики, вероятности выполнения временного условия разведывательного контакта средства добывания с источником информации. В зависимости, например, от принадлежности противоположного дома к жилому или административному, из окна которого возможно в принципе наблюдение за объектом защиты, существенно различаются оценки реальности использования этого оптического потенциального канала утечки для добывания информации. Если дом жилой, то злоумышленнику под видом сотрудника спецслужбы или за деньги проще договориться с жильцами о снятии на определенное время комнаты, чем с руководством организации. При определении реальности канала следует учитывать степень выполнения временного и энергетического условий разведывательного контакта с источником информации. Для обеспеченияврменного контакта надо или знать время проявления демаскирующих признаков объекта или наблюдение должно вестись непрерывно в течение, например, рабочего дня. Для выполнения энергетического условия разведывательного контакта необходимо, чтобы длина ка-

нала была больше расстояния от источника информации до злоумышленника или его приемника сигнала.

Моделирование угроз безопасности информации завершается их ранжированием в табл.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например по виду, положению в пространстве, способам и средствам защиты, угрозам.

Контрольные вопросы

1. Что включает в себя система передачи информации?
2. В чем заключается отличие канала утечки информации от основного канала связи?
3. Какой из факторов, влияющих на вероятность обнаружения (распознавания) объекта, является неконтролируемым для владельца объекта?
4. Насколько уровень шума должен превышать уровень речевого сигнала, чтобы обеспечить гарантированную защищенность речевой информации от подслушивания?
5. Что относиться к основным мерам защиты информации от утечки по вещественному каналу?

Лабораторная работа 2. Методы и средства защиты информации от утечки по техническим каналам.

Задание

1. Рассмотреть методы и средства технической защиты информации применительно к банку, медицинскому и образовательному учреждению.
2. Дать характеристику различным устройствам, используемым для технической защиты.

Защита информации от утечки по техническим каналам при ее обработке с использованием технических средств осуществляется с применением пассивных и активных методов технической защиты информации.

Пассивные методы защиты информации направлены на:

– ослабление побочных электромагнитных излучений (информационных сигналов) ОТСС на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

– ослабление наводок побочных электромагнитных излучений в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

– исключение или ослабление просачивания информационных сигналов в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Активные методы направлены на:

– создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала;

– создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала.

Рассмотрим более подробно наиболее распространенные методы пассивной и активной защиты.

Экранирование

Как известно из предыдущих лекций, при функционировании технических средств обработки, приема, хранения и передачи информации (ТСПИ) создаются побочные токи и поля, которые могут быть использованы злоумышленником для съема информации. Между двумя токопроводящими элементами могут возникнуть следующие виды связи:

– через электрическое поле;
– через магнитное поле;
– через электромагнитное поле;
– через соединительные провода.

Основной характеристикой поля является его напряженность. Для электрического и магнитного полей в свободном пространстве она обратно пропорциональна квадрату расстояния от источника сигнала. Напряженность электромагнитного поля обратно пропорциональна первой степени расстояния. Напряжение на конце проводной или волновой линии с расстоянием падает медленно. Следовательно, на малом расстоянии от источника сигнала имеют место все четыре вида связи. По мере увеличения расстояния сначала исчезают электрическое и магнитное поля, затем - электромагнитное поле и на очень большом расстоянии влияет только связь по проводам и волноводам.

Одним из наиболее эффективных пассивных методов защиты информации при обработке техническими средствами является экранирование. **Экранирование** - локализация электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами.

Различают три вида экранирования:

– электростатическое;
– магнитостатическое;
– электромагнитное.

Электростатическое экранирование заключается в замыкании электростатического поля на поверхность металлического экрана и отводе электрических зарядов на землю (на корпус прибора) с помощью контура заземления. Последний должен иметь сопротивление не больше 4 Ом. Применение металлических экранов весьма эффективно и позволяет полностью устранить влияние электростатического поля. При правильном использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника сигнала в ? раз, где ? - относительная диэлектрическая проницаемость материала экрана.

Эффективность применения экрана во многом зависит от качества соединения корпуса ТСПИ с экраном. Здесь особое значение имеет отсутствие соединительных проводов между частями экрана и корпусом ТСПИ.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов.

Электромагнитное экранирование применяется на высоких частотах. Действие такого экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданными вихревыми токами обратного напряжения. Этот способ экранирования может ослаблять как магнитные, так и электрические поля, поэтому называется электромагнитным.

Упрощенная физическая сущность электромагнитного экранирования сводится к тому, что под действием источника электромагнитной энергии на стороне экрана, обращенной к источнику, возникают заряды, а в его стенках - токи, поля которых во внешнем пространстве противоположны полям источника и примерно равны ему по интенсивности. Два поля компенсируют друг друга.

