Содержание:

Введение

В современном мире создаются все новые и новые информационные технологии, которые улучшают и облегчают деятельность человека. Доступ к необходимой информации открывает неограниченные возможности. Но, в настоящее время, доступ к информации, представляющей ценность и являющейся собственностью ограничен нормативно-правовыми актами (документами), устанавливающими права доступа к информации. Тем не менее всегда существует информационная угроза в лице конкурентов, недоброжелателей, иностранных разведок. Развитие средств вычислительной техники и глобальных сетей дают человеку, владеющему информацией, значительные приемущества. Естественно, что доступ к информации в ряде случаев должен быть ограничен.

Проблема защиты информации существовала всегда, но в настоящее время из-за огромного скачка научно-технического прогресса она прибрела особую актуальность. Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое распространение средств электронной вычислительной техники (ЭВТ); усложнение криптографических технологий и средств; необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн; расширяющиеся возможности несанкционированных действий над информацией.

Кроме того, в настоящее время получили широкое распространение средства и методы несанкционированного и негласного добывания информации. Они находят все большее применение не только в деятельности государственных правоохранительных органов, но и в деятельности разного рода преступных группировок.

Необходимо учитывать, что естественные каналы утечки информации образуются практически постоянно, в силу специфических особенностей объекта защиты.

Искусственные каналы утечки информации создаются преднамеренно с применением активных методов и способов получения информации. Активные способы предполагают намеренное создание технического канала утечки

информации с использованием специальных технических средств - электронных средств негласного получения информации (ЭУНПИ). К ним можно отнести незаконное подключение к каналам, проводам и линиям связи, высокочастотное навязывание и облучение, установка в технических средствах и помещениях микрофонов и телефонных ЭУНПИ, а также несанкционированный доступ к информации, обрабатываемой в автоматизированных системах (АС) и т.д.

Исходя из практики мероприятий обеспечения ИБ, требуются лишь известные усилия соответствующих органов, сил и средств, а также их соответствующее обеспечение всем необходимым.

Вместе с тем, проблемных вопросов по защите информации множество, их решение зависит от объективных и субъективных факторов, в том числе и дефицит возможностей.

Объектом исследования являются объекты вычислительной техники, выделенные помещения.

Предметом исследования являются методы и средства предотвращения утечки информации по техническим каналам.

Цель курсовой работы - систематизация и расширение знаний, умений в ходе оценки эффективности технической защиты информации типового объекта ТСПИ.

Провести оценку эффективности мероприятий ТЗИ и разработать рекомендации должностным лицам органов ТЗИ службы ЗГТ по повышению защищенности объектов ТСПИ от утечки по техническим каналам.

1. Анализ угроз утечки защищаемой информации

1.1. Классификация и возможности технических разведок иностранных государств

По направлениям разведывательной деятельности иностранные разведки подразделяется на политическую, экономическую, военную и научно-техническую разведки.

Политическая разведка осуществляет деятельность по добыванию сведений внутриполитического и внешнеполитического характера в стране, являющейся объектом разведки, организует действия по подрыву политического строя государства. Примером могут служить организация «цветных революций» в некоторых странах постсоветского пространства, свержение неугодных режимов на Ближнем Востоке.

Экономическая разведка занимается сбором сведений, раскрывающих экономический потенциал определенной страны. К таким сведениям относятся характеристики природных ресурсов, промышленности, транспорта, финансовой системы, торговли и т.п.

Военная разведка направлена на сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники. Особое внимание иностранные разведки уделяют добыванию информации о научно-исследовательских центрах, видных ученых и специалистах. Научно-техническая разведка занимается добыванием сведений по новейшим теоретическим и практическим разработкам в области науки и техники.

Основные формы разведывательной деятельности:

- агентурная разведка;

- легальная разведка;

- техническая разведка;

- аналитическая обработка первичной информации.

Техническая разведка предполагает сбор информации с использованием технических разведывательных средств.

Техническую разведку (ТР) можно классифицировать по нескольким признакам. Первый признак связан с используемыми носителями средств добывания информации, в соответствии с которым ТР делится:

а) по принадлежности:

1) к государству;

2) к структуре.

б) по местоположению носителей разведывательной аппаратуры:

1) космическая;

2) наземная;

3) воздушная;

4) морская.

в) по территориальным особенностям применения средств разведки:

1) с территории иностранных государств;

2) по территории России;

3) в нейтральных водах;

4) в территориальных водах.

Второй признак связан с используемой аппаратурой и способами ведения разведки. Согласно этому признаку к ТР относятся следующие виды разведок:

а) оптическая и оптоэлектронная разведки;

б) визуально-оптическая разведка;

в) фотографическая разведка;

г) инфракрасная разведка (ИКР);

д) радиоэлектронная разведка (РЭР);

е) радиоразведка;

ж) радиотехническая;

к) радио- и радиотехническая разведки;

л) радиолокационная разведка;

м) телевизионная разведка;

н) лазерная разведка;

п) фотометрическая разведка;

р) гидроакустическая разведка;

с) акустическая разведка.

В зависимости от физической природы возникновения сигналов, среды распространения акустических колебаний и способов их перехвата, акустические каналы утечки информации можно разделить на воздушные, вибрационные, акустоэлектрические, оптико-электронные и параметрические.

По способу применения технические средства перехвата акустической информации можно классифицировать следующим образом.

Средства, устанавливаемые заходовыми методами:

а) радио-ЭУНПИ;

б) ЭУНПИ с передачей акустической информации в инфракрасном диапазоне;

в) ЭУНПИ с передачей информации по сети 220 В;

г) ЭУНПИ с передачей акустической информации по телефонной линии;

д) диктофоны;

е) проводные микрофоны;

ж) «телефонное ухо».

Средства, устанавливаемые беззаходовыми методами:

а) аппаратура, использующая микрофонный эффект;

б) аппаратура высокочастотного навязывания;

в) стетоскопы;

г) лазерные микрофоны.

