МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.02 –	Информационная безопасность телекоммуникационных систем
Специализация -	Разработка защищенных телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПОДВИЖНАЯ ИСПЫТАТЕЛЬНАЯ ЛАБОРАТОРИЯ СПЕЦИАЛЬНЫХ ПРОВЕРОК

Студент ____ Маслюк Константин Владиславович

Руководитель _____ Безяев Д.Ю.

Нормоконтролер _____ Иванов А.П.

Рецензент ведущий инженер АО «Рубин» _____ Будникова М.В.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой _____(протокол заседания ГЭК от _____ № ____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2017

РЕФЕРАТ

Пояснительная записка содержит 107 с., 28 рис., 9 табл., 26 источников.

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, СПЕЦИАЛЬНЫЕ ПРОВЕРКИ, ПОДВИЖНАЯ ИСПЫТАТЕЛЬНАЯ ЛАБОРАТОРИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ.

Предметом проектирования является подвижная испытательная лаборатория, предназначенная для проведения специальных проверок.

Целью выпускной квалификационной работы является разработка подвижной испытательной лаборатории проведения специальных проверок.

В процессе проектирования были проанализированы и описаны стандарты и нормативно-методические документы, на которые опирается подвижная испытательная лаборатория в своей деятельности, изучены основные методики обнаружения и выявления технических каналов утечки информации, проанализированы специальные требования и рекомендации по технической защите информации. В ходе проектирования была разработана и описана структура подвижной испытательной лаборатории, выбрано оборудование, используемое подвижной испытательной лабораторией для осуществления своей деятельности, а также разработана и описана схема его питания. Были разработаны методические рекомендации оператору, а также методические рекомендации по проведению специальной проверки с использованием подвижной испытательной лаборатории.

В результате проектирования была разработана подвижная испытательная лаборатория, предназначенная для проведения специальных проверок.

СОДЕРЖАНИЕ

Введение 6

1 Теоретические аспекты защиты информации 9

1.1 Анализ актуальных основных угроз и рисков информационной безопасности 9

1.2 Технические каналы утечки информации 20

1.3 Описание особенностей каналов утечки информации 26

1.3.1 Возможные каналы утечки 26

1.3.2 Побочные электромагнитные излучения элементов ТСПИ 28

1.3.3 Электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ и ВТСС 28

1.3.4 Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ 28

1.3.5 Электрические каналы утечки информации 29

1.3.6 Параметрический канал утечки информации 31

1.3.7 Классификация и характеристика технических каналов утечки акустической (речевой) информации 32

2 Выбор методов и средств защиты информации и их классификация. 35

2.1 Методы и средства поиска утечки информации по техническим каналам 35

2.2 Технические устройства иностранного производства, применяемые для негласного съема информации 42

2.3 Пространственное электромагнитное зашумление 44

2.4 Заземление технических средств 44

2.5 Экранирование 45

2.6 Цифровые методы защиты информации от ПЭМИН 46

2.7 Выбор оборудования и анализ существующей современной аппаратуры, необходимой для поиска ЭУНПИ, и для использования в лаборатории 50

2.8 Анализ современных схемотехнических и конструктивно-технических принципов построения технических средств иностранного производства 69
3 Проектирование подвижной испытательной лаборатории 72
3.1 Требования к стенду рентгенографического неразрушающего контроля 72
3.2 Методика выявления устройств негласного съема информации..... 78
3.3 Описание выбранного автомобиля и размещение оборудования.... 90
3.4 Рекомендации к рабочему месту оператора..... 94
3.5 Программа проведения специальной проверки..... 96
Заключение 101
Список использованных источников 103

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

НСД – несанкционированный доступ;

ПЭМИ – побочные электромагнитные излучения;

ПЭМИН – побочные электромагнитные излучения и наводки;

ПО – программное обеспечение;

ОТСС – основное техническое средство и система;

ВТСС – вспомогательное техническое средство и система;

ТС – техническое средство;

СЗИ – средство защиты информации;

ЗУ – закладное устройство;

ТСИП – техническое средство иностранного производства;

ЭВМ – электронно-вычислительная машина:

ПЭВМ – персональный ЭВМ (компьютер);

ТСР – технические средства разведки;

СТС – специальные технические средства;

НСД – несанкционированный доступ;

СБ – служба безопасности;

ТСПИ – технические средства передачи информации;

СПО(ПО) – специализированное программное обеспечение;

СП – специальная проверка;

ЭУНПИ – электронное устройство негласного получения информации;

РМ – радио микрофоны;

ТРП – телефонные радиопередатчики;

ВВЕДЕНИЕ

В современном мире в условиях информатизации и быстрого роста возможностей технических средств в сфере радиоэлектроники, предоставляется возможность получения доступа к закрытой информации, через широкий спектр радиоустройств.

По статистике основной объем данных добывается путем внедрения средств негласного съема информации, которые могут быть в виде, как технических модулей, так и закамуфлированные под технические элементы устройства, элементы одежды, бытовые предметы. Передача перехватываемой информации таких устройств может осуществляться [1]:

- с одновременной передачей перехватываемой информации;
- с накоплением перехватываемой информации;
- с передачей перехватываемой информации по команде;
- время и место внедрения закладных устройств [1], [2];
- строительство и реконструкции объекта. Строительство или реконструкция объекта имеет свободный и неконтролируемый доступ в помещение, его системам освещения, сигнализации, связи. В этот период могут быть установлены довольно сложные устройства, в том числе с дистанционным управлением;
- ежедневная деятельность предприятия, когда доступ в помещение не контролируется. Закладки могут быть установлены в интерьерах помещений, предметах повседневного обихода при проведении профилактических работ на системах электропитания, связи и сигнализации, а также уборке помещений. Например, установка сетевой закладки вместо обычной розетки, замена обычного удлинителя подобным;
- повседневная деятельность предприятия, когда доступ в помещение контролируется, но в нем в течение короткого времени могут находиться посетители. В этом случае наиболее целесообразно установление закладок непосредственно в интерьерах помещения, например, под креслом

или столом, или использование закладок, закамуфлированных под ручку. Кроме того, закладки могут быть установлены путем замены предметов, на оборудованные закладками.

- повседневная деятельность предприятия, когда доступ в помещение невозможен, но не исключен доступ в соседние помещения. В этом случае для доступа к информации целесообразно использовать радиостетоскопы, которые позволяют осуществлять получение интересующей информации путем съема акустических сигналов со стен помещения, внешних оконных стекол, труб систем отопления и водоснабжения.

Технические средства радиомониторинга окружающей среды используются для проведения организационно-технических мероприятий по наблюдению за радиоэфиром, целями которого являются [3], [4]:

- поиск источников радиоизлучений, в том числе закладных устройств;
- местоопределение этих источников;
- установление их технических параметров;
- выделение передаваемой информации;
- определение допустимости работы на отмеченных частотах или в отмеченных режимах и т.д.

Если грамотно и своевременно найти комплексный подход к организации обеспечения информационной безопасности, можно выявить источник излучения, используя различные технические средства:

- детекторы излучений;
- частотомеры;
- частотомеры с расширенными функциями поиска;
- сканирующие (коммутационные) приемники;
- автоматизированные комплексы сканирования, радиомониторинга и обнаружения источников электромагнитных излучений.

Актуальность темы исследования. Быстрые темпы развития человечества на фоне благополучия развитых стран и деклараций о необходимости защиты ценностей общества характеризуются обострением конкуренции между странами, организациями и отдельными членами общества за конкурентоспособное место на рынке, качество жизни.

В условиях глобализации, интеграции и интернационализации экономики информация становятся главным фактором конкурентоспособности. Поскольку получение информации путем проведения собственных исследований являются достаточно дорогостоящим, в этой связи расширяется сфера добывания информации, что является более дешевым, хотя является незаконным. Данному обстоятельству способствуют недостатки правовой базы по защите интеллектуальной собственности, которые позволяют злоумышленникам избегать юридической ответственности за свои противоправные действия. Также данного рода действиям способствует наличие на рынке различных технических средств по нелегальному добыванию информации. В связи с данными обстоятельствами, возрастает актуальность защиты конфиденциальной информации во всех сферах деятельности государства, организаций и личной жизни населения. Постоянное соперничество методами и реализующих их средствами добывания и защиты информационных ресурсов привело к возникновению на рынке различных устройств защиты информации. Но стоит отметить, что это появление не решает проблемы утечки информации, поскольку возникла следующая проблема – проблема рационального выбора и применения данных устройств для защиты конкретной информации в конкретных условиях места и времени.

Целью работы является проектирование подвижной испытательной лаборатории специальных проверок, предназначенной для поиска устройств негласного съема информации. Лаборатория должна быть оснащена оборудованием, позволяющим обнаружить работу таких устройств, проверить эффективность деятельности предлагаемых средств для

повышения уровня защищенности специальных помещений, должна иметь автомобильную базу и источник резервного питания.

1 Теоретические аспекты защиты информации

1.1 Анализ актуальных основных угроз и рисков информационной безопасности

В общем случае под угрозой для системы защиты информации или объекта понимается потенциально возможное действие или событие, реализация которого может принести ущерб интересам защищаемого объекта или его владельцу. Определение списка возможных угроз защиты информации составляется с целью формирования полного описания требований по защите информации к формируемой системе защиты. Также перечень угроз для объекта с указанием вероятности их реализации необходимы для анализа возможных рисков для защищаемой системы и формулировки требований к используемым методам и способам защиты информации к системе обеспечения информационной безопасности автоматизированной системы. Данный список должен быть составлен с учетом классификации угроз и уязвимостей, а также рисков по ряду признаков. Каждый из таких признаков может отражать одно из выделенных требований к системам защиты информации. При этом для каждого признака могут быть детализированы относящиеся к нему угрозы.

Классификация всех возможных угроз информационной безопасности АС представлена на рисунке 1.1. В зависимости от рассматриваемой предметной области в каждом конкретном случае классификация может быть дополнена. Рассмотрим классификацию угроз информационной безопасности по базовым признакам [7]:

- по природе возникновения;
- по степени преднамеренности проявления;
- по непосредственному источнику угроз;
- по положению источника угроз;
- по степени зависимости от активности АС;

- по степени воздействия на АС;
- по способу доступа к ресурсам АС;
- по текущему месту расположения информации, хранимой и обрабатываемой в АС.

Рисунок 1.1 – Классификация угроз информационной безопасности

Независимо от определения конкретного вида или класса угроз система защиты информации должна удовлетворять требованиям тех лиц, которые ее эксплуатируют, а также должна обеспечивать общие свойства информации и систем ее обработки [8].

Исследование угроз безопасности информации [1], [4] позволило классифицировать уязвимости компонентов распределенной вычислительной системы, наиболее подверженных атакам, как показано на рисунке 1.2.

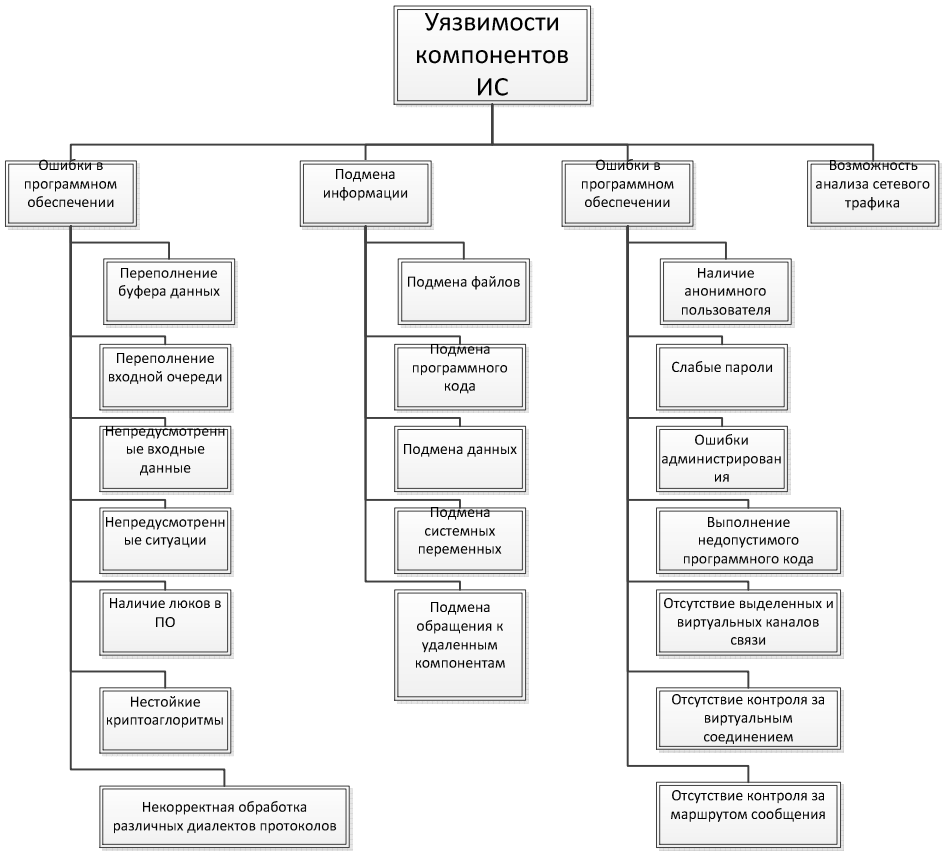

Рисунок 1.2 – Классификация уязвимостей компонентов информационных систем

Для создания защищенной информационной системы необходимо определить, на каком из этапов возможно проявление того или иного изъяна защиты, то есть источника появления той или иной уязвимости.

На рисунке 1.3 [4] приведено сопоставление уязвимостей компонентов вычислительной системы и ошибок, допущенных на различных этапах ее создания. Анализ уязвимостей компонентов распределенной вычислительной системы и методов защиты позволил сделать следующие выводы [14]:

– источники появления изъянов защиты в основном связаны с неправильным применением и внедрением моделей безопасности, целостности и работоспособности;

– большое количество атак связано с нарушением конфиденциальности информации.