Выбор материала для экрана зависит от многих условий. Металлические материалы выбирают по следующим критериям и условиям:

– необходимость достижения определенной величины ослабления электромагнитного поля при наличии ограничения размеров экрана и его влияния на объект защиты;

– устойчивость и прочность металла как материала.

Среди наиболее распространенных металлов для изготовления экранов можно назвать сталь, медь, алюминий, латунь. Популярность этих материалов в первую очередь обусловлена достаточно высокой эффективностью экранирования. Сталь популярна также вследствие возможности использования сварки при монтаже экрана.

К недостаткам листовых металлических экранов можно отнести высокую стоимость, большой вес, крупные габариты и сложность монтажа. Этих недостатков лишены **металлические сетки**. Они легче, проще в изготовлении и размещении, дешевле. Основными параметрами сетки является ее шаг, равный расстоянию между соседними центрами проволоки, радиус проволоки и удельная проводимость материала сетки. К недостаткам металлических сеток относят, прежде всего, высокий износ по сравнению с листовыми экранами.

Для экранирования также применяются **фольговые материалы**. К ним относятся электрически тонкие материалы толщиной 0,01…0,05 мм. Фольговые материалы в основном производятся из диамагнитных материалов - алюминий, латунь, цинк.

Перспективным направлением в области экранирования является применение **токопроводящих красок**, так как они дешевые, не требуют работ по монтажу, просты в применении. Токопроводящие краски создаются на основе диэлектрического пленкообразующего материала с добавлением в него проводящих составляющих, пластификатора и отвердителя. В качестве токопроводящих пигментов используют коллоидное серебро, графит, сажу, оксиды металлов, порошковую медь, алюминий.

Токопроводящие краски лишены недостатков листовых экранов и механических решеток, так как достаточно устойчивы в условиях резких климатических изменений и просты в эксплуатации.

Следует отметить, что экранироваться могут не только отдельные технические средства, но и помещения в целом. В неэкранированных помещениях функции экрана частично выполняют железобетонные составляющие в стенах. В окнах и дверях их нет, поэтому они более уязвимы.

При экранировании помещений используются: листовая сталь толщиной до 2 мм, стальная (медная, латунная) сетка с ячейкой до 2,5 мм. В защищенных помещениях экранируются двери и окна. Окна экранируются сеткой, металлизированными шторами, металлизацией стекол и оклеиванием их токопроводящими пленками. Двери выполняются из стали или покрываются токопроводящими материалами (стальной лист, металлическая сетка). Особое внимание обращается на наличие электрического контакта токопроводящих слоев двери и стен по всему периметру дверного проема. При экранировании полей недопустимо наличие зазоров, щелей в экране. Размер ячейки сетки должен быть не более 0,1 длины волны излучения.

В защищенной ПЭВМ, например, экранируются блоки управления электронно-лучевой трубкой, корпус выполняется из стали или металлизируется изнутри, экран монитора покрывается токопроводящей заземленной пленкой и (или) защищается металлической сеткой.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ИС считается групповое размещение их информационных кабелей в экранирующий распределительный короб.

Контрольные вопросы

1. Какие мероприятий защиты информации относятся к инженерно-техническим?
2. Что составляет систему защиты информации?
3. Что относится к недостаткам аппаратных средств инженерно-технической защиты.
4. Что относится к достоинствам программных средств инженерно-технической защиты.
5. Назвать средства защиты информации от утечки информации по техническим каналам связи.
6. Назвать несколько приборов для технической защиты информации?
7. Какая организация занимается сертификацией приборов технической защиты информации?

Лабораторная работа3. Контроль эффективности защиты информации от ее утечки по техническим каналам.

Задание

1. Изучить возможности операционной системы специального назначения «AstraLinuxSpecialEdition» РУСБ.10015-01 для выполнения контроля эффективности защиты информации от ее утечки по техническим каналам.
2. Изучить возможности программных продуктов XSpiderEducation, MaxPatrolEducation для выполнения контроля эффективности защиты информации от ее утечки по техническим каналам.

Контрольные вопросы

1. Какие мероприятий выполняются для контроля эффективности защиты информации?
2. Что составляет систему защиты информации?
3. Что относится к недостаткам аппаратных средств инженерно-технической защиты.
4. Перечислить направление инженерно-техническая защита.
5. Выполнить классификация средств инженерно-технической защиты.
6. Дать краткую характеристику основных классов средств инженерно-технической защиты.
7. Перечислить способы защиты информации.
8. Выделить классы способов защиты (мероприятий по защите информации).

Лабораторная работа4. Организация работ по защите информации от утечки по техническим каналам.

Задание.

1. Заполнить таблицу 1, 2, 3, 4 для банка, медицинского и образовательного учреждения.

Так как не существует формальных методов синтеза вариантов предотвращения угроз информации, то разработка мер по защите информации проводится эвристическим путем на основе знаний и опыта соответствующих специалистов. Перечень типовых способов и средств защиты информации приведен в табл.