Основными принципами разведки по добыванию информации являются:

а) целеустремленность;

б) активность;

в) непрерывность;

г) скрытность;

д) комплексное использование сил и средств добывания информации.

Многообразие видов носителей информации породило множество видов технической разведки. Ее классифицируют по различным признакам. Наиболее широко применяются две классификации: по физической природе носителей информации и видам носителей технических средств добывания.

Классификация технической разведки по физической природе носителя информации представлена на рисунке 1.

Широко распространена классификация разведки по виду носителей средств добывания (наземная, воздушная, космическая, морская разведка).

Кроме того, в практике ТЗИ применяется следующая классификация:

а) стационарная ТСР устанавливаемая в наземные объекты;

б) возимая устанавливается, в основном, в транспортные средства;

в) носимая устанавливается, в основном, на границе КЗ.

Рисунок 1. Классификация технических разведок по физической природе носителя информации

1.2. Технические каналы утечки информации

Наибольший интерес, с точки зрения образования каналов утечки информации, представляют ОТСС и ВТСС, имеющие выход за пределы контролируемой зоны (КЗ). Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС.

Зона с возможностью перехвата разведывательным оборудованием побочных электромагнитных излучений, содержащих информацию, ограниченного доступа называется опасной зоной. Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется опасной зоной 1.

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ.

В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте.

Общая классификация ТКУИ изображена на рисунке 2:

а) по физической природе носителя (оптические, радиоэлектронные, акустические, материально-вещественные);

б) по информативности (информативные, малоинформативные);

в) по времени функционирования (постоянные, эпизодические, случайные);

г) по структуре (одноканальные, составные);

К основным причинам образования ТКУИ относятся:

а) несовершенство элементной базы;

б) несовершенство схемных решений;

в) эксплуатационный износ;

г) злоумышленные действия;

Показатели ТКУИ, позволяющие оценит риск утечки информации:

а) пропускная способность ТКУИ;

б) длина ТКУИ;

в) относительная информативность ТКУИ.

Условия существования ТКУИ:

а) наличие источника с ненулевой мощностью информационного сигнала на выходе

б) наличие канала с конечным уровнем помех, длиной и погонным затуханием, обеспечивающее достаточное соотношение сигнал/шум на входе ТСР

в) ТСР с достаточной чувствительностью для приема информационного сигнала

Рисунок 2. Общая классификация ТКУИ

Основным каналом утечки информации при ее обработке ТСПИ является электромагнитный канал, обусловленный побочными информативными электромагнитными излучениями основных технических средств обработки информации. К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений ОТСС. Побочные электромагнитные излучения (ПЭМИ) – это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ЭМИ) ОТСС:

а) излучений элементов ОТСС;

б) излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;

в) излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ОТСС. В ОТСС носителем информации является электрический ток, параметры которого изменяются по закону информативного сигнала.

Электромагнитные излучения на частотах работы ВЧ генераторов ОТСС и ВТСС. В состав ОТСС и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам относят: задающие генераторы, генераторы тактовой частоты, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

Самовозбуждение УНЧ ОТСС возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов.

Перехват побочных электромагнитных излучений ОТСС осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Зона, в которой возможен перехват побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации, называется опасной зоной 2.

Причинами возникновения электрических каналов утечки информации могут быть:

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

б) просачивание информационных сигналов в цепи электропитания ТСПИ;

в) просачивание информационных сигналов в цепи заземления ОТСС.

Наводки электромагнитных излучений ОТСС возникают при излучении элементами ОТСС информационных сигналов, а также при наличии гальванической связи соединительных линий ОТСС и посторонних проводников или линий ВТСС.

Просачивание информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства.

Просачивание информативных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций.

Параметрический канал утечки информации состоит в следующем: перехват обрабатываемой в технических средствах информации возможен также путем их “высокочастотного облучения”.

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют параметрическим.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

Контактный способ используется в основном для перехвата информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа.

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индукционный канал перехвата информации, не требующий контактного подключения к каналам связи. Современные индукционные датчики способны перехватывать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного перехвата информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

Все многообразие задач защиты объектов от ТСР можно свести к трем типовым задачам:

скрытие защищаемых объектов или их элементов от обнаружения ТСР;

исключение возможности измерения (или снижение точности измерений) характеристик скрываемых объектов;

исключение распознавания скрываемых объектов ТСР.

Решение задач защиты от ТСР осуществляется применением различных способов защиты. В зависимости от характера решаемых задач по защите объектов от ТСР применяются способы скрытия и дезинформации.

Пассивное скрытие должно исключать или существенно затруднять обнаружение и определение характеристик объектов разведки путем устранения или ослабления их демаскирующих признаков. Оно обеспечивается проведением организационных мероприятий и технических мер (рисунок 3).

Рисунок 3. Мероприятия по технической защите информации.

К организационным мероприятиям относят:

а) создание в структуре предприятия подразделения по защите информации (назначить штатного специалиста по защите информации);

б) разработка положения о подразделении по защите информации, должностные инструкции сотрудников;

в) назначение должностных лиц, ответственных за обеспечение защиты информации на объектах и в подразделениях предприятия;

г) определение обязанностей и прав должностных лиц подразделений объекта, ответственных за разработку, обеспечения выполнения мероприятий по защите информации на объекте с соответствующими подразделениями данного объекта;

д) определение подразделения или должностных лиц, ответственных за аттестацию рабочих мест, стендов, вычислительных комплексов, выделенных помещений и т.д., установить форму документирования результатов аттестации и порядка выдачи разрешения на проведение работ с секретной информацией;

е) проведение категорирования объектов информатизации по степени секретности информации, циркулирующей в них. Организовать аттестацию объектов информатизации по требованиям безопасности информации. Провести аттестацию помещений, используемых в качестве выделенных. На каждое помещение оформить аттестационный паспорт.