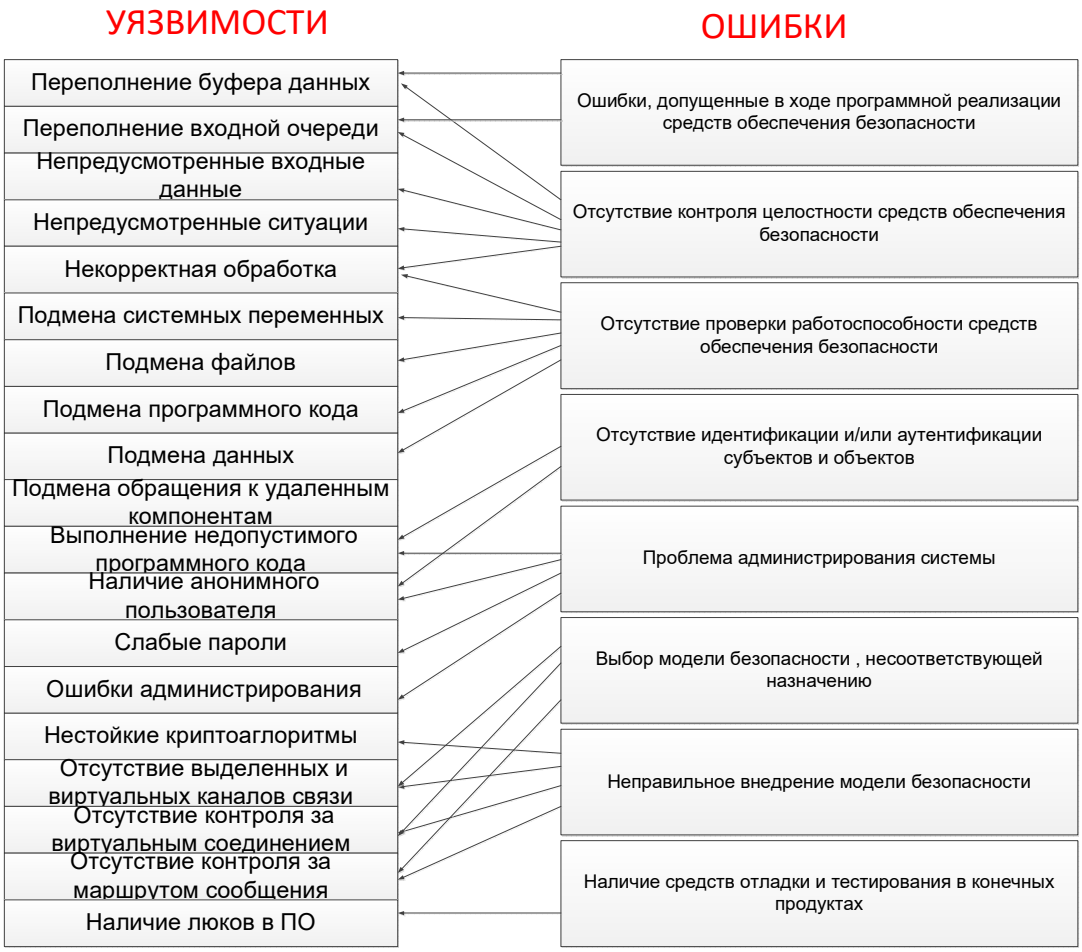

Рисунок 1.3 – Сопоставление уязвимостей компонентов вычислительной системы и ошибок, допущенных на различных этапах ее создания

Нарушение безопасности системы связано не только с операциями чтения и записи, но и с операциями создания объектов на удаленных компонентах распределенной вычислительной системы, удаления компонентов распределенной вычислительной системы и выполнения удаленного программного кода [12]. Большое число разнообразных атак связано с удаленным выполнением программного кода. Модель распределенной вычислительной системы должна быть симметричной, так как сетевой трафик является двунаправленным. Наиболее уязвимым объектом распределенной вычислительной системы являются информационные блоки (буферы).

На основании проведенного компанией InfoWatch исследования утечек можно выделить следующие наиболее актуальные каналы утечки информации [10].

На рисунке 1.4 представлено, что за 1 полугодие 2016 года аналитическим центром InfoWatch зарегистрировано 840 случаев утечки конфиденциальной информации. Это на 16% больше, чем за аналогичный период 2015 года (723 утечки) [41].

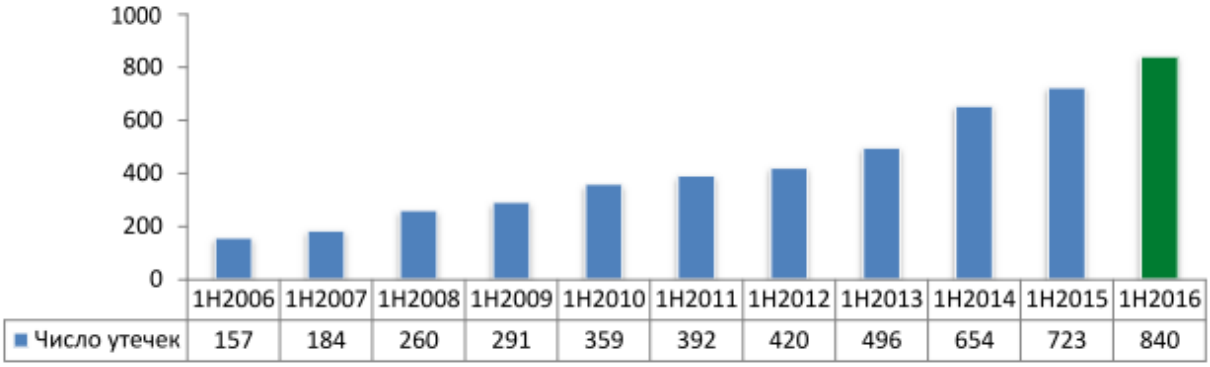

Рисунок 1.4 – Число зарегистрированных утечек информации, 1 полугодие 2006 года – 1 полугодие 2016 года

В результате утечек скомпрометировано 1,06 миллионов персональных данных (записей ПДН и платежных данных) – номера социального страхования, реквизиты пластиковых карт, иная критически важная информация. Для сравнения – за весь 2015 год скомпрометированы 965,9 миллионов записей.

На рисунке 1.7 показано, что зарегистрировано 506 (67%) утечек информации, причиной которых стал внутренний нарушитель. В 250 (33%) случаях утечка информации произошла из-за внешнего воздействия.

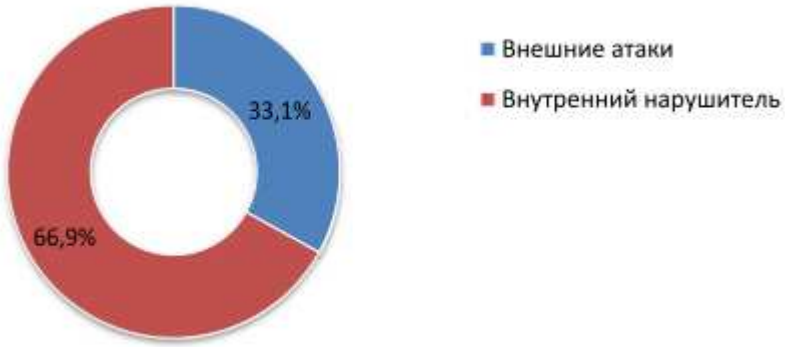

Рисунок 1.5 – Распределение утечек по вектору воздействия, 1 полугодие 2016 года

По сравнению с 1 полугодием 2015 года, изменений в распределении утечек по вектору не наблюдается. Ранее на протяжении нескольких лет отмечалось постепенное увеличение доли утечек под воздействием внешних атак. Таким образом, сделанный нами ранее прогноз на долгосрочный рост доли утечек под воздействием внешнего злоумышленника (с соответствующим сокращением доли утечек, спровоцированных злонамеренными или неосторожными действиями внутреннего нарушителя) не оправдался. Это, впрочем, не отменяет вывода исследований предыдущих лет о том, что «внешние утечки» по своей природе более разрушительны, чем утечки данных, спровоцированные внутренним нарушителем.

В 1 полугодии 2015 года в результате внешнего воздействия скомпрометировано 603 миллиона персональных данных (2,41 миллиона на утечку). Итогом воздействия внутреннего нарушителя стала компрометация 406 миллионов записей (0,80 миллионов на утечку).

Внешние атаки спровоцировали 16 из 23 зафиксированных «мега-утечек». На «мега-утечки» приходится 982 миллиона записей о персональных данных, скомпрометированных в результате утечек в I полугодии 2016 года (92% от общего числа).

Распределение утечек по виновнику за год практически не изменилось. Доля утечек под воздействием внешнего злоумышленника снизилась на 4% и составила 30%. В 67% случаев виновниками утечек информации были

настоящие или бывшие сотрудники – 66% и 1% соответственно. Менее чем в 1% случаев зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов). Доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, составила 2%, что представлено на рисунке 1.6

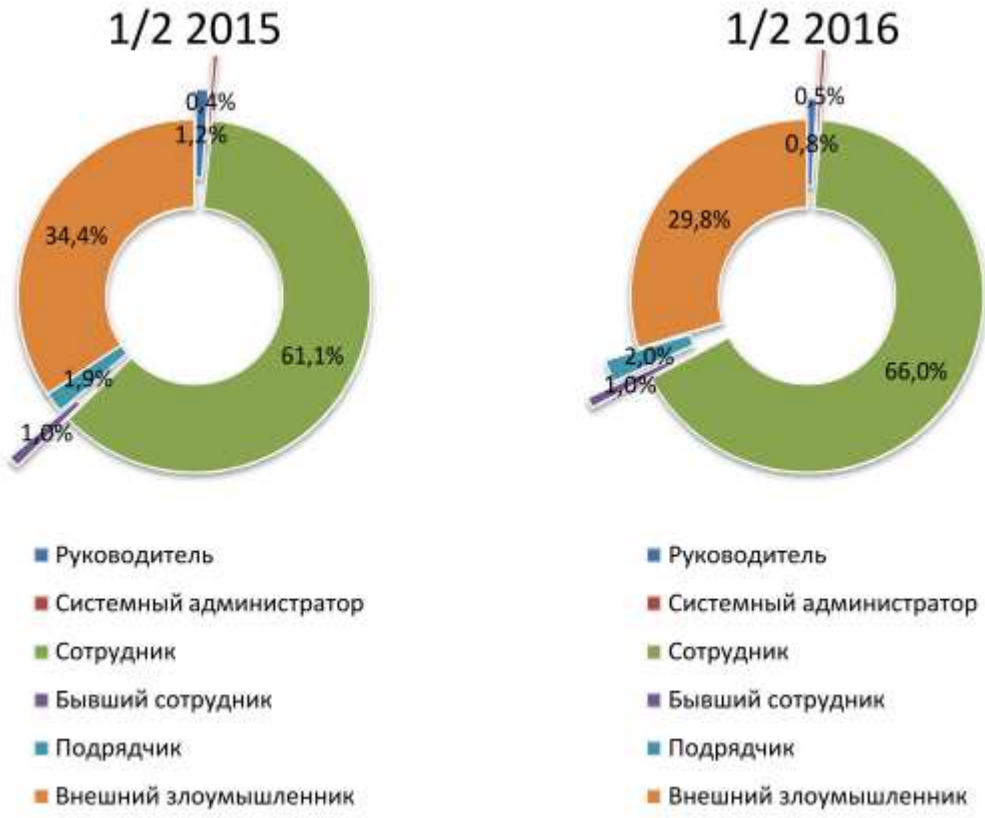

Рисунок 1.6 – Распределение утечек по источнику (виновнику), 1 полугодие 2015 года – 1 полугодие 2016 года

Совокупная доля утечек персональных и платежных данных выросла на 4% и составила 94%. При этом на персональные данные пришлось 88% утечек. В 6% случаев утекала платежная информация. Как правило, при утечке платежной информации речь идет о компрометации реквизитов платежных карт.

Причем за последние полгода возросло число утечек платежной информации, в ходе которых скомпрометировано свыше миллиона записей.

По сравнению с 1 полугодием 2015 года, наблюдается незначительное уменьшение долей утечек информации, составляющей государственную и коммерческую тайну, что показано на рисунке 1.7.

Рисунок 1.7 – Распределение утечек по типам данных, 1 полугодие 2015 года – 1 полугодие 2016 года

Огромный объем скомпрометированных персональных данных и платежной информации, высокая доля утечек этих типов данных свидетельствует о растущей год от года ценности личной информации в цифровом виде. Причем, это касается не только персональных данных отдельных граждан, но и сведений о физических лицах – представителях организаций-контрагентов, которые (сведения) аккумулированы в клиентских базах коммерческих компаний.

В 2016 году доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества снизилась и составила 8%. Доля утечек данных, сопряженных с неправомерным доступом к информации (злоупотребление правами доступа, внутренний шпионаж), составила 11%, что представлено на рисунке 1.8.

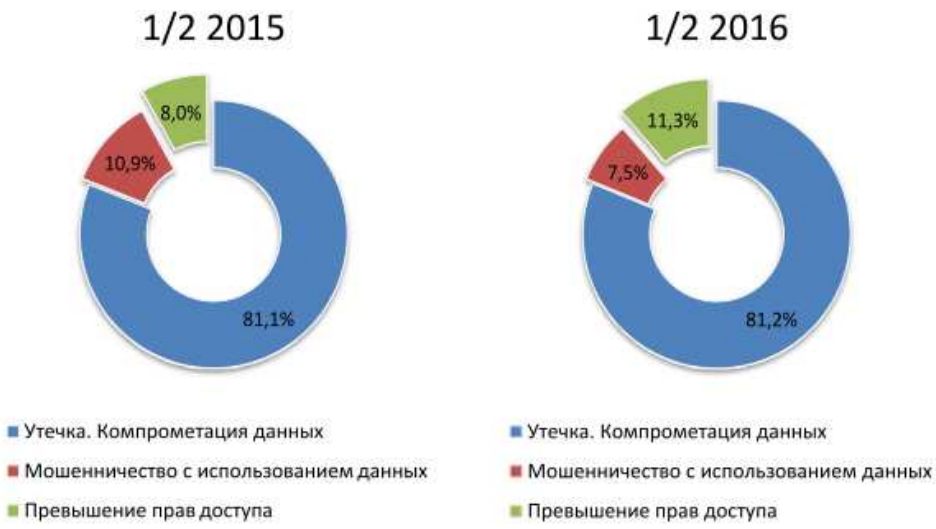

Рисунок 1.8 – Распределение утечек по характеру, 1 полугодие 2015 года – 1 полугодие 2016 года

81% инцидентов, сопряженных с потерей контроля над информацией, относится к типу «классических» утечек, не сопряженных с дополнительными нарушениями – нет превышения прав доступа, нет использования в целях мошенничества. На диаграмме мы их обозначили как утечки, приведшие к компрометации данных.

Невозможно однозначно сказать, в каком случае последствия для владельца данных (коммерческой компании, государственного органа) будут более разрушительными.

Не очевидно, что обычный хакер, которому посчастливится пробраться внутрь защищенного периметра, натворит меньших бед, чем профессиональный мошенник.

Распределение случайных и умышленных утечек в 1 полугодии 2016 года и за аналогичный период 2015 года представлено ниже. На рисунке 1.9 показан незначительный рост доли умышленных утечек по отношению к случайным.

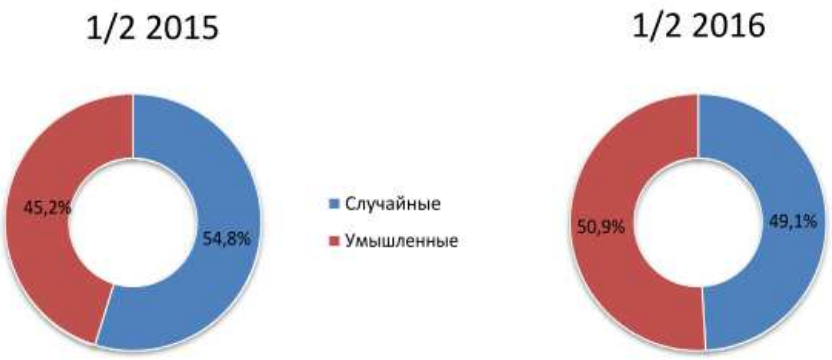

Рисунок 1.9 – Соотношение случайных и умышленных утечек, 1 полугодие 2015 года – 1 полугодие 2016 года

На протяжении нескольких лет наблюдается относительная стабильность картины утечек. Существенными изменениями в пределах исследуемого периода можно считать увеличение объема скомпрометированных записей в расчете на утечку в 3,5 раза, трехкратный рост числа «мега»-утечек (с 8 до 23) по сравнению с 1 полугодием 2015 года, рост доли утечек персональных данных.