Таблица 1.

Угрозы и способы их реализации	Типовые способы и средства предотвращения угроз
Физический контакт злоумышленника с источником информации	Механические преграды (заборы, КПП, двери, взло-мостойкие стекла, решетки на окнах, хранилища, сейфы), технические средства охраны, телевизионные средства наблюдения, дежурное и охранное освещение, силы и средства нейтрализации угроз
Пожар	Технические средства пожарной сигнализации, средства пожаротушения, огнестойкие хранилища и сейфы
Наблюдение	Маскировочное окрашивание, естественные и искусственные маски, ложные объекты, аэрозоли, пены, радиолокационные отражатели, радио- и звукопоглощающие покрытия, теплоизолирующие материалы, генераторы радио- и гидроакустических помех
Подслушивание	Скремблирование и цифровое шифрование, звукоизолирующие конструкции, звукоизолирующие материалы, акустическое и вибрационное зашумление, обнаружение, изъятие и разрушение закладных устройств
Перехват	Выполнение требований по регламенту и дисциплине связи, отключение источников опасных сигналов, фильтрация и ограничение опасных сигналов, применение буферных устройств, экранирование, пространственное и линейное зашумление
Утечка информации по вещественному каналу	Учет и контролируемое уничтожение черновиков, макетов, брака, сбор и очистка от демаскирующих веществ отходов

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в табл.

Таблица 2

Угроза	*Способы предотвращения угрозы*	*Средства предотвращения угрозы*	*Затраты на предотвращения угроз*	*Выбранные способы и средства предотвращения угроз*	*Затраты на выбранные способы и средства*
1	2	3	4	5	6
…	…	…	…	…	…

Совокупность рассмотренных таблиц, планов и схем с результатами- моделирования объектов защиты и угроз, а также предложений по способам и средствам защиты информации создают основу проекта по построению соответствующей системы или предложении по совершенствованию существующей системы.

В итоговой части проекта (служебной записке, предложениях) целесообразно оценить полноту выполнения задач по защите информации для выделенных ресурсов, а также нерешенные задачи и необходимые для их решения ресурсы.

Подготовленные документы (проект, служебная записка, предложения) предъявляются руководству для принятия решения. Наличие в них нескольких вариантов решений способствует более активному участию в построении или совершенствованию системы защиты информации руководителя организации в качестве как наиболее опытного и квалифицированного специалиста, так и распорядителя ресурсов организации.

После принятия проекта (предложений) начинается этап их реализации. Основные задачи специалистов по защите информации заключаются в контроле за работами по выполнению организационных и технических мероприятий, участие в приемке результатов работ и проверке эффективности функционирования элементов и системы защиты в целом.

Результаты оформляются в виде предложений (проекта) в кратком сжатом виде, а материалы моделирования — в виде приложения с обоснованием предложений.

В заключение следует отметить, что материалы с предложениями и их обоснованием, в которых раскрываются методы и средства защиты информации, нуждаются в обеспечении высокого уровня безопасности, а обобщенные документы должны иметь наиболее высокий гриф из применяемых в организации.

Выбор технических средств охраны

Многообразие технических средств физической защиты порождает весьма сложную задачу их рационального выбора для конкретных условий по критерию эффективность-стоимость. На рубежах охраны технические средства обнаружения определяются с учетом вида рубежа, способов обнаружения злоумышленника и пожара, а также значений конкретных тактико-технических характеристик (ТТХ) средств охраны.

Выбор извещателей

Тип извещателя выбирается с учетом вида охраняемого рубежа или зоны, их размеров и конфигурации, вида воздействия злоумышленника и помех на преграду, затрат на приобретение, установку (строительство) и эксплуатацию инженерных конструкций и технических средств.

Эффективное использование технических возможностей извещателей достигается, когда размеры блокируемого участка (зоны) близки к соответствующим характеристикам извещателя. Рекомендуемое соотношение между длиной (площадью) $L_{бл}(S_{бл})$ реальной охраняемой (блокируемой) зоны и максимальной дальностью (площадью) зоны охраны$L_{из}(S_{из})$ извещателя:

$$L_{бл}(S_{бл}) = (0,7\text{-}0,9)L_{из}(S_{из}).$$

Виды воздействий злоумышленников на механические преграды указаны в табл.

Таблица 3

№ п/п	Объект охраны	Вид воздействия
1	Капитальные стены	Удар, разрушение
2	Некапитальные стены и перегородки	Пролом
3	Металлические двери и ворота	Открывание, удар
4	Дверные проемы, погрузочно-разгрузочные люки, деревянные ворота	Открывание, пролом
5	Остекленные конструкции	Открывание, разрушение
6	Вентиляционные короба	Открывание, разрушение

Существенное влияние на выбор извещателя оказывает помеховая ситуация в районе его размещения в интервале времени, когда он находится во включенном состоянии. Помеховая ситуация может существенно изменяться. Например, рядом с охраняемым зданием могут начаться строительные работы с использованием тяжелой техники, работа которой вызывает значительные акустические помехи. Усредненное влияние помех различных типов на извещатели характеризуется данными табл.