ж) проведение сертификации средств защиты информации, организовать контроль их эффективности;

к) разработка плана финансирования мероприятий по защите информации на предприятии;

л) определение исполнителей работ по защите информации;

м) организация обучения сотрудников по вопросам защиты информации;

н) определение порядка взаимодействия в области защиты информации с предприятиями при выполнении совместных работ, применяемые совместные организационные и технические мероприятия по защите информации, ответственность, права и обязанности взаимодействующих сторон.

К методически мероприятиям относят:

а) разработка внутреннего Руководства по защите информации от технических разведок и от ее утечки по техническим каналам на предприятии в соответствии с требованиями руководящих документов;

б) разработка общих требований по защите информации на объекте с учетом его категории;

в) определение цели, которая должна быть достигнута в результате проведения мероприятий по защите информации, и пути достижения этой цели. Разработать перечень охраняемых сведений об объекте и его деятельности;

г) определение демаскирующих признаков, которые раскрывают охраняемые сведения об объекте, в том числе демаскирующие признаки, возникающие в связи с использованием средств обеспечения его деятельности.

д) составление перечня видов, средств и возможностей технической разведки, источников угроз несанкционированного доступа к информации, опасных для объекта, в том числе со стороны преступных группировок.

е) определение требований к содержанию планов мероприятий по защите информации, порядок разработки, согласования, утверждения и оформления планов, установить порядок отчетности и контроля за выполнением планов;

ж) определение порядка контроля состояния защиты информации, перечень органов и подразделений, имеющих право проверки состояния защиты информации на объекте, привлекаемые силы и средства контроля;

к) установление периодичности и вида контроля, порядок оформления результатов контроля, определить действия должностных лиц по устранению нарушений норм и требований по защите информации и порядок разработки мероприятий по устранению указанных нарушений;

л) определение внутриобъектовой схемы оповещения и действия должностных лиц при оповещении.

К техническим мероприятиям относят:

а) обеспечение устранения или ослабление демаскирующих признаков и закрытие возможных технических каналов утечки охраняемой информации, осуществить мероприятия по защите информации при постоянном контролируемом и неконтролируемом нахождении иностранных граждан как на территории объекта,

так и в непосредственной близости от него;

б) проведение мероприятия по закупке и установке сертифицированных средств и устройств защиты, оборудование помещений, предназначенных для обработки информации, содержащей государственную тайну, по требованиям режима секретности;

в) проведение государственной аттестации созданной в организации системы защиты информации по требованиям безопасности информации.

2. Методология оценки эффективности мероприятий технической защиты информации объекта

Контроль эффективности предполагает проверку соответствия качественных и количественных показателей эффективности мер технической защиты установленным требованиям или нормам эффективности защиты информации.

Виды контроля эффективности защиты делятся на:

организационный контроль проверку соответствия мероприятий по технической защите информации требованиям руководящих документов;

технический контроль – контроль эффективности технической защиты информации, проводимый с использованием технических средств контроля.

Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что утечка информации с объекта невозможна, т.е. на объекте отсутствуют технические каналы утечки информации. Технический контроль состояния защиты информации в системах управления производствами, транспортом, связью, энергетикой, передачи финансовой и другой информации осуществляется в соответствии со специально разрабатываемыми программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством по подчиненности объекта контроля.

По способу проведения и содержанию технический контроль эффективности технической защиты информации относится к наиболее сложным видам контроля и

может быть:

комплексным, когда проверяется возможная утечка информации по всем опасным каналам контролируемого объекта;

целевым, когда проводится проверка по одному из интересующих каналов возможной утечки информации;

выборочным, когда из всего перечня технических средств на объекте для проверки выбираются только те, которые по результатам предварительной оценки с наибольшей вероятностью имеют опасные каналы утечки защищаемой информации.

В зависимости от вида выполняемых операций методы технического контроля делятся на:

инструментальные, когда контролируемые показатели определяются непосредственно по результатам измерения контрольно-измерительной аппаратурой;

инструментально-расчетные, при которых контролируемые показатели определяются частично расчетным путем и частично измерением значений некоторых параметров физических полей аппаратными средствами;

расчетные, при которых контролируемые показатели рассчитываются по методикам, содержащимся в руководящей справочной литературе.

С целью исключения утечки информации не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на средствах и информационных системах, находящихся в процессе обработки информации.

Технический контроль состояния защиты информации в автоматизированных системах управления различного назначения осуществляется в полном соответствии со специально разработанными программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством, которому подчиняется объект контроля.

Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что на объекте отсутствуют технические каналы утечки информации.

Контроль состояния защиты информации заключается в проверке соответствия организации и эффективности защиты информации установленным требованиям и нормам в области защиты информации.

Организационный контроль эффективности защиты информации заключается в проверке полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием технических и программно-технических средств контроля.

Средство контроля эффективности защиты информации – техническое, программно-техническое средство, вещество и материал, используемые для контроля эффективности защиты информации.

Технический контроль определяет действенность и надежность принятых мер защиты объектов информатизации от воздействия технических средств разведки.

Технический контроль предназначен для:

а) выявления возможных каналов утечки конфиденциальной информации;

б) проверки соответствия и эффективности принятых мер защиты нормативным требованиям;

в) разработки рекомендаций по совершенствованию принятых защитных мероприятий.

Технический контроль проводится по отдельным физическим полям, создаваемых объектами информатизации, и состоит из:

а) сбора исходных данных, характеризующих уязвимости объекта информатизации по отношению к воздействиям технической разведки;

б) определения возможных типов и средств технической разведки;

в) предварительного расчета зон разведдоступности;

г) определения состава и подготовки к работе контрольно-измерительной аппаратуры;

д) измерения нормируемых технических параметров защищаемого объекта по отдельным физическим полям на границе контролируемой зоны;

е) определения эффективности принятых мер защиты и в отдельных случаях разработки необходимых мер усиления защиты.