В 1 полугодии 2016 года продолжилось увеличение доли утечек по таким каналам, как съемные носители, электронная почта. Снизились доли утечек данных в результате кражи/потери оборудования, через сеть, бумажные документы. Почти на 1% возросла доля утечек по голосовому каналу, что представлено на рисунке 1.10.

Рисунок 1.10 – Распределение утечек по каналам, 1 полугодие 2015 года – 1 полугодие 2016 года

При этом распределения умышленных и случайных утечек по каналам впервые за все время наблюдений не имеют драматических отличий (за исключением «электронной почты»). Например, доля умышленных утечек через бумажные документы отличается от доли случайных по тому же каналу лишь на 6 п. п., что отражено на рисунке 1.11.

Рисунок 1.11 – Распределение утечек по каналам, 1 полугодие 2016 года

Для сравнения – по данным 1 полугодия 2015 года на бумажные документы пришлось всего 2% умышленных утечек при 23% случайных утечек по тому же каналу.

Сопоставимо меньшие доли умышленных утечек (по сравнению со случайными) зафиксированы по таким каналам, как съемные носители, электронная почта, бумажная документация. Именно эти каналы исторически наиболее чувствительны к применению технических средств защиты данных. Не секрет, что изначально системы предотвращения утечек контролировали как раз электронную почту, бумажные документы, копирование данных на флеш-накопителе.

Увеличение доли случайных утечек свидетельствует о возрастающей эффективности таких решений, все большем проникновении систем защиты информации, благодаря которым и удается в итоге эти утечки обнаружить.

С другой стороны, внутренние злоумышленники все меньше используют эти каналы для совершения противоправных действий. «Продвинутый» нарушитель осведомлен, что современные средства контроля позволяют успешно перехватывать передачу конфиденциальной информации практически по всем перечисленным каналам, и не рискует понапрасну.

1.2 Технические каналы утечки информации

К одной из основных угроз безопасности информации ограниченного доступа относится утечка информации по техническим каналам, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации [8].

Совокупность источника информативного сигнала (в данном случае СВТ), технического средства, осуществляющего перехват информации, и физической среды, в которой распространяется информативный сигнал, называется техническим каналом утечки информации, он представлен на рисунке 1.12.

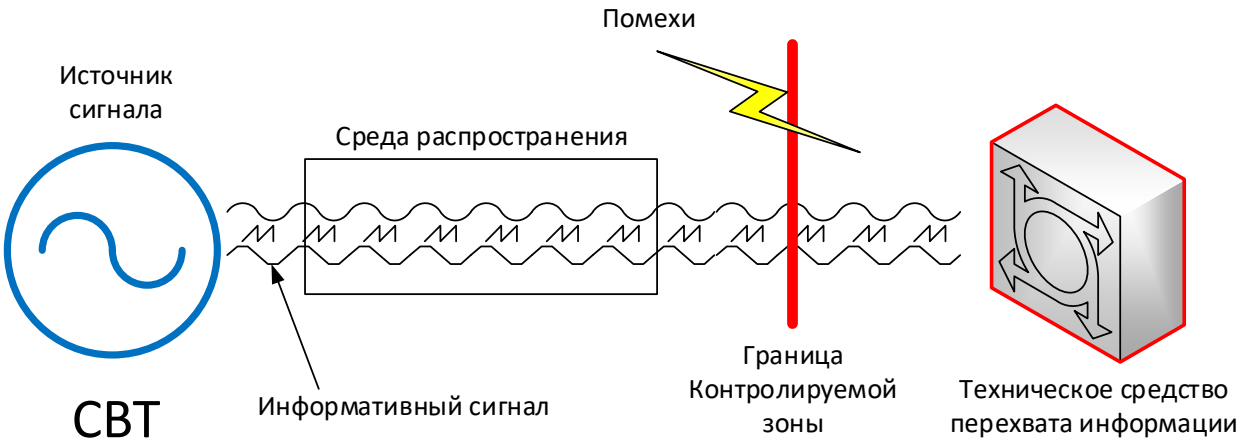

Рисунок 1.12 – Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники

Иностранные разведки для перехвата информации используют технические средства разведки (ТСР). Для перехвата информации,

обрабатываемой СВТ, используются технические средства разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).

Другие заинтересованные субъекты (юридические лица, группы физических лиц, отдельные физические лица) для перехвата информации используют специальные технические средства (СТС), приспособленные или доработанные для негласного получения информации.

В зависимости от природы образования информативного сигнала технические каналы утечки информации можно разделить на естественные и специально создаваемые. Это показано на рисунке 1.13.

Рисунок 1.13 – Классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники (СВТ)

Естественные каналы утечки данных появляются за счет сторонних электромагнитных излучений, возникающих при использовании данных СВТ (электромагнитные каналы утечки данных), а также в результате наводок различных передаваемых сигналов в линиях питания СВТ, соединительных линиях ВТСС и других проводниках (электрические каналы утечки данных).

Специально создаваемыми каналами утечки данных можно назвать каналы, создаваемые путем использования в СВТ электронных средств для перехвата данных – закладных устройств, и методом «высокочастотного облучения» СВТ.

Стандартный комплекс разведки ПЭМИ состоит из: специальное приемное устройство, ПЭВМ (или монитор), профессиональное ПО и широкодиапазонную направленную антенну.

Средства разведки ПЭМИ могут работать в близлежащих зданиях или машинах, которые находятся за пределами контролируемой зоны объекта, как представлено на рисунке 1.14.

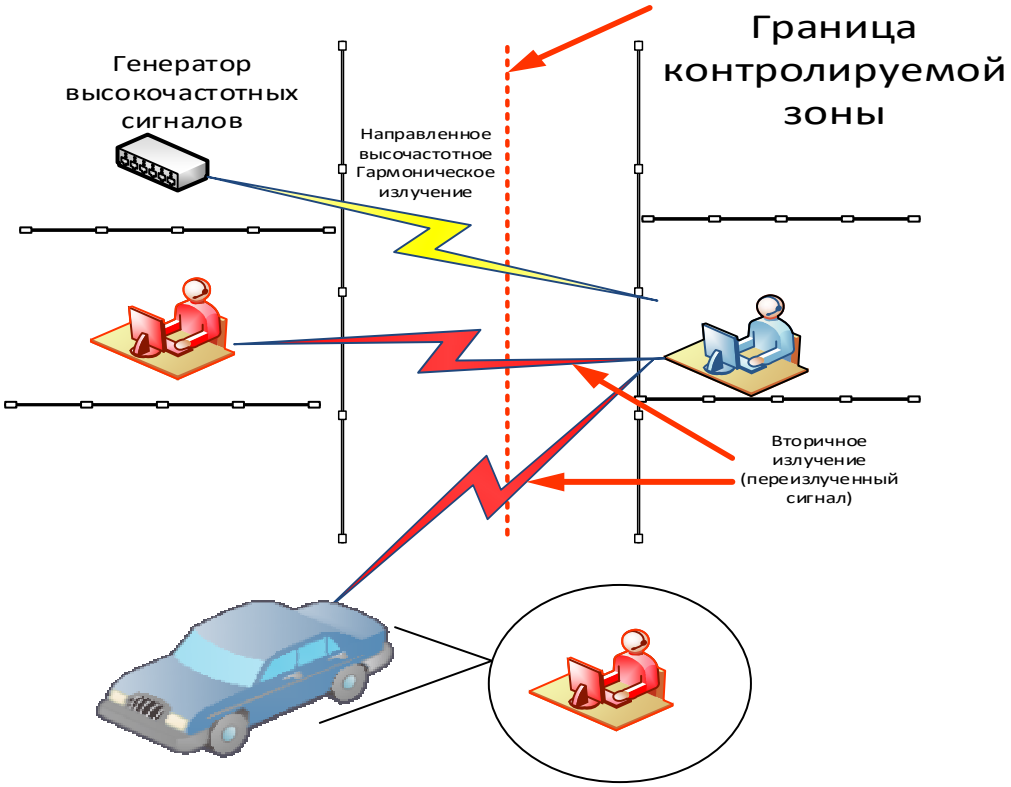

Рисунок 1.14 – Перехват побочных электромагнитных излучений (ПЭМП) средств вычислительной техники (СВТ) техническими средствами разведки побочных электромагнитных излучений (ТСР ПЭМПН)

Наиболее опасным (с точки зрения утечки информации) режимом работы СВТ является вывод информации на экран монитора. Учитывая широкий спектр ПЭМИ видеосистемы СВТ и их незначительный уровень,

перехват изображений, выводимых на экран монитора ПЭВМ, является довольно трудной задачей.

Дальность перехвата ПЭМИ современных СВТ, как правило, не превышает 30-50 метров. Качество перехваченного изображения значительно хуже качества изображения, выводимого на экран монитора ПЭВМ.

Особенно трудная задача – перехват текста, выводимого на экран монитора и написанного мелким шрифтом.

Возможные каналы утечки информации представлены на рисунке 1.15 [2].

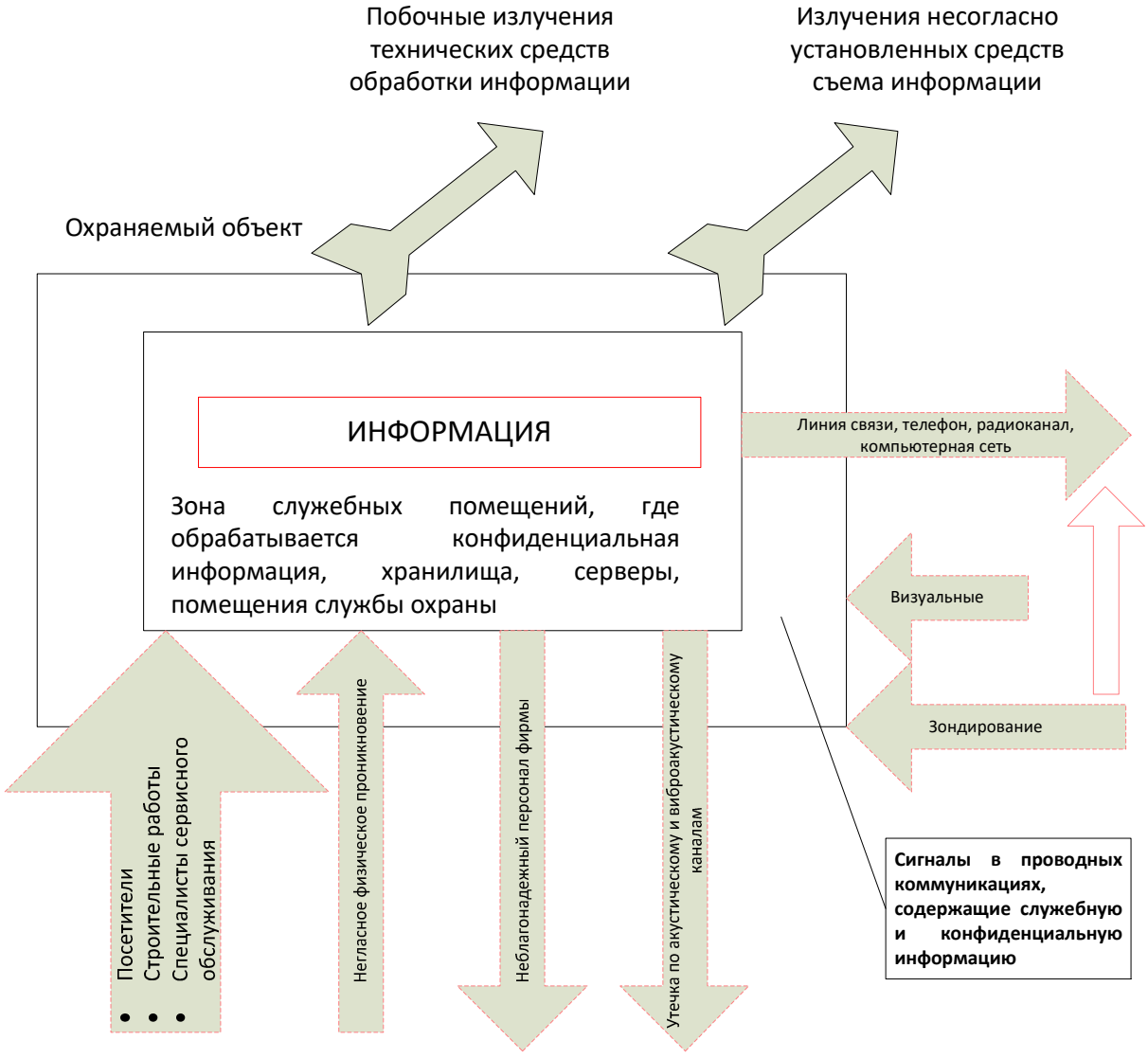

Рисунок 1.15 – Возможные каналы утечки информации

Рассмотрим следующие технические каналы утечки информации, которые существуют на объекте информатизации:

- акустический;
- виброакустический;
- электромагнитный;
- проводной;
- оптико-электронный.

Следует отметить, что приведенная классификация связана с конкретным классом аппаратуры защиты информации и поиском технических средств промышленного шпионажа. Делается это для лучшего понимания угрозы утечки информации. Охарактеризуем каждый из каналов.

Акустический канал – это канал воздушной проводимости звуковых колебаний в диапазоне слухового восприятия человека от 20 Гц до 20 кГц, но обычно он значительно уже и зависит от особенностей человеческой речи. Таким каналом может быть и открытое летом окно, и воздуховод системы вентиляции и кондиционирования, а также различные технологические отверстия, проделанные во время строительства и реконструкции здания.

Из практики работы известно, что конфиденциальные разговоры, ведущиеся в кабинете, оснащенном системой вентиляции, слышны в другом помещении за несколько метров от него и для их подслушивания нет необходимости внедрять специальные микрофоны в указанный кабинет. Наиболее простым выходом из создавшегося положения является установка специальных акустических фильтров.

Кроме того, перехват информации такого рода осуществляется с помощью микрофонов, скрыто установленных в ограждающих конструкциях помещения, различном оборудовании и предметах обихода, размещенных в нем.

Микрофоны подслушивания могут быть установлены во время строительства, ремонта или реконструкции помещений. Наибольшую опасность представляют элементы и узлы, поступающие в готовом виде, мебель и оборудование, изготовленные на заказ, а также всевозможные подарки и сувениры.

Существует опасность съема акустической информации с помощью направленных микрофонов. Вести конфиденциальные переговоры при открытых окнах, особенно если они выходят в сторону неконтролируемой территории, не следует. Переговоры необходимо проводить в специально отведенных помещениях.

К выделенным помещениям предъявляется ряд требований:

- выделенное помещение должно размещаться не ниже второго этажа;
- выбирать выделенное для переговоров помещение нужно в центре здания, окна которого выходят во внутренний двор, являющийся контролируемой территорией. Если окна выходят за контролируемую зону, то необходимо применять систему акустической защиты, закрывать окна и форточки во время переговоров;
- в выделенном помещении рекомендуется устанавливать пластиковые окна с двойными или тройными стеклопакетами, которые монтируются на виброизоляционные резиновые прокладки;
- двери в такие помещения должны быть двойные, с тамбуром и звукоизоляцией. При строительстве в стены укладывают звукоизоляционные материалы.