Таблица 4

№ п/п	Вид помехи	Вид извещателя				
		акустический	оптико-электронный	радиоволновый	емкостной	вибрационный
1	Внешние акустические шумы (уличные, раскаты грома и др.)	+	–	–	–	+
2	Внутренние (в контролируемой зоне) акустические шумы (холодильники, ТА, шум воды в трубах и др.)	+	–	–	–	–
3	Внешний свет (свет фар, солнечные блики)	–	+	–	–	–
4	Движение воздуха в помещении (сквозняки, вентиляторы, батареи отопления)	–	+	–	–	–
5	Движение предметов (штор, лопастей вентилятора, воды на стеклах, листьев и др.)	+	+	+	–	–
6	Электромагнитные помехи (сварочные ап-ты, разряды высоковольтных линий, трамваев, троллейбусов, люминесцентные лампы и др.)	–	–	–	+	–
7	Мелкие животные, крупные насекомые	+	+	+	+	+

Методические указания к практическим занятиям

Практическая работа 1.Современные угрозы и модели каналов утечки информации

Задание.

Провести анализ возможных технических каналов утечки информации организации или предприятия. Определить и классифицировать потенциальные угрозы информации, демаскирующие признаки объектов защиты, элементы системы защиты предприятия

Требования: Описание мер и используемых инженерно-технических средств, для обеспечения мер информационной безопасности АС организации; анализ возможных технических каналов утечки информации организации; рекомендации по устранению возможной утечки информации по техническим каналам; соответствия оформления и содержания требованиям выпускной квалификационной работе; защита проекта с использованием мультимедийных средств.

Контрольные вопросы

6. Что включает в себя система передачи информации?
7. В чем заключается отличие канала утечки информации от основного канала связи?
8. Какой из факторов, влияющих на вероятность обнаружения (распознавания) объекта, является неконтролируемым для владельца объекта?
9. Насколько уровень шума должен превышать уровень речевого сигнала, чтобы обеспечить гарантированную защищенность речевой информации от подслушивания?
10. Что относиться к основным мерам защиты информации от утечки по вещественному каналу?

Практическая работа 2. Методы и средства защиты информации от утечки по техническим каналам.

Задание

1. Рассмотреть банковское предприятие с точки зрения утечки информации по техническим каналам связи. Предложить методы и средства защиты информации от утечки информации по техническим каналам связи.

Контрольные вопросы

1. Какие мероприятий защиты информации относятся к инженерно-техническим?
2. Что составляет систему защиты информации?
3. Что относится к недостаткам аппаратных средств инженерно-технической защиты.
4. Что относится к достоинствам программных средств инженерно-технической защиты.
5. Назвать средства защиты информации от утечки информации по техническим каналам связи.

Практическая работа3. Контроль эффективности защиты информации от ее утечки по техническим каналам.

Задание

1. Для задания, выполненного на предыдущем занятии выработать набор мероприятий для контроля эффективности защиты информации.

Контрольные вопросы

1. Какие мероприятий выполняются для контроля эффективности защиты информации?
2. Что составляет систему защиты информации?
3. Что относится к недостаткам аппаратных средств инженерно-технической защиты.
4. Перечислить направление инженерно-техническая защита.
5. Выполнить классификация средств инженерно-технической защиты.
6. Дать краткую характеристику основных классов средств инженерно-технической защиты.
7. Перечислить способы защиты информации.
8. Выделить классы способов защиты (мероприятий по защите информации).

Практическая работа4. Организация работ по защите информации от утечки по техническим каналам.

Задание.

1. Рассмотреть набор документов, необходимый для разработки системы защиты информации от утечки по техническим каналам на предприятии
2. Разработать техническое задание для разработки системы защиты информации от утечки по техническим каналам для банка.
3. Разработать техническое задание для разработки системы защиты информации от утечки по техническим каналам для медицинского учреждения.
4. Разработать техническое задание для разработки системы защиты информации от утечки по техническим каналам для образовательного учреждения.

Контрольные вопросы

1. Какой набор документов необходим для разработки системы защиты информации?
2. Что представляет собой техническое задание на разработку системы защиты информации
3. Каковы уровни доступа к информации с точки зрения законодательства?
4. Что такое информация ограниченного распространения?
5. Каковы виды доступа к информации?
6. В чем может заключаться ответственность за нарушение законодательства в информационной сфере?
7. Что такое Доктрина ИБ РФ?