Все контролируемые нормативные показатели разделяются на информационные и технические.

Информационные показатели относятся к вероятности обнаружения, распознавания и измерения технических характеристик объектов с заданной точностью.

Техническими показателями эффективности принятых мер защиты являются количественные показатели, характеризующие энергетические, временные, частотные и пространственные характеристики информационных физических полей объекта.

Инструментально-расчетные методы применяются в случаях, когда комплект контрольно-измерительной аппаратуры не позволяет получить сразу конечный результат или не обладает достаточной чувствительностью.

Расчетные методы технического контроля применяются в случае отсутствия необходимой контрольно-измерительной аппаратуры, а также при необходимости оперативного получения предварительных ориентировочных результатов о зонах разведдоступности, например, перед аттестацией объекта.

При проведении технического контроля требуется контрольно-измерительная аппаратура, которая, в большинстве случаев, обеспечивает получение объективных характеристик контролируемых параметров или исходных данных для получения инструментально-расчетных характеристик. Контрольно-измерительная аппаратура по возможности должна быть портативной, что важно для аттестующих организаций, иметь достаточную чувствительность, соответствующую чувствительности аппаратуры разведки, быть надежной в эксплуатации.

Как правило, при проведении контроля расчетно-инструментальным методом проводится большое число измерений на дискретных интервалах и соответственно большое число сложных расчетов, что приводит к быстрой утомляемости оператора. Поэтому современная тенденция развития контрольно-измерительной

аппаратуры заключается в разработке для целей контроля программно-аппаратных комплексов, обеспечивающих полную автоматизацию измерения параметров физических полей и расчета нормируемых показателей защищенности объекта. По результатам контроля состояния и эффективности защиты информации составляется заключение с приложением протоколов контроля.

3. Оценка эффективности технической защиты информации

3.1. Оценка эффективности структурной и пространственной моделей защиты

Первым шагом в построении системы защиты информации является построение структурной модели объекта защиты. Для этого необходимо выбрать элементы информации, подлежащие защите.

Моделирование является основным методом анализа объекта защита, выявления возможных угроз и построения соответствующей системы защиты. Моделирование предусматривает создание модели и ее исследование. Модель объекта защиты представляет собой описание объекта с учетом всех элементов информации, их источников и их месторасположений. В модели учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта.

Моделирование объекта защиты включает в себя:

1) структурирование защищаемой информации

2) разработку пространственной модели защиты.

Структурирование информации производится путем классификации информации в соответствии с функциями, задачами и структурой организации с привязкой элементов информации к ее источникам.

Для каждого элемента информации устанавливаются градации важности защиты защищаемой информации, то есть производится ее категорирование. Для категорирования информации были выбраны следующие уровни:

а) для служебного пользования (ДСП);

б) секретно (С);

в) совершенно секретно (СС).

Для каждого элемента информации устанавливается ценность информации. Ценность определяет величину ущерба, который будет причинен организации при потере или разглашении защищаемой информации. Ценность одного элемента информации определяется долей ущерба при потере или разглашении данного элемента информации от ущерба, нанесенного потерей или разглашением всей защищаемой информации.

Источником информации может выступать физическое лицо, материальный объект или физическое поле. Это могут быть сотрудники организации, бумажные источники и электронные файлы на различных носителях.

Гриф и цена элемента могут быть назначены исходя из принятой шкалы классификации конфиденциальной информации, отраженной в таблице 1. Цена информации Z выражается в условной стоимости единицы информации.

Необходимо учитывать, что информация в бумажном и цифровом виде не должна дублировать друг друга, т.е. учитываться должен только объем уникальной информации. Также необходимо применять для вычисления объем полезной информации, т.е. информации в чистом виде, т.к. иногда небольшое количество информации может занимать значительный объем, что особенного характерно для электронной информации.

Для учета полезной информации вводим «Коэффициент полезности». В среднем данный коэффициент имеет значение 5-15% в зависимости от типа носителя и формы представления. Для расчета таблицы принимаем усредненное значение 10%. Средний объем страницы размера А4 для шрифта 14 составляет 4 кБ, но так как фактически страница никогда не бывает заполнена знаками полностью, то примем средний объем 2,5 кБ.

Таблица 1.

Коэффициенты полезности информации

Категория (гриф) секретности	**Относительная стоимость бита информации, Z_k**	**Требуемая надежность защиты Q(%)**	**Категория защиты**
ОВ	10^4	99,99	Предельно высокий уровень
СС	10^3	99,9	Высокий уровень
С	10^2	99	Достаточный уровень
ДСП	10	90	Допустимый уровень
О	1	37	Низкий уровень

Результаты структурирования защищаемой информации приведены в таблице 2.

Таблица 2.

Структура защищаемой информации

№	**Наименование элемента информации**	**Гриф секретности**	**Ценность информации, кБ (%)**	**Наименование источника информации**	**Место расположения источника информации**

1	Документация на бумажных носителях	СС	1,25 МБ (0,0004%)	Документация в т.ч. правила эксплуатации, схема обслуживания, сертификаты, правила работы, и иная документация относящаяся к отделению ОБИ.	Металлический сейф с разделенными секциями
2	Документация на бумажных носителях	С	3,75 МБ (0,0012%)		
3	Документация на бумажных носителях	ДСП	5 МБ (0,0016%)		
4	Информация хранящаяся в цифровом виде	СС	1024 МБ (6,0%)		
5	Информация хранящаяся в цифровом виде	С	130000 МБ (77,9%)	Документация относящаяся к сведениям составляющим государственную тайну обрабатываемая на ПЭВМ	Жесткие диски ПЭВМ, серверной и хранилище данных общим объемом памяти 4 ТБ
6	Информация хранящаяся в цифровом виде	ДСП	269000 МБ (16,1%)		
7	Общая информация		3,6 ТБ		

Пространственная модель объекта – это модели пространственных зон с указанным месторасположением источников защищаемой информации

Моделирование объекта защиты включает в себя также описание пространственного расположения основных мест размещения источников информации, выявления путей распространения носителей защищаемой информации за пределы контролируемых зон, описание с указанием характеристик

существующих преград на путях распространения носителей с информацией за пределы контролируемых зон. Моделирование проводится на основе пространственной модели контролируемых зон с указанием расположения источников информации.