Виброакустический канал связан с распространением колебаний звуковой частоты по строительным конструкциям и инженерным коммуникациям. Практика подтверждает хорошее распространение звуковых колебаний по арматуре ограждающих конструкций, трубам отопления и водоснабжения. При удачном стечении обстоятельств с расстояния нескольких десятков метров можно прослушать разговоры, ведущиеся в помещении, с помощью вибродатчика (стетоскопа), установленного на трубу отопления или строительную конструкцию.

Наиболее эффективный способ защиты в этом случае – применение системы активной виброзащиты с установкой вибродатчиков на трубы центрального отопления помещения, шахты вентиляции и

кондиционирования. Стены помещения при строительстве или реконструкции нужно отделывать звукоизоляционными и виброизоляционными материалами.

Электромагнитный канал – это все средства связи и ПЭВМ, использующие электромагнитное излучение: радиостанции, сотовые телефоны, беспроводные телефонные трубки. Следует взять за правило не обсуждать конфиденциальные вопросы, используя указанные средства.

Определим технические каналы утечки информации, обрабатываемой в технических средствах приема, обработки, хранения и передачи информации:

- электромагнитные – перехват побочных электромагнитных излучений и наводок (ПЭМИН) элементов технических средств приема и обработки информации;
- параметрические – перехват информации путем «высокочастотного облучения» основных технических средств связи (ОТСС);
- электрические – съем наводок электромагнитных излучений (ЭМИ) ОТСС, соединительных линий вспомогательных технических средств и систем (ВТСС) и посторонних проводников, съем информационных сигналов с линий электропитания и заземления ОТСС, съем информации путем установки в ОТСС электронных устройств перехвата информации в комплексе с устройствами передачи информации по радиоканалу (аппаратных закладок).

Побочные излучения промодулированы информационным сигналом, который обрабатывается на данном компьютере. В этом случае достаточно разместить неподалеку контрольный пункт со специальным радиоприемником и портативным компьютером.

1.3 Описание особенностей каналов утечки информации

1.3.1 Возможные каналы утечки

Возможные каналы утечки информации создаются [1]:

– низкочастотными электромагнитными полями, которые возникают во время работ ТСПИ и ВТСС;

– во время влияния на ТСПИ и ВТСС электрических, магнитных и акустических полей;

– при возникновении паразитной высокочастотной (ВЧ) генерации;

– при прохождении информативных (опасных) сигналов в цепи электропитания;

– при взаимном влиянии цепей;

– при прохождении информативных (опасных) сигналов в цепи заземления;

– при паразитной модуляции сигнала;

– вследствие ошибочных коммутаций и несанкционированных действий.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации по каналам ПЭМИН можно разделить на электромагнитные, электрические и параметрические, как представлено на рисунке 1.16 [2].

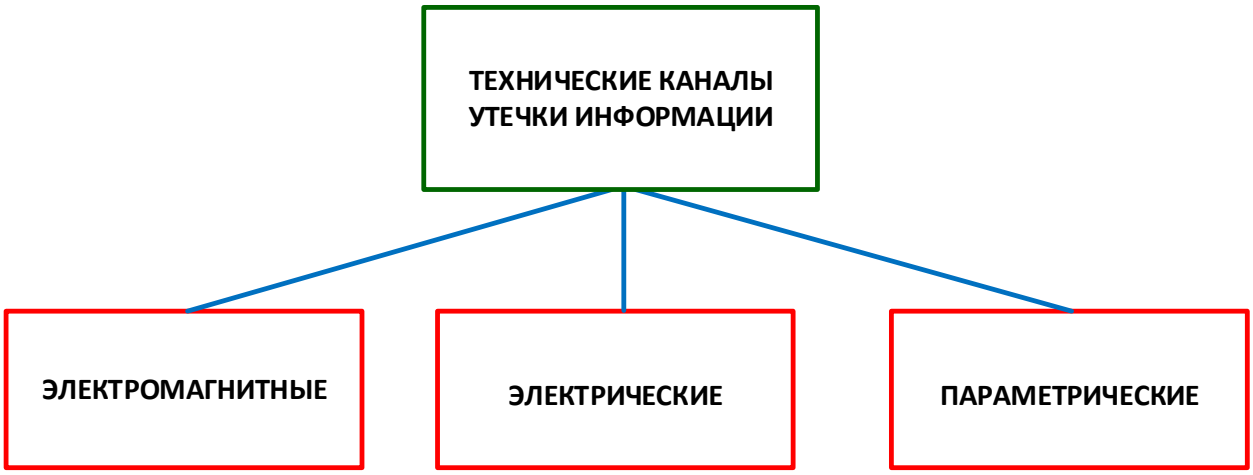

Рисунок 1.16 – Классификация технических каналов утечки информации

К электромагнитным каналам утечки данных обычно относят:

- сбор побочных ЭМИ элементов ТСПИ;
- сбор ПЭМИ в пределах частот работы высокочастотных генераторов в ТСПИ и ВТСС;
- сбор ПЭМИ в пределах частоты самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

1.3.2 Побочные электромагнитные излучения элементов ТСПИ

В ТСПИ хранилищем данных является электрический ток, числовые характеристики которого (амплитуда, частота, фаза) могут меняться по закону изменения информационного сигнала. В процессе прохождения электрического тока по токопроводящим составляющим ТСПИ рядом с ними могут образовываться магнитные и электрические поля. Благодаря этому элементы ТСПИ можно рассматривать в качестве излучателей электромагнитного поля, передающего какие-то данные.

1.3.3 Электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ и ВТСС

В состав ТСПИ и ВТСС могут включатся различного рода генераторы высокой частоты. К таким устройствам относятся: задающие генераторы, генераторы стирания и подмагничивания, генераторы тактовой частоты и маломощные генераторы радио и телевизионных устройств.

В процессе внешних воздействий сигнала (к примеру, электромагнитных колебаний) на элементах ВЧ-генераторов появляются электрические сигналы, которые образуют паразитное изменение собственных ВЧ-колебаний генераторов. Эти измененные ВЧ-колебания направлены в окружающее пространство.

1.3.4 Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ

Самовозбуждение УНЧ ТСПИ (к примеру, усилителей систем звука и звукового сопровождения, магнитофонов, систем громкоговорящей связи) имеет место за счет возникновения некоторых паразитных обратных связей, в итоге приводящее к переключению усилителя в режим автоматической

генерации сигналов. Сигнал на частотах самовозбуждения обычно оказывается уже измененным информационным сигналом. Самовозбуждение определено, в основном, при переводе УНЧ в режим работы на перегрузке.

Отлов сторонних электромагнитных излучений ТСПИ возможен при помощи средств радиотехнической разведки, находящихся вне контролируемой зоны.

1.3.5 Электрические каналы утечки информации

Основными причинами появления электрических каналов утечки данных становятся:

− наводки ЭМИ ТСПИ на соединительные элементы ВТСС и сторонние проводники, которые находятся все зоны контроля – образуются при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также в случае имеющейся гальванической связи соединительных линий ТСПИ и сторонних проводников или линий ВТСС. Влияние наводимых сигналов в большей степени зависит от мощности излучения, отдаленности до проводников, а также общей длины совместного взаимодействия соединительных линий ТСПИ и посторонних проводников.

Случайной антенной называется цепь ВТСС или другие проводники, способные реагировать на побочные электромагнитные излучения.

Случайные антенны характеризуются как распределенные и сосредоточенные. Сосредоточенная случайная антенна существует в виде компактного технического средства, например, телефон, громкоговоритель радиотрансляционной сети и распределенной случайной антенной являются случайные антенны с различными параметрами: провода, кабели, металлические трубы и остальные проводящие ток коммуникации:

− поступление информационных сигналов в цепи электропитания ТСПИ – имеет место при устойчивой магнитной связи между выходным трансформатором усилителя и трансформатором выпрямителя. Помимо этого, токи усиливаемых информационных сигналов замыкаются через

какой-то источник электропитания, делая на его внутреннем сопротивлении низкое напряжение, которое при малом затухании в фильтре выпрямительного устройства может быть найдено в линии электропитания. Такой сигнал попадает в цепи питания также в процессе того, что усредненное значение используемого тока в оконечных каскадах усилителей так или иначе связано с амплитудой информационного сигнала, что производит неравномерную нагрузку на выпрямитель и ведет к изменению используемого тока по закону изменения информационного сигнала - попадание информационных сигналов в цепи заземления ТСПИ.

Кроме заземляющих проводников, которые создаются непосредственно для соединения ТСПИ с контуром заземления, гальваническую связь с землей могут также имеют проводники, которые находятся все зоны контроля. К ним часто относят нулевой провод сети электропитания, экраны (металлические конструкции) соединительных кабелей, металлические трубы систем водоснабжения и отопления, металлическая арматура железобетонных конструкций и т.д. Подобные проводники, совместно с устройством заземления реализуют разветвленную систему заземления, на которой расположены информационные сигналы. Кроме того, в грунте около заземляющего устройства имеется электромагнитное поле, которое также можно считать источником данных.

Перехват данных по электрическим каналам утечки имеет место путем подключения к месту соединения линий ВТСС с посторонними проводниками, проходящими через помещения, где установлены ТСПИ, а также к их системам электропитания и заземления. Для этого часто применяются различные средства радиотехнической разведки, а также специфическая измерительная аппаратура.

Получение данных с применением аппаратных закладок. Электронные устройства захвата данных, которые находятся в ТСПИ, называют аппаратными закладками. Они напоминают внешне миниатюрные устройства, излучение которых изменяется информационным сигналом.

Зачастую закладки устанавливаются в ТСПИ импортного производства, однако есть риск их установка и в отечественных средствах.

Электрический канал перехвата данных, передаваемых по кабельным линиям связи, так или иначе определяет подключение аппаратуры разведки к кабельным линиям связи посредством прямого контакта.

Наиболее легкий способ – это реализация параллельного подключения к линии связи. Но подобный факт легко отслеживается, так как ведет к изменению параметров линии связи ввиду падения напряжения.

Поэтому средства разведки подключаются к линии связи при помощи согласующего устройства, минимизирующего падение напряжения, либо через устройства возмещения падения величины напряжения. В таком случае аппаратура разведки и прибор компенсации падения напряжения соединяется с линией связи последовательно, что существенно усложняет обнаружение несанкционированного подключения к ней.

Подобный контактный способ применяется для снятия данных с коаксиальных, а также с низкочастотных кабелей связи. А для кабелей, в которых имеется повышенное давление воздуха, используются устройства, минимизирующие его снижение, что позволяет предотвратить срабатывание специальной сигнализации.

Электрический канал может быть использован для перехвата телефонных разговоров. В таком случае считываемая информация может непосредственно переносится на диктофон или отсылаться по радиоканалу в пункт приема для ее сохранения и анализа.

1.3.6 Параметрический канал утечки информации

Перехват обрабатываемой в технических средствах информации возможен также путем их «высокочастотного облучения». При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля [3]. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и

переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения ТСПИ могут использовать импульсные сигналы.

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.

Таким образом, перехват информации, обрабатываемой техническими средствами, может осуществляться путем:

- перехвата побочных электромагнитных излучений, возникающих при работе технических средств;
- перехвата наводок информационных сигналов с соединительных линий ВТСС и посторонних проводников;
- перехвата информационных сигналов с линий электропитания и заземления ТСПИ;
- высокочастотного облучения ТСПИ;
- внедрением в ТСПИ закладных устройств.

1.3.7 Классификация и характеристика технических каналов утечки акустической (речевой) информации

Акустическая информация – это данные, носителем которых являются акустические сигналы. В таком случае рассматриваются данные, передаваемые с помощью человеческой речи, то есть речевые. Источники речевой информации встречаются как первичные – когда источниками акустических колебаний выступают механические колебательные системы, например, органы речи человека, так и вторичные – различного типа преобразователи, в том числе электроакустические. Последние относятся к классу устройств, предназначенных для изменения акустических колебаний в электрические и обратно. К ним относят пьезоэлементы, микрофоны, телефоны, громкоговорители. В различных формах акустических колебаний

можно выделить простые и сложные сигналы. Тональным является сигнал, вызываемый колебанием, происходящим по синусоидальному закону. Сложный сигнал состоит из целого спектра гармонических составляющих. Под речевым сигналом понимается сложный акустический сигнал в частотном диапазоне от 200-300 Гц до 4-6 кГц. В соответствии с физической природой возникновения подобных сигналов, среды распространения колебаний делят на воздушные, вибрационные, электроакустические, параметрические и оптико-электронные. Классификация технических каналов утечки представлена на рисунке 1.17.

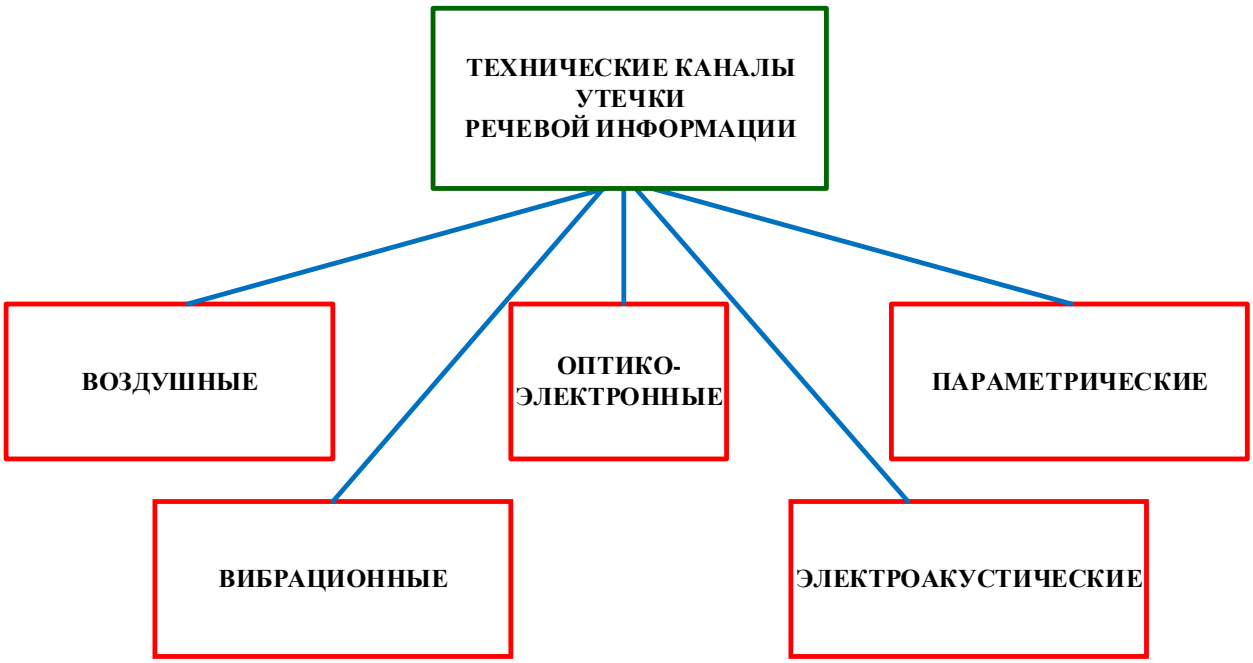

Рисунок 1.17 – Классификация технических каналов утечки речевой информации

В воздушных технических каналах утечки данных средой прохождения акустических сигналов выступает воздух, и для их перехвата применяются миниатюрные высокочувствительные микрофоны и разработанные направленные микрофоны. Компактные микрофоны соединяются с компактными звукозаписывающими устройствами (диктофонами) или другими портативными передатчиками.