Моделирование состоит в анализе на основе рассмотренных пространственных моделей, какие могут быть пути распространения информации за пределы контролируемой зоны.

3.2. Оценка информативности технических каналов утечки информации

Технические каналы утечки информации характеризуются показателями, которые позволяют оценить риск утечки. Такими показателями являются:

а) пропускная способность технического канала утечки;

б) длина технического канала утечки информации;

в) относительная информативность технического канала утечки информации.

По аналогии с каналом связи интегральные возможности ТКУИ оцениваются его пропускной способностью. Предельная пропускная способность канала связи в битах в секунду определяется по формуле:

$C = \Delta F \log_2(1+P_c / P_n)$,

где ΔF – ширина полосы пропускания канала связи в Гц;

P_c и P_n - мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Из нее следует, что пропускная способность тем больше, чем шире полоса пропускания частот канала и больше отношение сигнал/шум на входе приемника канала связи.

Любое сообщение в общем случае можно описать с помощью трех основных параметров: динамическим диапазоном D_c , шириной спектра частот F_c и длительностью передачи T_c . Произведение этих трех параметров называется объемом сигнала:

$V=\Delta F_c D_c T_c$,

где $\Delta F_c = F_{max} - F_{min}$;

$D_c = U_{max}/U_{min}$,

а при выражении в децибелах - $D_c = 20\lg(U_{max}/U_{min})$.

В трехмерном пространстве объем сигнала можно представит в виде параллелепипеда.

Для обеспечения неискаженной передачи сообщения объемом V_c, необходимо чтобы характеристики среды распространения и непосредственно приемника соответствовали ширине спектра и динамическому диапазону сигнала.

Так как пропускная способность канала связи зависит от его полосы пропускания и отношения сигнал/шум, то каналы можно разделить на узкополосые и широкополосные, с низкой и высокой энергетикой сигнала.

Наибольшую пропускную способность имеет оптический канал связи, наименьшую – акустический. Радиоэлектронные каналы связи по ширине полосы частот пропускания делятся на узкополосые и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300-3400 Гц и относится к узкополосным, а шириной 8 МГц для передачи телевизионных сигналов – к широкополосным. Если ширина спектра сигнала ΔF_c, содержащего информацию, равна полосе пропускания частот канала $\Delta F_к$, то передача информации происходит в реальном масштабе времени.

Для исключения потери информации на входе канала связи применяется буферное запоминающее устройство, на вход которого поступает с определенной скоростью информация и с которого информация считывается со скоростью, обеспечивающей согласование ширины спектра сигнала с шириной полосы пропускания частот канала. При этом, время передачи увеличивается, т.е. режим реального времени не обеспечивается. Если $\Delta F_к < \Delta F_c$, то спектр сигнала не урезается, но в более широкополосном канале увеличивается уровень помех. В результате этого уменьшается отношение сигнал/помеха, что также приводит к снижению пропускной способности канала связи.

Пропускная способность составного канала (состоящего из нескольких последовательно соединенных простых каналов) оценивается пропускной способностью простого канала, имеющего наименьшие значения. Например,

составной канал наблюдения объектов с космического аппарата включает широкополосный оптический канал «наземный объект – фотоаппарат КА» и менее широкополосный радиоэлектронный канал «сброса» изображения с КА получателю. Для передачи полученного при фотографировании объема видеоинформации изображения на пленке считывается с меньшей скоростью, но в течение более длительного времени. Следовательно, наибольшую пропускную способность имеет оптический канал утечки информации, так как его полоса пропускания существенно выше полосы пропускания любого другого канала. Наименьшей пропускной способностью обладает акустический канал утечки информации.

Другим показателем, который применялся для оценки канала утечки, является его длина. Длина технического канала утечки информации оценивается расстоянием от источника сигнала до его приемника при условии обеспечения при приеме допустимого качества информации. Длина канала зависит от показателей элементов канала передачи информации: энергии сигнала, степени его ослабления в среде распространения, чувствительности и разрешающей способности приемника злоумышленника, уровня помех в канале и др. Чем выше длина канала, тем на большем удалении от источника возможно добывание информации и тем меньше риск злоумышленника. Если длина канала больше расстояния от источника сигнала до границы контролируемой зоны, то риск злоумышленника при добывании информации существенно меньше, так как он может разместить приемник сигнала за пределами контролируемой зоны. Таким образом злоумышленник стремится всеми возможными методами увеличить длину ТКУИ.

Для добывания информации с требуемым качеством необходимо обеспечить на входе приемника минимально допустимое для каждого вида информации и носителя отношение сигнал/помеха. Это отношение достигается на различном удалении от источника сигнала, в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей – электромагнитная волна в длинноволновом диапазоне частот.

Электромагнитная волна из помещения затухает, в основном, в элементах здания. Коэффициенты затухания приведены в таблице 3.

Таблица 3.

Коэффициенты затухания ЭМ волны для типовых помещений

Тип здания	Ослабление радиосигнала в дБ на частоте		
	100 МГц	500 МГц	1 ГГц
Деревянное здание с толщиной стен 20 см	5-7	7-9	9-11
Кирпичное здание с толщиной стен 1,5 кирпича	13-15	15-17	16-19
Железобетонное здание с ячейкой арматуры 15х15 и толщиной 16 см	20-25	18-19	15-17

Уменьшение затухания электромагнитной волны в железобетонных стенах с повышением ее частоты вызвано снижением экранирующего эффекта металлической арматуры железобетона. На частоте 1 ГГц длина волны равна 30 см, соизмеримая с размерами ячеек арматуры.

При ослаблении электромагнитной волны стенами здания 20 дБ дальность ее распространения уменьшается на 1 порядок.

Качественная оценка пропускной способности и длины технических каналов утечки информации указана в таблице 4.

Таблица 4.

Оценка пропускной способности ТКУИ

№ п/п	Вид канала	Показатели простого канала утечки информации	
		Пропускная способность	Длина

1	Оптический	Высокая	В пределах прямой видимости
2	Акустический	Низкая	Малая (единицы- сотни м)
3	Радиоэлектрический	Высокая	Любая (сотни м- тысячи км)
4	Вещественный	Низкая	Любая

Чем более широкую пропускную способность имеет канал утечки, и чем он длиннее, тем большую потенциальную угрозу создает такой канал. Но рассмотренные показатели не учитывают ценность (полезность) передаваемой информации. При наличии канала утечки далеко не вся информация источника, имеющая определенную цену, попадет к злоумышленнику. Часть ее будет утеряна в канале утечки. Следовательно, цена информации, полученной злоумышленником, в общем случае всегда будет меньше цены информации источника. Поэтому важнейшим показателем технического канала утечки информации является его информативность. Следовательно информативность зависит от информативности источника информации. Поэтому корректно говорить не об абсолютной информативности канала утечки, а об относительной информативности. Под относительной информативностью ТКУИ понимается величина в интервале 0-1, соответствующая доли информации источника, которая может быть передана по рассматриваемому каналу.

Если информация объемом $V_c = \Delta F_c D_c T_c$ добывается по каналу утечки информации с частотным диапазоном $\Delta F_к$ и динамическим диапазоном $D_к$ в реалном масштабе времени (т.е. $T_c = T_k$) то информативность такого канала утечки информации будет определяться по формуле:

$$I = \Delta F_k D_k T_k / \Delta F_c D_c T_c = \Delta F_k D_k / \Delta F_c D_c$$

Например, оптический канал наблюдения за объектом разведки в помещении противоположного дома имеет высокую пропускную способность, но количество добываемой с его помощью информации зависит от разрешающей способности оптического приемника. Не вооруженный оптическим прибором наблюдатель может рассмотреть лишь крупные объекты, а с помощью специального телескопа

можно рассмотреть текст документа в руках человека. Так как оптический приемник является элементом технического канала утечки информации, то его разрешающая способность характеризует относительную информативность этого канала.

3.3. Средства инструментальной оценки эффективности технической защиты информации

Мобильный комплекс «Корвет С-СК» применяется при проведении мероприятий по оценке защищенности информации, циркулирующей в технических средствах, а также обсуждаемой в выделенных помещениях, от её утечки по техническим каналам, в том числе на территориально удалённых объектах и защиты информации от утечки по техническим каналам при оперативной подготовке помещений к ведению переговоров, совещаний с обсуждением сведений, содержащих государственную тайну.

Для оценки эффективности мероприятий можно применить входящие в его состав средства:

а) программно-аппаратный комплекс «Аист-СР» для измерения параметров и анализа сигналов звукового диапазона частот в проверяемых устройствах и в токопроводящих коммуникациях; измерения параметров и анализа электромагнитного поля в диапазоне звуковых частот; генерации акустических сигналов различной формы.

Включает в себя:

1) анализатор сигналов «СА86002».

2) источник электропитания ВТСС «ИЭВС».

3) адаптер для подключения к сети 220 В «АПС220».

4) телефонный адаптер «ТЕЛАД».

5) измерительный микрофон «АИСТ-МИК».

6) вибропреобразователь «АР98-100».

7) измерительная магнитная антенна «Сектор».

8) экранированная акустическая система «АС-2».

б) программно-аппаратный комплекс «СПРУТ-СР» для проведения акустических и виброакустических измерений при контроле выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам, утечки за счет низкочастотных наводок на линии связи и токопроводящие элементы ограждающих конструкций зданий и сооружений, а также за счет акустоэлектрических преобразований; измерение параметров звуко- и виброизоляционных свойств конструкций; исследования характеристик и проверки эффективности систем акустического и виброакустического зашумления.

В его состав входят:

1) измерительный шумомер-виброметр-анализатор «Спрут-ШВА».

2) измерительный микрофон «40АЕ.

3) вибропреобразователь «АР98-100».

4) экранированная акустическая система «АС-2».

5) измерительные усилители «ИУС-1» и «ИУС-2».

6) источник электро-питания ВТСС «ИЭВС».

7) модуль источника тестового акустического сигнала

8) модуль радиоканала «Спрут-МРК».

9) ноутбук Lenovo ThinkPad Edge.

в) программно-аппаратный комплекс «Сапфир-СР» для измерения параметров волоконно-оптических систем передачи и оценки защищенности волоконно-оптических линий связи.

Состоит из:

1) оптический рефлектометр «Сапфир-СР-Р».

2) измеритель уровня оптической мощности

3) программируемый оптический аттенюатор «Сапфир-СР-А»

4) оптические переключатели «Сапфир-СР-КО» и

5) волоконно-оптический ответвитель-прищепка

6) малогабаритный источник оптических сигналов

г) программно-аппаратный комплекс «Навигатор-СР» для поиска и измерения побочных электромагнитных излучений и наводок (ПЭМИН), при контроле защищенности объектов информатизации от утечки информации; оценки эффективности средств защиты информации от утечки за счет ПЭМИН; автоматизации измерений и расчетов показателей защищенности информации при проведении специальных исследований.

Состоит из:

1) вспомогательное оборудование «Зонд-СР-3».

2) вспомогательное оборудование «Зонд-СР-12».

3) источник эталонного электропитания «ИЭЭП-СР».

4) вспомогательное электрооборудование «ЭС-300-СР» и «РИС-СР».