Переносные устройства, включающие в себя компактные микрофоны и передатчики, принято называть закладными устройствами сбора речевой информации, или по другому, акустическими закладками.

Собранные такими устройствами данные могут отправляться по радиоканалу, оптическому каналу (в нужном диапазоне длин волн), по сети переменного тока, соединительным линиям ВТСС, другим проводникам (трубам водоснабжения и канализации, металлоконструкциям). И для передачи данных по трубам и металлоконструкциям применяются не только электромагнитные, но и ультразвуковые и механические колебания.

Чтобы перехватить данные по данному каналу, помимо закладного устройства нужен особый передатчик с направленным излучением и приемник.

2 Выбор методов и средств защиты информации и их классификация

2.1 Методы и средства поиска утечки информации по техническим каналам

Борьба с внедренными на охраняемые объекты устройствами несанкционированного съема информации (НСИ) является на сегодняшний день одним из важных направлений деятельности служб безопасности (СБ) по обеспечению информационной безопасности. Как известно, под НСИ понимается незаконное получение конфиденциальной информации, в том числе и с использованием различных технических средств. Одним из «технических» способов НСИ является использование закладных устройств (ЗУ), скрытно внедряемых (закладываемых или вносимых) в места возможной циркуляции конфиденциальной информации. Номенклатура таких устройств на сегодняшний день чрезвычайно обширна. Она включает средства перехвата информации с каналов связи, диктофоны, радиомикрофоны, сетевые микрофоны, устройства скрытого видеонаблюдения, стетоскопы, преобразователи (усилители) информативных сигналов и т. п. Современные ЗУ, как правило, отличаются хорошим качеством маскировки, высокими техническими характеристиками и простотой установки. Необходимо также учитывать и тот фактор, что эти средства постоянно совершенствуются, поэтому тактико-технические вопросы их выявления представляют для СБ большие сложности.

Классификация технических средств обнаружения и локализации закладных устройств приведена на рисунке 2.1. Учитывая, что радиоизлучающие закладки преобладают на рынке ЗУ, существуют разнообразные средства радиоконтроля обследуемых помещений: от простейших индикаторов электромагнитного поля до сложных автоматизированных комплексов. Классификация средств обнаружения радиоизлучений закладных устройств представлена на рисунке 2.2.

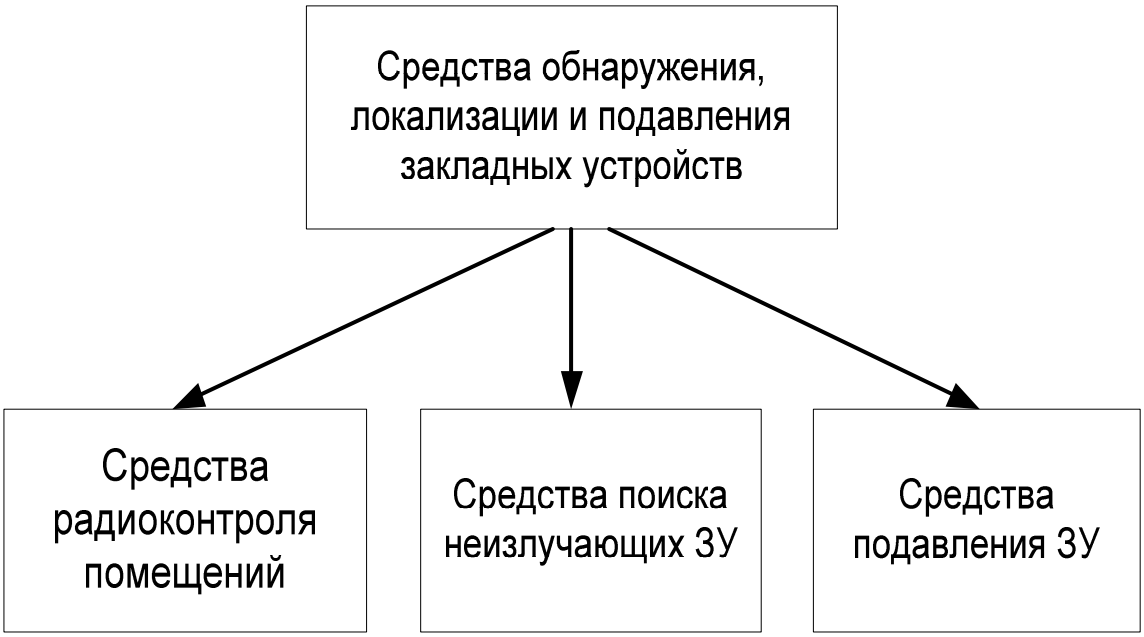

Рисунок 2.1 – Классификация технических средств обнаружения и локализации закладных устройств

Рисунок 2.2 – Классификация средств обнаружения радиоизлучений закладных устройств

Изучение практики использования приборов поиска показывает, что с их помощью можно решить и соответственно обнаружить конкретные виды ЗУ.

Первый вид защиты – выявление факта работы (обнаружение) и локализация местоположения радиоизлучающих ЗУ:

- радиомикрофоны (РМ);
- «сетевые» радиомикрофоны (с питанием от сети 220 В);
- телефонные радиопередатчики (ТРП);
- радиостетоскопы;
- скрытые видеокамеры с радиоканалом передачи информации;
- технические средства систем пространственного высокочастотного (ВЧ) облучения в радиодиапазоне.

Второй вид защиты – обнаружение и локализация местоположения ЗУ, использующих проводные линии различного предназначения:

- ЗУ, использующие для передачи перехваченной информации линии сети переменного тока 220 В и способные работать на частотах до 5 МГц;
- ЗУ, использующие для передачи перехваченной информации абонентские телефонные линии, линии систем пожарной и охранной сигнализации и т. п.;
- технические средства систем высокочастотного навязывания.

Третий вид защиты – обнаружение и локализация местоположения ЗУ, работающих с излучением в инфракрасном (ИК) диапазоне:

- ЗУ, регистрирующие акустическую информации в контролируемом помещении с ее последующей передачей по каналу в ИК-диапазоне;
- ЗУ пространственного облучения в ИК-диапазоне.

Для разработки тактико-технических рекомендаций по проведению поиска различных видов ЗУ, на наш взгляд, необходимо провести анализ

основных методов идентификации ЗУ, применяемых в рассматриваемых поисковых приборах. Изучение практики их применения показывает, что для идентификации ЗУ используют следующие основные методы:

- амплитудный метод (АМ);
- метод акустической завязки (АЗ);
- метод классификации принимаемых сигналов «на слух»;
- метод контроля параметров сигналов по осциллограммам и спектрограммам.

Как известно, АМ основан на регистрации возрастания уровня принимаемого поисковым прибором сигнала при приближении приемной антенны прибора к месту расположения источника сигнала. Радиус зоны обнаружения источника зависит от мощности излучаемого им сигнала, направленности его антенны и уровня фона электрического поля в точке расположения приемной антенны прибора.

Метод АЗ основан на возникновении положительной акустической обратной связи между микрофоном радиозакладки и динамиком прибора. Признаком возникновения АЗ является появление характерного «свиста», тон и интенсивность которого изменяются при приближении динамика прибора к микрофону радиозакладки.

Метод классификации принимаемых сигналов «на слух» основан на возможности прослушивания анализируемых сигналов.

В качестве одного из основных поисковых методов применяется также визуальный метод контроля параметров сигналов по осциллограммам и спектрограммам. Практический интерес может представлять конкретизация применения указанных методов для идентификации различных видов ЗУ.

Анализ ЗУ показывает, что к категории опасных в сочетании с внешними можно отнести радиосигналы, источниками которых могут быть:

- РМ с выносным акустическим микрофоном;

- ТРП, установленные на линии связи за пределами контролируемого помещения;
- радиостетоскопы, установленные с наружной стороны ограждающих помещение поверхностей;
- вынесенные передатчики скрытых видеокамер;
- устройства внешнего высокочастотного облучения.

С другой стороны, к неопасным в сочетании с внешними можно отнести радиосигналы, источниками которых могут быть широковещательные радиостанции, станции телевизионного вещания, средства радиосвязи и т. п. В качестве источников внутренних неопасных радиосигналов могут рассматриваться прежде всего электроприборы, оргтехника, бытовые средства, а также их блоки питания.

Таким образом, представленная классификация выявляемых поисковыми приборами сигналов по совокупности критериев позволяет оперативно «фильтровать» фиксируемые сигналы и нацеливать усилия оператора только на анализ «опасных» сигналов от ЗУ.

Основные особенности обнаружения и локализации радиоизлучающих закладных устройств

Рассмотрим основные характеристики и особенности идентификации поисковыми приборами РМ. Изучение практики показывает, что в целом в эту группу можно включить следующие их виды:

- с параметрической стабилизацией частоты передатчика;
- с кварцевой стабилизацией частоты;
- с вынесенным передатчиком;
- с закрытым или маскированным радиоканалом.

Рассмотрим основные характеристики и особенности идентификации РМ поисковыми приборами.

Основная особенность РМ с параметрической стабилизацией частоты передатчика большие пределы изменения несущей частоты (до нескольких

МГц). Изучение накопленного опыта показывает, что для поиска и локализации РМ с параметрической стабилизацией частоты можно использовать все перечисленные методы идентификации.

РМ с кварцевой стабилизацией частоты имеют небольшие пределы изменения несущей частоты (до десятка КГц) и низкий уровень звукового сигнала на выходе амплитудного детектора приемника поискового прибора, что приводит к значительно меньшим размерам зоны возникновения АЗ. Поэтому для поиска и локализации такого типа ЗУ целесообразно использование всех ранее перечисленных методов, кроме метода АЗ.

Особый интерес для СБ могут представлять наработанные тактические варианты проведения поисковых мероприятий с использованием вышеперечисленных приборов по обнаружению «высокопрофессиональных» средств негласного получения информации, а именно РМ с вынесенным передатчиком и РМ со сложным видом радиосигнала, закрытым или маскированным радиоканалом. Сразу же следует отметить, что поиск высокопрофессиональных ЗУ весьма непрост ввиду высокой сложности их идентификации. Тем не менее имеются некоторые тактические варианты по обнаружению подобных ЗУ с определенной степенью вероятности.

Опыт показывает, что при проведении поиска РМ с вынесенным передатчиком необходимо применение ранее перечисленных методов поиска с учетом следующих нюансов. Для локализации микрофона рассматриваемого РМ необходимо использование метода АЗ, а для поиска радиопередатчика РМ (который может находиться в проверяемом помещении или за его пределами) АМ.

Высокопрофессиональными средствами НСИ являются и РМ со сложным видом радиосигнала, с закрытым или маскированным радиоканалом. Их основная особенность состоит в том, что принятый и демодулированный сигнал не несет в себе информации об акустическом фоне помещения. Это объясняется использованием для закрытия (маскирования) радиоканала методов инверсии спектра, цифровых методов

передач и сложных видов модуляции. Проведенный анализ таких закладок показал, что к основным способам «ухода» от обнаружения ЗУ рассматриваемого типа, прежде всего относятся:

- сокращение времени излучения РМ, что достигается путем использования ЗУ с дистанционным управлением;
- применение ЗУ с накоплением информации и последующей импульсной передачей на приемное устройство (импульсные передатчики это устройства, которые накапливают и сохраняют информацию в течение некоторого времени, а затем передают ее коротким импульсом. Такие устройства используют цифровую модуляцию и обычно имеют очень широкую полосу пропускания в зависимости от периодичности импульсов и рабочего цикла. Период передачи импульсов зависит от типа устройства: он может составлять от нескольких миллисекунд до нескольких минут. Возможно использование импульсного передатчика, передающего сигнал лишь раз в несколько часов. Передатчик такого типа крайне сложно обнаружить из-за длительного периода отсутствия сигнала передачи);
- использование ЗУ со скачкообразным изменением частоты излучения (ЗУ со скачкообразной перестройкой частоты устроены таким образом, чтобы передавать информацию на одной частоте очень непродолжительное время (от 5 до 100 миллисекунд), а затем изменять частоту на новую. Такие передатчики переключаются между несколькими различными частотными каналами в пределах четко заданной полосы. Передатчик со скачкообразной перестройкой обычно передает цифровой сигнал, но может быть и аналоговым;
- применение в ЗУ «закрытия» передаваемой информации с использованием различных модулирующих функций, в частности цифровых (в том числе с дельтамодуляцией), шумоподобных. Технология шумоподобного сигнала распределяет его энергию по более широкому участку спектра частот, что делает передатчик менее заметным.

Для выявления внешних потенциально опасных ИК-излучений обследуются оконные проемы, при этом ИК-детектор поисковых приборов ориентируется в сторону окна. Далее, путем плавного изменения его пространственного положения проводится обследование всей площади оконного проема. Поскольку зондирующий сигнал не имеет модуляции, его наличие может быть оценено только по показаниям индикатора уровня и тональной индикации.

Локализация источников ИК-излучения осуществляется АМ.

2.2 Технические устройства иностранного производства, применяемые для негласного съема информации

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.

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), радиозакладки в виде авторучек, пепельниц, картона, «забытых» личных вещей, стандартных элементов телефонных аппаратов. К этой же категории средств относятся различные варианты миниатюрных диктофонов, микрокамер, телекамер.

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.

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 другие.

2.3 Пространственное электромагнитное зашумление

Одним из наиболее опасных технических каналов утечки информации на объектах информатизации является канал, возникающий вследствие побочных электромагнитных излучений (ПЭМИ) технических средств обработки информации (ТСОИ), в том числе средств вычислительной техники (СВТ). Такой канал утечки информации часто называют электромагнитным [8].

Защита объектов информатизации от утечки информации, возникающей за счет ПЭМИ, достигается экранированием и заземлением технических средств и их соединительных линий, экранированием помещений, а также использованием систем пространственного электромагнитного зашумления.

2.4 Заземление технических средств

Эффективным способом уменьшения уровня ПЭМИ является защита их источников. В процессе создания электромагнитного экранирования

важно заземление экрана источника ПЭМИ, где подразумевается заранее спланированное соединение самого экрана с заземляющим устройством.

Заземляющее устройство обычно состоит из заземлителя и заземляющих проводников, соединяющих экран с заземлителем.

Заземлитель является проводящей частью или совокупностью соединенных друг с другом проводящих частей, находящихся в непосредственном электрическом контакте с землей или при помощи промежуточной проводящей среды.

Часть земли, которая расположена вне зон действия какого-либо заземлителя, и электрический потенциал которой равняется нулю, становится зоной нулевого потенциала (так называемая относительная земля), а отдельная часть земли между заземлителем и нулевым потенциалом является зоной растекания (либо же локальная земля). Именно поэтому под определением «земля» зачастую подразумевается земля в зоне растекания.

Заземление можно разделить на два главных вида в зависимости от выполняемой роли: защитное и рабочее.

Защитное заземление подразумевает заземление, реализованное в целях электробезопасности, в свою очередь рабочее заземление включает в себя заземление точки или точек токоведущих частей оборудования, внедряемое для обеспечения его непосредственной работы.

Заземление, применяемое в целях электромагнитного экранирования, можно отнести к рабочему заземлению, но оно также поддерживает функции и защитного заземления.

2.5 Экранирование

Эффективным методом снижения уровня ПЭМИ является экранирование их источников.

Различают следующие способы экранирования: электростатическое, магнитостатическое и электромагнитное [7].