5) стол поворотный диэлектрический «СПД-СР».

6) антенная мачта диэлектрическая «АМД-СР».

7) анализатор спектра «FSV13».

8) ПЭВМ.

9) специальное программное обеспечение.

10) активная магнитная антенна «АИР 3-2».

11) дипольная активная широкополосная антенна «АИ 5-0».

12) развязывающие устройство УР 1.6.

13) антенна «ЛПА-2».

14) штатив диэлектрический «ШД-СР».

15) пробник напряжения пассивный однопроводный

4. Разработка рекомендаций по повышению защищенности объектов от утечки информации по техническим каналам

Наибольшую важность, помимо результатов поиска ЭУНПИ, представляют рекомендации по повышению защищенности проверенных помещений и предотвращению утечки и перехвата защищаемой информации по выявленным потенциальным техническим каналам ее утечки. В зависимости от объема и степени детализации, эти рекомендации могут составлять отдельный отчетный документ.

Такие рекомендации обычно включают:

перечень выявленных потенциальных ТКУИ для каждого проверенного помещения;

схемы выявленных потенциальных ТКУИ с краткими пояснениями;

оценку вероятности использования противником потенциальных ТКУИ и существующей на время проверки защищённости каждого помещения от негласного получения информации по выявленным потенциальным ТКУИ;

конкретные рекомендации по мерам и способам предотвращения утечки защищаемой информации по выявленным ТКУИ и повышению защищённости помещений по каждому ТКУИ;

рекомендации по организационным, в том числе, режимным мерам;

рекомендации по изменению элементов конструкции помещений, инженерно-технических коммуникаций и другим инженерным мерам устранения потенциальных ТКУИ;

рекомендации по установке специальных приборов и систем защиты, комплексных систем защиты помещений от утечки информации по техническим каналам, и другим техническим мерам повышения защищённости помещений;

сводный перечень технических средств и систем защиты информации, рекомендуемых к установке на предприятии для повышения защищённости;

предложения по практическому использованию рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации.

Потенциальные ТКУИ отличаются от реальных только своей временной невостребованностью, то есть временным отсутствием в своем составе средств разведки противника. Перечень выявленных потенциальных ТКУИ обычно состоит из естественных каналов. В отличие от искусственно созданных, естественные ТКУИ не обеспечивают комфортных условий приёма перехваченной информации, но существуют постоянно и могут быть использованы противником в любой момент.

Выявление и строгая количественная оценка потенциальных ТКУИ требует специальных измерений и исследований, проводимых по особым методикам и, как правило, не включаемых в число работ по комплексной специальной проверке помещений.

Целесообразно заранее, ещё на этапе подготовительных работ выяснить, нужны ли специальные исследования для получения точных количественных оценок защищённости помещении, или можно ограничиться качественными критериями. В подавляющем большинстве случаев достаточно знать, имеются ли в помещении незакрытые потенциальные технические каналы утечки информации, и может ли выявленный противник воспользоваться этими каналами для перехвата информации.

Приемлемая качественная оценка возможности утечки защищаемой информации через разнообразные потенциальные ТКУИ может быть получена путём анализа сведений о конструктивных особенностях здания и помещений, визуального осмотра проверяемых и соседних с ними помещений и проверки наличия информативных сигналов на «концах» потенциальных ТКУИ, доступных противнику.

Стандартный набор специального оборудования и технических средств, рекомендованный нами для проведения комплексной специальной проверки помещений и объектов указанные ранее, позволяет органам ТЗИ «сработать за противника», имитируя его действия по съёму защищаемой информации с потенциальных ТКУИ. Так, оценить степень слышимости и разборчивости акустических и виброакустических сигналов на границе контролируемой зоны вокруг проверяемых помещений можно с помощью многофункционального

поискового прибора ПИРАНЬЯ. Приборы поиска сигналов в проводных линиях позволяют оценить возможность съёма информации противником за счёт «микрофонного» эффекта и наводок. Комплекс обнаружения радиоизлучающих средств и радионаблюдения Бастион-М даёт возможность сравнить уровни информативных ПЭМИН средств оргтехники с уровнями известных источников излучения. Следует, тем не менее, хорошо понимать, что эти приборы позволяют имитировать средства разведки не слишком изощрённого, технически слабо вооружённого противника, поскольку ориентированы, главным образом, на поиск преднамеренно созданных, «комфортных» ТКУИ. Поэтому для полномасштабных исследований ПЭМИН, звуко- и виброизоляции помещений, акустических и виброакустических сигналов и наводок следует применять специализированные программно-аппаратные комплексы типа НАВИГАТОР П5Г, СПРУТ-11 или им подобную измерительную аппаратуру.

С учётом этих соображений, при отсутствии специальных исследований можно допустить грубую оценку вероятности использования противником потенциальных ТКУИ по субъективной слышимости или регистрации приборами информативных сигналов из проверяемого помещения на границе контролируемой зоны. При такой оценке вероятность использования потенциального ТКУИ можно считать высокой, если информативные сигналы слышны и разборчивы, уверенно регистрируются приборами.

В случае слабой разборчивости информативных сигналов использование противником потенциального ТКУИ приходится считать вполне возможным, поскольку для специалистов не составляет особого труда применить известные способы и средства шумоочистки сигналов.

Следовательно, если сигналы из проверяемого помещения регистрируются поисковой аппаратурой на фоне шумов, но их информативная значимость не ясна, то использование противником потенциального ТКУИ можно считать маловероятным, однако полностью исключить возможность использования противником таких сигналов всё же нельзя. Рекомендуется считать вероятность использования противником такого потенциального ТКУИ малой.