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 электростатического 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 [7], [11].

С целью уменьшения уровня побочных электромагнитных излучений средства обработки информации ограниченного доступа выпускаются в специальном защищенном исполнении.

2.6 Цифровые методы защиты информации от ПЭМИН

Маскировка («зашумление») ЭМИ используется не только в задачах защиты информации. Традиционно и широко маскировка ЭМИ применяется в радиоэлектронной борьбе (РЭБ), как способ подавления радиоэлектронных средств радиолокации, радионавигации и радиосвязи [3]. История использования этого способа в РЭБ насчитывает свыше 100 лет, и до восьмидесятых годов двадцатого века для этих целей также использовались генерация и излучение мощных широкополосных шумов [4], [5].

Однако логика развития радиоэлектронных средств (РЭС), увеличение числа РЭС, их несущих частот и ширины спектра сигналов заставили вместо генерации и излучения шумов использовать для маскировки ЭМИ защищаемые радиосигналы путем цифрового запоминания их структуры, наделения их в цифровом виде дополнительными помеховыми модуляциями и излучения их после цифроаналогового преобразования [5], [6].

Тридцатилетний опыт использования в РЭБ такого способа маскирования ЭМИ показал [6], [7], [8], что:

- таким способом достигается высокое качество маскирования ЭМИ в широком диапазоне частот при использовании передатчиков помех с мощностью на порядки меньших, чем при излучении шумов;
- осуществляется автоматическая адаптация характеристик излучаемых помех к изменениям частотной и временной структуры защищаемых сигналов и характеристик каналов ЭМИ;
- современные достижения микроэлектроники и цифровой технологии обработки широкополосных радиосигналов позволяют реализовать данный способ в виде компактных устройств (специализированные большие интегральные схемы – СБИС);
- цифровой способ маскирования ЭМИ позволяет существенно повысить электромагнитную совместимость с другими средствами за счет уменьшенной (на порядки) мощности излучаемых помех, а также за счет «экономного» излучения помех только на тех частотных составляющих спектра ЭМИ, которые совпадают с частотными составляющими спектра маскирующего сигнала.

Логично и целесообразно использовать цифровой способ маскирования защищаемых сигналов в задачах защиты информационных систем от утечек информации по паразитным каналам ЭМИ.

Рассмотрим вариант использования цифрового способа защиты на примере защиты персональных ЭВМ (ЭВМ) от утечек информации по паразитным каналам ЭМИ, обусловленными работой цифровых устройств ЭВМ.

Обобщенная схема цифровой защиты ПЭВМ приведена на рисунке 2.3.

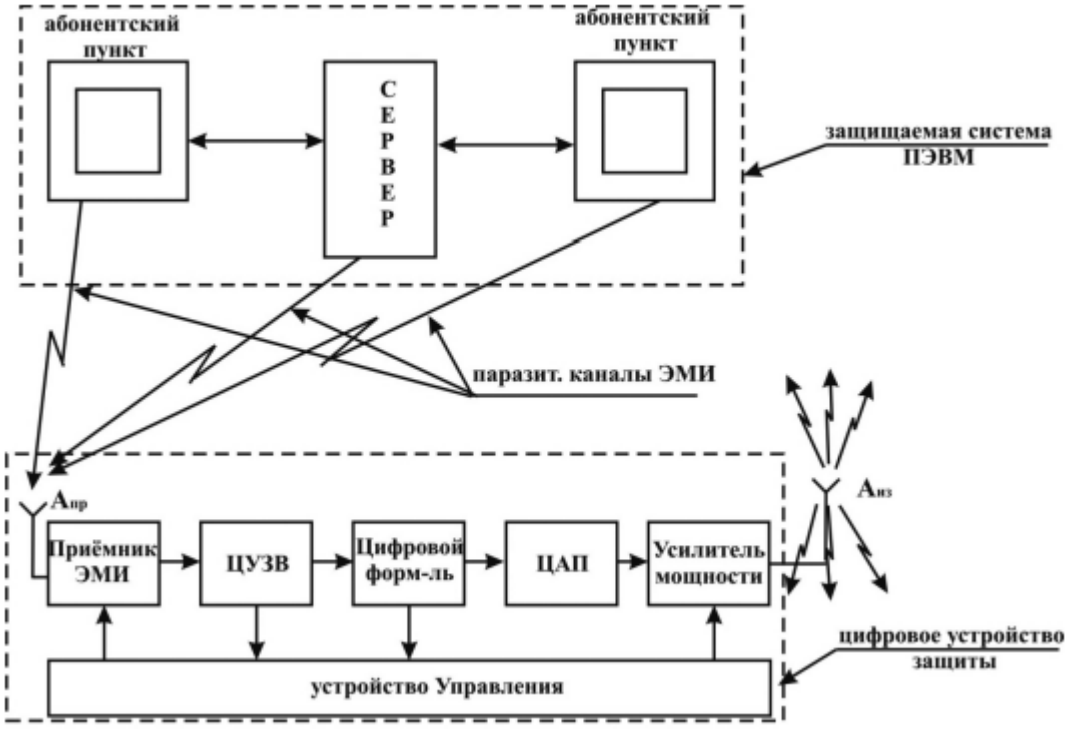

Рисунок 2.3 – Обобщенная схема цифровой защиты ПЭВМ от утечек информации по паразитным каналам

Согласно этой схеме ЭМИ компьютеров регистрируются приемником радиосигналов, которые после усиления, преобразования, фильтрации подаются на широкополосное цифровое устройство запоминания и воспроизведения радиосигналов (ЦУЗВ). В ЦУЗВ принятые сигналы ЭМИ преобразуются в последовательность цифровых слов и запоминаются в ОЗУ В результате формируется подробный цифровой «портрет» ЭМИ компьютеров. В цифровом модуляторе путем дополнительной модуляции цифрового портрета, разбиения его на отдельные части и их перемешивания формируется цифровая копия маскирующего сигнала, частотная и временная структура которой совпадает со структурно-временной структурой сигнала ЭМИ. Цифровая копия маскирующего сигнала преобразуется в радиосигнал в цифро-аналоговом преобразователе (ЦАП), усиливается по мощности и излучается через антенну .В результате в паразитных каналах ЭМИ присутствует смесь сигналов ЭМИ компьютеров и сформированного маскирующего сигнала. Так как по частотной и временной структуре эти

сигналы практически идентичны, то выделить полезную информацию из этой смеси очень трудно.

Проведенные исследования показали [9], что при равенстве мощностей сигналов ЭМИ и цифрового маскирующего сигнала выделить полезную информацию из смеси невозможно.

Устройство цифровой защиты ПЭВМ периодически обновляет записанную в ОЗУ копию сигналов ЭМИ, что позволяет постоянно отслеживать изменения параметров сигналов ЭМИ и автоматически адаптировать под них частотную и временную структуру маскирующего сигнала.

На сегодняшний день на рынке интегральных схем предлагается большое разнообразие СБИС, реализующих ЦУЗВ в широком частотном диапазоне, способных производить запись сигналов ЭМИ в полосе тысяча МГц и более [8], [10].

Кроме того, на рынке предлагаются программируемые логические интегральные схемы (ПЛИС) общего назначения, на базе которых возможно создание цифровых устройств защиты с расширенным частотным диапазоном.

Таким образом, на базе современных достижений микроэлектроники и цифровых технологий обработки сигналов можно создать новый класс цифровых устройств защиты систем обработки информации от утечек по паразитным каналам ЭМИ, осуществляющих маскирование сигналов ЭМИ цифровым способом на основе цифрового запоминания и воспроизведения сигналов ЭМИ.

Цифровой способ маскирования сигналов ЭМИ позволяет без увеличения габаритов и излучаемой мощности многократно увеличить полосу частот маскируемых сигналов и автоматически осуществлять адаптацию их характеристик при изменениях параметров ЭМИ защищаемой системы.

Следует отметить, что описанный цифровой метод применим для маскирования излучений не электромагнитной природы, например виброакустических излучений.

2.7 Выбор оборудования и анализ современной аппаратуры необходимой для поиска ЭУНПИ и для использования в лаборатории

Основываясь на демаскирующих признаках устройств негласного получения информации, а также сформированных требованиях по выбору этих устройств, остановимся на следующих типах оборудования:

- нелинейные локаторы (устройства для поиска полупроводниковых элементов);
- вспомогательное оборудование для визуального обнаружения устройств негласного получения информации;
- дозиметры;
- устройства для проведения ИКК;
- обнаружитель радиопередающих устройств стандарта GSM;
- автоматизированный комплекс выявления и идентификации несанкционированных электронных устройств беспроводной связи;
- автоматизированный комплекс выявления ПДУ;
- переносная рентгенотелевизионная установка;

Для выбора поисковых приемников ближней зоны (для выявления маломощных передатчиков) сравним по таблице 2.1 следующее аналогичное оборудование.

Таблица 2.1 – Сравнение поисковых приемников ближней зоны

Характеристика	Скорпион v.3.5	Кордон	Контур
1	2	3	4
Диапазон частот	30-2000 МГц	50-8000 мГц	33-2000 МГц
Чувствительность 30 – 1000 МГц 1000 – 2000 МГц	не хуже 50 мкВ не хуже 1000 мкВ	не хуже 1 мВ не хуже 2 мВ	не хуже 25 мкВ не хуже 100 мкВ
Время просмотра диапазона	не более 15 с	не более 15 с	не более 10 с

Характеристика	Скорпион v.3.5	Кордон	Контур
1	2	3	4
Диапазон измерения уровня входного			

Продолжение таблицы 2.1

Характеристика	Скорпион v.3.5	Кордон	Контур
сигнала	50 дБ	55 дБ	50 дБ
Мощность прицельной помехи	не менее 50 мВт	не менее 50 мВт	не менее 55 мВт
Количество запоминаемых частот	524	524	256 шт
Индикация	ЖКИ-дисплей	ЖКИ-дисплей	ЖКИ-дисплей
Питание	батареи или внешний источник 9,6...12 В	батареи или внешний источник 9,6...12 В	4 элемента типа «ААА»
Потребление	200 мА	200 мА	не более 150 мА
Габариты (без антенн)	165x90x29 мм	179 x 67 x 30 мм	160x62x38 мм

На основании проведенного сравнения выбираем поисковый приемник ближней зоны «Контур».

Для выбора поисковых приемников сравним следующее оборудование по таблице 2.2:

- многофункциональный поисковый прибор ST 032;
- поисковый прибор ST-031 «Пиранья»;
- поисковый комплекс СРМ-700.

Сравнение характеристик поисковых приемников приведено в таблице 2.2.

Таблица 2.2 – Сравнение характеристик поисковых приемников

Параметр	ST 032	ST-031 «Пиранья»	СРМ-700
Диапазон рабочих частот, МГц	30-2500	30-2500	15 кГц до 3000 ГГц
Чувствительность, мВ	(30МГц-1000МГц) <1 (1000МГц-1800МГц) <4	200МГц-1000МГц <-2 1000МГц-1600МГц <-4 1600МГц-2000МГц <-8	<4
Динамический диапазон, дБ	63	60	60
Чувствительность	<15 (100МГц-	<-10	<15

частомера, мВ	1200МГц)		

Наиболее важной характеристикой прибора является его чувствительность. Как видно из приведенной таблицы, наибольшей чувствительностью отличается ST-031 «Пиранья», следовательно, именно этот прибор выбираем в качестве используемого.

Далее сравним по таблице 2.3 наиболее распространенные на рынке модели нелинейных локаторов.

Таблица 2.3 – Сравнение моделей нелинейных локаторов

Технические характеристики	Катран	SuperBroom	NR-μ
Режим излучения	Непрерывный.	Непрерывный.	Непрерывный
Мощность излучения, Вт	2.5	0,014...1,4	не менее 2 Вт
Частота излучения, МГц	885 -895, с шагом 1МГц	885,5	1 696, 2 544
Частота приема, МГц	2-я, 3-я гармоники	1777 2665,5	1 696, 2 544
Вид излучаемого сигнала	ЧМ Девиация 1,5 кГц	ЧМ	ЧМ
Чувствительность, дБм	-127	-127	-150
Коэффициент усиления пере-дающей и приемной антенн, дБ	6	3	не менее 8
Напряжение питания, В	12	12	12
Цена, рублей	190000	600000	150000

Таким образом, по стоимости (минимальная) и чувствительности (максимальная) выбираем нелинейный локатор NR-μ.

Портативный измеритель частоты MFP, представленный на рисунке 2.7. MFP – 8000 способен реагировать на любые источники радиоизлучений в диапазоне частот до 8 ГГц, имеющие мощность сигнала в точке приема не менее 0,5х10 Вт и превышающую естественный фон на 3...5 дБ с расстояния до 8-ми метров, фиксировать излучение радиопередающего устройства с выходной мощностью 5 мВт, работающего на согласованную четвертьволновую антенну.

Рисунок 2.4 – Портативный измеритель частоты MFP-8000

MFP-8000 позволяет пользователю в ручном и автоматическом режимах:

- определять частоту входного сигнала в диапазоне частот от 100 кГц до 8 ГГц;
- измерять мощность входного сигнала в диапазоне уровней от –53 дБм до +30дБм;
- идентифицировать во входном сигнале наличие признаков протокола обмена данными для сотовой и телефонной систем связи (GSM 900/1800/1900, DECT), в GSM определять режим работы «SMS», «Talk» и определять значение частоты;
- автоматически (посредством встроенного интерфейса) настраивать панорамные радио приемники или другие устройства на измеренную MFP-8000 частоту сигнала (опция по специальному заказу);
- использовать (встроенные) память прибора, часы и календарь для протоколирования и хранения результатов измерений;
- задействовать встроенный интерфейс при использовании MFP-8000 в качестве измерительного элемента в составе автоматизированных систем мониторинга эфира;

- осуществлять режим «акустозавязывания», используемый при проведении поисковых работ;
- поддерживать сторожевой режим по критерию превышения мощностью сигнала заданного порога.

Для выявления и идентификации несанкционированных электронных устройств беспроводной связи воспользуемся аппаратурой «Цифра».

Комплекс «Цифра» разработан специально для решения задач спецпроверок технических средств и специальных обследований помещений на наличие устройств несанкционированного получения информации в соответствии с действующими методиками и нормативными документами. Комплекс предназначен для исследований каналов наиболее распространенных беспроводных интерфейсов на наличие признаков несанкционированной передачи информации. Цифра позволяет оперативно выявлять сигналы устройств несанкционированной передачи информации в сетях GSM900/1800, UMTS (3G), DECT, WiFi, Bluetooth, ZigBee Pro и локализовывать места установки таких устройств в помещении.

Состав:

- управляющая ПЭВМ типа Notebook;
- антенная система, содержащая комплект антенн на рабочие диапазоны частот;
- блок аналоговой ВЧ обработки;
- блок логической обработки;
- блок активного обнаружения; селективный обнаружитель цифровых радиопередающих устройств системы электропитания, сопряжения и коммутации;
- комплект документации.

Далее рассмотрим дозиметр-радиометр МКС/СРП-08А. МКС/СРП-08А – поисковый дозиметр-радиометр для поиска источников и измерения

мощности эквивалентной дозы фотонного (гамма и рентгеновского) излучения, плотности потока альфа- и бета-частиц.

Простой в обращении высокочувствительный дозиметр-радиометр, удобный для проведения радиационных обследований, позволяющий проводить замеры в полевых условиях, при отсутствии сетевого электропитания, в мобильных лабораториях, а также в труднодоступных местах при использовании телескопической штанги длиной 1,5 метра, входящей в комплект поставки. Благодаря наличию звуковой сигнализации и аналоговой шкалы, мгновенно реагирующей на изменение плотности потока гамма и рентгеновского излучения, прибор удобен для проведения экспрессной оценки изменений радиационной обстановки.

Микропроцессорная система управления обеспечивает выполнение следующих функций:

- автоматический расчет мощности дозы с выравниванием ЭЗЧ по восстановленному действующему спектру фотонного излучения;
- вывод параметров на табло индикации;
- хронометраж измерения;
- масштабирование аналоговой шкалы (8 ступеней с шагом 1);
- установка на измерительной шкале маркера, соответствующего опорному замеру;
- контроль состояния аккумулятора;
- подсветка табло индикации.

Назначение:

- поиск источников гамма и рентгеновского излучения;
- измерение мощности эквивалентной дозы гамма и рентгеновского излучения;
- использование в составе прибора альфа-бета радиометрического блока детектирования позволяет проводить измерение плотности потока альфа и бета излучения с поверхности.

Технические характеристики:

- детектор;
- гамма-излучение: сцинтилляционный CsI(Na) или NaI(Tl);
- альфа и бета-излучение: счетчик Гейгера-Мюллера.

Диапазон измеряемых значений:

- мощность эквивалентной дозы фотонного излучения 0,03: 500 мкЗв/ч;
- плотности потока альфа-частиц 0,1: 700 см-2с-1;
- плотности потока бета-частиц 0,1: 700 см-2с-1.

Пределы допускаемой основной относительной погрешности измерения:

- мощность эквивалентной дозы гамма и рентгеновского излучения ±25%;
- энергетическая зависимость чувствительности относительно эффективной энергии 662 кэВ не более 25%.

Вывод информации:

- цифровая индикация результатов измерения мощности эквивалентной дозы фотонного излучения или скорости счета импульсов;
- цифровая индикация результатов измерения плотности потока альфа- или бета-частиц;
- интенсиметр – шкала загрузки измерительного тракта (аналог стрелочной индикации);
- звуковая сигнализация (через наушники);
- рабочая температура от –20 до +40 °С;
- конструктивное исполнение пульт в пластмассовом корпусе крепится либо на телескопической штанге, либо непосредственно на блоке детектирования;
- питание 4 аккумулятора типа АА;
- время непрерывной работы без подзарядки не менее 15 часов.

Для АРТМ используем аппаратуру Крона А-1. Комплекс «КРОНА А1» предназначен для обнаружения и локализации электронных устройств негласного получения информации (ЭУНПИ), передающих данные по радиоканалу, использующих все известные средства маскирования, выявления каналов утечки информации, созданных за счет акустопараметрических преобразований, а также для решения широкого круга задач радиомониторинга.

Позволяет обнаруживать пассивные и полуактивные акустопараметрические электромагнитные отражатели (эндовибраторы) в диапазоне частот от 30 МГц до 12 ГГц.

Комплекс разработан на основе многолетнего опыта создания подобных систем и реализует в себе наиболее передовые алгоритмы обнаружения ЭУНПИ. Применение нескольких алгоритмов обнаружения, каждый из которых основан на индивидуальных принципах демаскирования ЭУНПИ, позволяет с высокой степенью достоверности определить наличие ЭУНПИ, имеющих средства маскировки как по алгоритмам модуляции, так и по способам передачи (ЭУНПИ с цифровыми каналами передачи данных, с накоплением информации, с перестраиваемой частотой).

«КРОНА А-1» может использоваться как для экспресс-анализа наличия радиопередающих ЭУНПИ в контролируемом помещении, так и для долговременного круглосуточного мониторинга электромагнитной обстановки в одном или нескольких контролируемых помещениях.

Комплекс «КРОНА А-1» имеет эффективный алгоритм выделения полезного информативного сигнала в сложной помеховой обстановке, высокую точность измерений, что обеспечивает достоверные результаты поиска каналов утечки речевой информации, образованных за счет акустопараметрических преобразований.

Особенности:

- обнаружение и локализация радиопередающих электронных устройств негласного получения информации, использующих все известные средства маскирования;
- обнаружение пассивных и полуактивных акустопараметрических электромагнитных отражателей (эндовибраторов);
- анализ сигналов с нескольких антенн, используя встроенный антенный коммутатор;
- автоматическое распознавание цифровых каналов передачи данных;
- анализ сигналов в силовых сетях и слаботочных линиях, обнаружение ИК-излучателей;
- контроль диапазона частот, фиксированных частот, сетки частот;
- выполнение комплексных заданий;

Состав:

- основной блок;
- блок генераторов;
- комплект двухкомпонентных приемных и передающих антенн со штативами для их установки;
- комплект антенн «АШП-1» (4 штуки);
- конвертор для исследования в силовых сетях и слаботочных линиях с зондом для обнаружения ИК-излучателей;
- комплект кабелей;
- активная акустическая система, обеспечивающая требуемое звуковое давление в широком диапазоне частот;
- имитатор акустопараметрического отражателя;
- комплект специального программного обеспечения;
- ПЭВМ типа ноутбук с сумкой;
- ударопрочные герметичные кейсы для переноски;

- комплект документации.

Для проведения ВОК необходимо использовать базу данных Парнас-СПБД v2.0. Программа обеспечивает:

- разграничение доступа персонала к функциям и информационным ресурсам программы;
- встроенный классификатор ТС и ЭКБ, принятых за эталон (классификатор может организован по функциональному назначению ТС и ЭКБ, по производителю ТС и ЭКБ, по модели ТС и ЭКБ);
- встроенный классификатор угроз (перечень возможных каналов утечки);
- возможность сопоставления эталонов с каналами утечки информации;
- учет ТС и ЭКБ, принятых за эталон по установленным параметрам;
- добавление к эталону различных документов;
- редактирование информации об эталоне;
- автоматическое отображение информации об эталоне;
- поиск информации по различным параметрам;
- совместную работу пользователей;
- удаленную работу пользователя с программой, в том числе механизм предварительного просмотра данных (при использовании медленных каналов связи).

Программа обеспечивает возможность выполнения перечисленных ниже функций:

- разграничение доступа персонала к функциям и информационным ресурсам программы;
- добавление, изменение, состава пользователей, назначение ролей и прав пользователя, блокировка и разблокировка пользователей;
- персональные настройки доступа для любого пользователя;

- добавление, изменение, состава персональных компьютеров пользователей (ПК);
- защиту от использования на незарегистрированных в форме администрирования ПК (аппаратный ключ защиты);
- учет изменений вносимых пользователями;
- удаленный доступ пользователей, из других сетей, к информации, с целью обеспечения выездных работ;
- классификатор ТС и ЭКБ, принятых за эталон. Хранение информации об эталонах должно быть организовано в виде каталога. Возможность отображения каталога по различным признакам (тип ТС, производитель, функциональное назначение и т.д.). Правила классификации определения места в каталоге для конкретного ТС и/или ЭКБ;
- классификатор угроз;
- классификатор и справочник возможных угроз (каналов утечки информации);
- возможность редактирования и изменения указанного классификатора и справочников к нему;
- сопоставление эталонов с каналами утечки информации. Для каждого эталона, согласно принятых классификатора ТС и ЭКБ, предусмотрена возможность сопоставления с каналами утечки информации, ввод и хранение информации об опасных каналах и признаках утечки информации, а также информации о мероприятиях, необходимых для предотвращения утечки информации;

Учет эталонного ТС и ЭКБ в виде:

- номер договора/счета;
- номер партии ТС;
- дата начала регистрации партии ТС для проведения работ;
- тип ТС и ЭКБ;
- модель ТС и ЭКБ;

- страна производитель ТС;
- серийный номер ТС и ЭКБ;
- информация о составе/включение в состав другого ТС и ЭКБ;
- результат работ по каждому этапу проведенных работ;
- типовой алгоритм выполнения работ с эталоном;
- порядок разборки/сборки, раскладки составляющих частей и крепежных элементов посредством добавления фото/видео материалов, комментариев к ним, сервис-мануалов и т.д.;
- фото и рентген материалы, проведенные проверки и условия их проведения, маркировка ТС и т.д.;
- типовой алгоритм движения ТС и ЭКБ между участками производства работ, сформированный на основе классификатора угроз и организационной структуры конкретной лаборатории.

Добавление к эталону файлов электронных документов. Возможность добавления к ТС и ЭКБ, принятых за эталон, различных файлов (фото/рентгенограмм/видео материалы в распространенных форматах, электронные документы, электронные таблицы). Автоматическое создание миниатюр фото и рентген материалов, для ускорения просмотра и сопоставления ТС и ЭКБ с эталоном. При навигации по каталогу эталонов, пользователю отображаются автоматически созданные миниатюры, оригинал материалов, открываться по отдельному запросу (двойной клик на миниатюре). Размер и качество миниатюры позволяет однозначно идентифицировать ТС и ЭБ с эталоном. Возможность поиска информации в таблицах. Редактирование информации связанной с эталоном.

Доступ к форме редактирования базы эталонов, может быть доступен только определенным пользователям. Механизм отображения информации об эталоне в определенном структурированном виде. Пользователю программы отображаться следующая информация:

- тип;

- производитель;
- наименование;
- модель;
- состав;
- модель ТС, в состав которого оно входит (в случае если входит в состав нескольких ТС, должен отображаться список ТС);
- фото/видео/рентген материалы;
- документы;
- другая хранимая в базе информация.

Возможность индивидуальной настройки отображаемых параметров. При совместной работе с программами «Управление СИСП» и «Рабочее место исполнителя» механизм автоматического отображения пользователю эталона и информации связанной с ним, при выполнении работ с техническими средствами и при выполнении проверок.

Поиск информации по различным параметрам. Поиск информации об эталоне по следующим параметрам:

- по типу;
- по модели;
- по названию;
- по производителю.

Совместная работа пользователей. Возможность многопользовательского режима работы. Количество одновременно работающих пользователей: не менее 1000 пользователей. Пользователи имеют возможность одновременного просмотра информации об эталоне. Совместное внесение изменений, редактирование информации об эталоне, добавление ТС и ЭКБ принятых за эталон не предусматривается. Данные процедуры производятся отдельно назначенными пользователями.

Типовой состав АПК «ПАРНАС-СПБД»:

- серверная часть программы «База эталонов» (сетевой вариант, одно хранилище);

- серверная часть программы «Управление СИСП» (сетевой вариант, интеграция с программой «База Эталонов»);
- программа «Рабочее место исполнителя» (сетевой вариант, интеграция с программами «База Эталонов», «Управление СИСП») в составе: участок специальных проверок, вариант работы с «ВИД ЭП»; участок специальных исследований.

Программа «Рабочее место исполнителя» устанавливается на каждое рабочее место.

Рассмотрим устройство ИКК «Бинафон-н2». Комплекс «БИНАФОН-Н2» предназначен для обнаружения:

- излучения передатчиков информации в ИК-диапазоне;
- акустических и виброакустических каналов утечки информации;
- фактов подключения средств съема информации, передающих сигналы по «слаботочным» (до 60 В) проводным коммуникациям или силовым сетям переменного тока;
- электрических и магнитных полей, излучаемых техническими средствами обработки информации и проводными кабельными линиями;
- эффекта акустоэлектрического преобразования в оконечных устройствах.

«БИНАФОН-Н2» обеспечивает выявление факта передачи информации по указанным выше каналам, прослушивание ее громкоговорителем или головными телефонами и запись контролируемых сигналов на SD карту памяти.

С помощью комплекса может быть осуществлен спектральный анализ сигналов в звуковом и высокочастотном диапазонах, а также демодуляция AM и FM сигналов.

В состав комплекса входят следующие датчики:

- датчики инфракрасного излучения, предназначенные для обнаружения источников излучения в ИК диапазоне от 400 до 2400 нм;

- внешний микрофон на телескопической штанге, позволяющий оценить утечку акустической информации по вентиляционным каналам, имеющимся сквозным щелям, трещинам и нарушениям уплотнителей;
- измеритель звукового давления, предназначенный для оценки ослабления уровня звуковых сигналов при прохождении их через строительные конструкции;
- виброакустический датчик, предназначенный для оценки виброакустических свойства ограждающих конструкций и инженерных коммуникаций;
- магнитная антенна, предназначенная для выявления побочных электромагнитных излучений в звуковом диапазоне частот;
- кабельный усилитель, предназначенный для обнаружения эффекта акустоэлектрического преобразования в оконечных устройствах;
- кабельный управляемый коммутатор «БИНАКОМ», предназначенный для обеспечения гальванической развязки между проводными коммуникациями и основным блоком, ручной и автоматической коммутации контактов входных разъемов, а также для подачи регулируемого напряжения смещения в обследуемые линии.

Состав комплекта:

- основной блок «БИНАФОН-Н2»;
- управляемый коммутатор «БИНАКОМ»;
- внешний микрофон на телескопической штанге;
- магнитная антенна;
- датчики инфракрасного излучения «IR№1», «IR№2»;
- датчик виброакустический;
- измеритель звукового давления «MIC»;
- кабельный усилитель;
- комплект соединительных кабелей;
- головные телефоны;

- внешний источник питания 5 В.

Далее рассмотрим осциллограф «TPS2014B». «TPS2014B» – осциллограф цифровой запоминающий Tektronix – прибор, предназначенный для исследования (наблюдения, записи; измерения) амплитудных и временных параметров электрического сигнала, подаваемого на его вход, либо непосредственно на экране, либо записываемого на фотоленте. Используются в прикладных, лабораторных и научно-исследовательских целях, для контроля/изучения электрических сигналов – как непосредственно, так и получаемых при воздействии различных устройств/сред на датчики, преобразующие эти воздействия в электрический сигнал.

ИК камера «Contour-M». ИК камера CONTOUR-M благодаря возможности регистрировать инфракрасное излучения типа GaAs в широком спектре. Камеру можно рекомендовать для работы с лазерами, ИК излучением и т.д. Встроенный 4-х дюймовый TFT-LCD дисплей разрешением 480x220 пикселей, что в сочетании с камерой на основе кремневого датчика с увеличенной чувствительности ИК излучения от 400 до 1700 нм, микролинзами и системой устранения помех гарантируют получение высокоточного и четкого изображения. Стандартный видеовыход позволяет выводить изображение на внешние устройства. Также возможна установка камеры на штатив. Питание камеры может осуществляться не только от сети с постоянным напряжением 12В, но и от 4-х аккумуляторов типа АА в отдельном отсеке.

Особенности:

- широкая область применения;
- встроенный 4-х дюймовый TFT-LCD дисплей;
- диапазон обнаружения ИК излучения от 400 до 1700 нм;
- видеовыход;
- питание от сети 12В или 4-х батарей типа АА;

- возможна установка на штатив.

Приблизительная чувствительность на расстоянии 20 см:

- 500 мВт/см2 при 1310 нм;
- 20-50 мВт/см2 при 1550 нм;
- 80-100 мВт/см2 при 1700 нм.

Дополнительные аксессуары:

- объектив 2Х, ИК светофильтр, дистанционное кольцо;
- нейтральный светофильтр 100Х;
- адаптер к микроскопу;
- диафрагма к объективу 1Х.