При отсутствии специальных исследований допустима только качественная оценка существующей на время проверки защищённости помещения от негласного перехвата информации по техническим каналам её утечки. Учитывая множественность потенциальных ТКУИ, в оценке защищённости помещения справедлив известный подход к оценке прочности цепи, состоящей из множества

звеньев: её прочность определяется наиболее слабым звеном. В нашем случае «слабость звена» может оцениваться вероятностью использования противником конкретного потенциального ТКУИ. Поэтому помещение можно считать незащищённым от негласного съёма информации в случае, если существует высокая вероятность использования противником хотя бы одного выявленного ТКУИ.

Рекомендации по мерам и способам предотвращения перехвата информации по выявленным ТКУИ следует давать отдельно для каждого помещения и каждого потенциального ТКУИ. В периодических изданиях и специальной литературе достаточно широко освещены возможные способы защиты информации от утечки по техническим каналам. Их перечисление и оценка не входят в число поставленных при написании данной работы задач. Во многих случаях наиболее эффективным и дешёвым способом перекрытия технических каналов утечки информации может стать применение активных систем зашумления. В качестве примеров таких систем можно назвать комплекс виброакустической защиты БАРОН, устройства активной защиты информации САЗ, генераторы шума ГРОМ-ЗИ.

Меры защиты должны быть адекватны степени угроз, в противном случае все ресурсы организации могут целиком уйти на создание системы защиты информации.

Следует учитывать, что утечка информации может проходить не только по техническим каналам. Поэтому в рекомендациях по установке технических средств и систем не следует забывать о средствах скрытого наблюдения, регистрации действий посетителей и персонала, системах сигнализации, блокировки и т.п. Системы гласного, осуществляемого с ведома и согласия персонала видеоконтроля, акустического мониторинга помещении, регистрации телефонных переговоров во многих случаях оказываются более действенными для предотвращения утечки информации, чем физическая охрана контролируемой зоны или, к примеру, применение аппаратуры защиты от перехвата информативных наводок.

За рекомендациями по способам и средствам предотвращения утечки информации по выявленным ТКУИ целесообразно разместить сводный перечень технических средств и систем защиты информации, рекомендуемых к установке на предприятии. Хорошо, если в перечне будет указан, помимо основного варианта, один или два аналога рекомендуемого средства защиты, тем более что сегодня на рынке предлагается достаточно большое количество примерно однотипных

средств. Не следует забывать о включении в перечень средств и систем контроля за работоспособностью и эффективностью рекомендованной техники защиты информации. Документ завершается предложениями по практическому использованию средств и систем защиты информации, рекомендуемых к установке на предприятии, и объединению или внедрению рекомендуемых технических средств и систем в единую комплексную систему защиты информации на предприятии. В предложениях по практическому использованию средств и систем защиты указать, в каком временном режиме целесообразно использовать средства защиты, кем должно приниматься решение на их применение, комплексно или по отдельности их лучше применять, как контролировать их работоспособность и эффективность, целесообразно ли вводить централизованное управление работой средств защиты и контроля.

Следует иметь в виду, что интеграция отдельных средств и систем защиты информации в единую комплексную систему, как правило, даёт заметный выигрыш в качестве защиты информации. Повышение эффективности защиты информации происходит, главным образом, за счет централизованного управления ресурсами системы, повышения качества контроля за работой составляющих её технических средств, возможности быстрого реагирования на возникновение новых угроз утечки информации.

Первой ступенью интеграции может быть создание условий для оперативного контроля занятости, работоспособности технических средств защиты информации и контроля, их быстрой замены или перенацеливания. Это может быть сделано, например, путём сведения этих средств в специально выделенное помещение и оборудования в нём поста контроля защиты информации. Современные средства и системы защиты информации, обеспечивающие возможность дистанционного управления их работой, контроля их эффективности, позволяющие одновременно контролировать сразу несколько помещений, существенно облегчают решение этой задачи.

Последующие ступени интеграции предусматривают обеспечение конструктивной, информационной, программной и эксплуатационной совместимости технических средств защиты информации и контроля. Одним из примеров интеграции различных средств и систем защиты помещения от утечки акустической информации может служить разработанный НПЦ Фирма «НЕЛК» комплекс защиты речевой информации КЗРИ-1, базовый вариант которого включает систему защиты телефонных линий «Прокруст-2000», систему виброакустического зашумления «Барон» и подавитель радиоэлектронных устройств негласной аудиозаписи

«Шторм».

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы выполнен анализ предметной области, с точки зрения оценки эффективности мероприятий технической защиты информации объекта ТСПИ. При этом показано, что объективной характеристикой качества СЗИ – степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов, может служить только вероятность достижения цели операции, выполнения задачи системой или иное.

Обоснована возможность получения необходимых данных для оценки эффективности мероприятий по повышению информационной безопасности объекта с помощью имитационного моделирования. Предложена методика расчета для оценки результата от воздействия проведенных мероприятий по технической защите, представленная на типовом объекте. В данной работе были обобщены и собраны в единое основные рекомендации должностным лицам органов технической защиты информации по повышению защищенности объектов ТСПИ от утечки информации по техническим каналам.

Список литературы

1. Зайцев, А.П. Технические средства и методы защиты информации [Текст]: учебник для вузов / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов – М.: Горячая линия - Телеком, 2014.
2. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам [Текст]: справочное издание /Г.А. Бузов – М.: Горячая линия – Телеком, 2014, – 586 с.
3. Кондратьев А. В. Организация и содержание работ по выявлению и оценке основных видов технического канала утечки информации, защита информации от утечки [Текст]: справочное пособие – М.: Маском, 2011.
4. Специальные требования и рекомендации по защите информации, обрабатываемой техническими средствами передачи и обработки информации в Вооруженных Силах Российской Федерации [Текст]: утверждены приказом Министра обороны Российской Федерации 1996 г. № 020.

5. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам [Текст]: утвержденной ГТК при Президенте РФ от 1997 г. № 055.
6. Модель иностранных технических разведок на период до 2020 г (модель ИТР-2020) [Текст], 2010 г.