Для метода АКЦП используем аппаратуру «Крокус». Аппаратно-программный комплекс «Крокус-КЦП» предназначен для проведения комплексных радиотехнических исследований с целью регистрации уровня низкочастотных электрических наводок в цепях электропитания функционирующих технических средств при воздействии на них тестовым акустическим сигналом и модулированным радиосигналом, а также регистрации модулированных сигналов в эфире при воздействии на техническое средство совокупностью гармонического радиосигнала и тестового акустического сигнала. Регистрация сигналов производится во вторичных (низковольтных) цепях электропитания технического средства, и в цепях первичного электропитания (220В, 50 Гц).

Таблица 2.4 – Технические характеристики «Крокус-КЦП»

Рабочий диапазон входных напряжений АНС	3 В – 60 В
Предельное входное переменное (50 Гц) напряжение АНС с сетевым адаптером, не менее	231 В
Напряжение пробоя гальванической развязки входов АНС, не менее	1500 В
Проходная емкость гальванической развязки входов АНС, не более	20 пФ
Динамический диапазон АНС без учета диапазона переключаемого предусилителя	120 дБ
Частота дискретизации АЦП в АНС	192 кГц
Разрядность оцифровки сигнала в АНС	24 бит
Чувствительность к входным сигналам, не хуже	100 нВ

Рабочий диапазон частот анализа сигналов	100 Гц - 96 кГц
Максимальная разрешающая способность анализа сигналов в частотном диапазоне, не хуже	0,1 Гц
Тип интерфейса дистанционного управления АНС	Ethernet-100 МБ
Электропитание АНС	220 В/50 Гц, не более 25 Вт
Габаритные размеры АНС	355х265х205 мм
Масса АНС	5 кг

Рассмотрим аппаратуру для проведения рентгенографического контроля «Норка». Изделие «Норка» предназначено для обнаружения элементов взрывных устройств, оружия, скрытно установленных средств негласного съема информации в отдельных предметах, посылках, мебели, багаже и т.д., а также контейнеров с опасными вложениями: отравляющими, раздражающими и радиоактивными веществами.

Основные особенности:

- исключительное удобство в работе;
- высокая производительность при хорошей выявляющей способности;
- слабое воздействие на окружающих и обслуживающий персонал;
- наличие у прибора компьютерной памяти, позволяющей записать теневое изображение, получаемое при просвечивании объекта, и использовать его в дальнейшей работе в качестве справочного материала;
- применение так называемых микрофокусных рентгеновских излучателей, позволяющих непосредственно во время просвечивания получить теневое изображение, увеличенное в 4-12 раз без потери его качества.

При создании рентгенотелевизионной установки «Норка» использован модульный принцип построения. В состав комплекта могут входить различные излучатели, преобразователи и блоки управления. По желанию заказчика можно подобрать конфигурацию системы, наилучшим образом отвечающую его требованиям.

Для сборки оборудования и разборки используем набор инструментов «Марс СП»:

- набор отверток электроизолированных –1 комплект;
- набор отверток для электроники – 1 комплект;
- набор отверток с удлиненным жалом – 1 комплект;
- магнитный подъемник (гибкий) – 1 шт;
- набор торцевых ключей со сменными головками – 1 комплект;
- набор Г-образных ключей – 1 комплект;
- универсальный переставной ключ – 1 шт;
- инструмент для удаления изоляции – 1 шт;
- длинногубцы с резцом– 1 шт;
- бокорез – 1 шт;
- силовые пассатижи – 1 шт;
- фонарь – 1 шт;
- маркер по металлу – 1 шт;
- паяльник – 1 шт;
- припой в виде оловянной проволоки с канифолью на катушке – 1 шт;
- мультиметр цифровой – 1 шт;
- индикаторная отвертка (пробник фазы) – 1 шт;
- рулетка металлическая – 1 шт;
- набор надфилей – 1 комплект;
- металлоискатель – 1 шт;
- молоток слесарный – 1 шт;
- пассатижи-трансформер – 1 шт;
- набор пинцетов – 1 комплект;
- набор зажимов – 1 комплект;
- зеркало малое с рукоятью – 1 шт;
- скальпель хирургический – 1 шт;
- комплект сумок для набора инструментов – 1 комплект;

Далее рассмотрим комплекс «СИРИУС». «СИРИУС» – комплекс для анализа сигналов в проводных линиях. Предназначен для обнаружения и анализа сигналов в проводных линиях и в подключенных к ним электронных устройствах, возникающих как за счет прямого формирования, так и путем акустоэлектрических преобразований. Исследование сигналов производится методами векторного спектрального анализа и анализа модулирующих сигналов с использованием метода ВЧ-навязывания [17].

Состав комплекта: основной блок; комплект соединительных кабелей и переходников; активная акустическая система «ПРИБОЙ»; имитатор параметрического микрофона; высокочастотный отсекающий фильтр; коммутатор входных сигналов; наушники.

Общие характеристики основного блока:

- напряжение питания от сети переменного тока – 100-240 В;
- потребляемая мощность – 100 Вт;
- габариты основного блока – 474х415х149 мм;
- вес основного блока – 12 кг.

2.8 Анализ современных схемотехнических и конструктивно технических принципов построения технических средств иностранного производства

В настоящее время актуальным является внедрение беспроводных технологий в различные сферы деятельности. Представляет интерес сравнение беспроводных технологий Wi-Fi и Li-Fi для расширения областей их применения. Wi-Fi – это беспроводная технология передачи данных по радиоканалу. Принцип действия Wi-Fi заключается в следующем. Адаптер Wi-Fi преобразует поток данных в электрический радиосигнал и передает его через антенну. Маршрутизатор, в свою очередь, получает радиосигнал и дешифрует его, отправляет данные с помощью физических, проводных соединений. Преобразование сигнала может происходить и в обратном направлении. Маршрутизатор получает информацию из интернета и переводит его в радиосигнал, который затем передается беспроводным

адаптером компьютера. Для работы Wi-Fi необходимо соответствующее оборудование беспроводной связи. Все оборудование делится на две группы: «точка доступа» и беспроводной роутер. Li-Fi - это современная беспроводная технология передачи данных с помощью света. Li-Fi состоит из четырех главных компонентов: светодиодной лампы, радиочастотного усилителя мощности, печатной платы и корпуса. Печатная плата управляет электрическими входами и выходами лампы микроконтроллера и используется для управления различных функций лампы. Радиочастотный сигнал генерируется в радиочастотном усилителе мощности и направляется в электрическое поле лампы. Высокая концентрация энергии в электрическом поле испаряет содержимое колбы в состояние плазмы в центре лампы, плазма формирует интенсивный источник света. Все они содержатся в алюминиевом корпусе. Принцип работы Li-Fi заключается в изменении параметров свечения светодиодных ламп с очень высокой скоростью, который не заметен человеческому глазу. Процессом управляет специальный микрочип, кодирующий информацию. Особый фотодетектор регистрирует световые пучки и осуществляет обратное преобразование данных. Вместо модемов в Li-Fi используется приемопередатчик, оборудованный в светодиодных лампах, которые могут передавать и принимать информацию и при этом использоваться для освещения комнаты. Светодиодные лампы являются точкой доступа для любого количества пользователей.

В настоящее время скорость передачи по данной технологии составляет 10Гбит/с, в лабораторных условиях уже достигла 15Гбит/с [3]. Но поток данных можно прервать любым препятствием (даже листом бумаги). Этот недостаток может считаться преимуществом, если вы не хотите, чтобы вашей сетью передачи данных пользовались посторонние. В таблицах 2.5 и 2.6 приведены сравнительные характеристики рассматриваемых технологий.

Таблица 2.5 – Сравнительный анализ технологий Wi-Fi и Li-Fi

Технологии	Режимы работы (частота)	Скорость передачи данных
Технология Wi-Fi	2,4 ГГц	11-300Мбит/с
Технология Li-Fi	100 МГц	10 Гбит/с

Таблица 2.6 – Преимущества и недостатки технологий Wi-Fi и Li-Fi

№	Технологии	Преимущества	Недостатки	Общие признаки
1	2	3	4	5
1	Технология Wi-Fi	сеть без прокладывания кабеля	работа на частоте 2,4 ГГц	сети удаленного доступа
		доступ к сети любых устройств	небольшая электромагнитная компонента вместимости	приемопередающий модуль

Продолжение таблицы 2.6

№	Технологии	Преимущества	Недостатки	Общие признаки
		удобство использования (свободное перемещение потребителя, создание групп пользователей)	низкая надежность	
2	Технология Li-Fi	дешевые комплектующие	передача данных может осуществляться только в пределах прямой видимости	
		доступ радиосвязи под водой и в полете		
		безопасное воздействие на здоровье человека		
		информационная безопасность		

По словам создателя технологии Li-Fi Харальда Хааса в скором времени скорость передачи информации достигнет более 100 Гбит/с и полностью вытеснит технологию Wi-Fi

3 Проектирование подвижной испытательной лаборатории

3.1 Требования к стенду рентгенографического неразрушающего контроля

Переносные рентгеновские установки применяются для просвечивания предметов, назначение которых не удается выявить без их разборки, прежде всего, тогда, когда разборка невозможна без разрушения найденного предмета.

Для использования в лаборатории была выбрана портативная переносная рентгентелевизионная установка с острофокусным излучателем «Норка-XL».

Основные достоинства:

- быстрое развертывание на месте обследования;
- исключительная оперативность в работе;
- высокая производительность;
- хорошая выявляющая способность;
- исключение «мокрого» фотографического процесса, связанного с обработкой рентгеновских фотопленок;
- возможность записи теневых изображений, получаемых в результате просвечивания, в электронную память прибора для последующего анализа и обработки;
- возможность работы от аккумуляторной батареи.

Микрофокусные излучатели «РИ» позволяют выявлять в контролируемых предметах проводники толщиной 20 мкм (например, провода детонатора). Основным преимуществом таких излучателей, по сравнению с импульсными и сильноточными серии «РАП», является возможность получения геометрического увеличения контролируемого объекта в несколько раз, без ухудшения качества изображения. Программное обеспечение позволяет получать псевдоцветные изображения, производить цифровое улучшение изображений, архивирование рентгентелевизионных

изображений, представлять изображения в негативе и позитиве, вносить речевые комментарии.

Установка комплектуется высокочувствительным блоком телекамеры, который устанавливается на один из трех сменных преобразователей.

Выбор конкретного преобразователя обуславливается габаритами контролируемого объекта и требуемым пространственным разрешением. В комплект поставки могут входить один, два, либо несколько преобразователей.

В установке «НОРКА-XL» может быть реализован метод двуэнергетической цифровой радиографии (дуальной энергии), с помощью которого возможно классифицировать содержание исследуемых объектов с определением принадлежности к классам «металл»-»не металл», с указанием относительной толщины материалов.

Состав установки:

- «РИ»-микрофокусный рентгеновский излучатель с переменным анодным напряжением (возможна поставка с сильноточным аппаратом серии РАП);
- «БУ»-блок управления и обработки изображений;
- «ПР»-сменный преобразователь;
- «СКБ»-сменный камерный блок;
- сетевой блок питания;
- аккумуляторный блок питания в комплекте с зарядным устройством;
- комплект соединительных кабелей;
- транспортные сумки либо кейс.

Состав комплекта «НОРКА-XL»:

- «БУ-4» – Блок управления LCD-12»;
- «РИ-150М» – Рентгеновский излучатель острофокусный 150 кэВ;

- «СКБ-3Д» – Цифровой сменный камерный блок (1280х1024 пикселей, 12 бит);
- «ПР-5» – Конвертер 400х300 мм;
- «БАП-2/ЗУ» – Аккумуляторный блок питания в комплекте с зарядным устройством;
- комплект транспортных сумок.

Аппараты для рентгеновской дефектоскопии имеют в своем составе рентгеновскую трубку, являющуюся интенсивным источником рентгеновского излучения, представляющего потенциальную опасность для здоровья людей. Кроме того, опасными и вредными факторами при эксплуатации аппаратов могут являться высокое напряжение, а также озон и окислы азота, образующиеся в результате радиолиза воздуха под действием рентгеновского излучения.

Рентгеновская трубка становится источником излучения лишь в момент подачи на нее высокого напряжения. Поэтому при перевозке и хранении аппараты не представляют радиационной опасности и не требуют принятия специальных мер защиты.

По способу использования аппараты делятся на стационарные, переносные и передвижные.

Стационарные аппараты используются в стационарных условиях дефектоскопических лабораторий в специальных защитных камерах, исключающих доступ людей внутрь камеры при работе аппарата и обеспечивающих радиационную защиту персонала, находящегося вне камеры.

Переносные дефектоскопы выполняются в носимом исполнении и не имеют радиационной защиты. Они могут быть оснащены специальными коллиматорами (диафрагмами, тубусами), формирующими направленный расходящийся пучок излучения в виде конуса с заданным углом раствора для фронтального просвечивания, либо кольцевой расходящийся пучок

излучения с заданным углом раствора для панорамного просвечивания. Радиационная защита персонала при работе аппарата обеспечивается удалением его от рентгеновского излучателя на безопасное расстояние.

Передвижные дефектоскопы монтируются на транспортных средствах и могут перемещаться вместе с ними. Они могут быть оснащены защитными экранами и коллиматорами, обеспечивающими уменьшение размеров радиационно-опасной зоны, возникающей при работе аппарата. Радиационная защита персонала при работе аппарата обеспечивается удалением его от рентгеновского излучателя на безопасное расстояние либо использованием специальной радиационной защиты рабочего места оператора.

Как переносные, так и передвижные аппараты могут использоваться в производственных помещениях, на открытых площадках и в полевых условиях.

К использованию на территории Российской Федерации допускаются аппараты, в том числе и импортные, имеющие санитарно-эпидемиологическое заключение федерального органа Госсанэпиднадзора о соответствии требованиям санитарных правил.

Получение, хранение аппаратов и проведение работ с ними осуществляется при наличии санитарно-эпидемиологического заключения о соответствии условий работы с источниками излучения санитарным правилам.

К работам с аппаратами допускаются лица не моложе 18 лет, имеющие специальную подготовку, отнесенные к персоналу группы А, прошедшие медицинский осмотр и не имеющие медицинских противопоказаний.

К самостоятельным работам по монтажу и ремонту аппаратов допускаются лица, окончившие специальные курсы, дающие право на выполнение такого рода работ, или имеющие стаж работы с аппаратами данного типа не менее 3-5 лет.

На основании типовых инструкций по радиационной безопасности и с учетом особенностей проведения рентгеновской дефектоскопии разрабатывает и утверждает детальные инструкции по радиационной безопасности, регламентирующие порядок проведения рентгенодефектоскопических работ. При любом изменении условий работы в утвержденные инструкции вносятся необходимые поправки и дополнения.

До начала проведения работ по рентгеновской дефектоскопии администрация организует обучение персонала безопасным методам работы и назначает лицо, ответственное за учет и хранение аппаратов.

Лица, временно привлекаемые к проведению рентгено-дефектоскопических работ, проходят обучение безопасным методам работы и инструктаж.

Для постоянного контроля за состоянием аппаратов администрация организации назначает специально подготовленного специалиста.

Поступившие в учреждение аппараты регистрируются в приходно-расходном журнале.

Выдача переносных и передвижных аппаратов из мест постоянного хранения для проведения работ на объектах производится лицом, ответственным за учет и хранение аппаратов, по письменному разрешению руководства организации. Выдача и возврат аппаратов регистрируются в журнале выдачи переносных аппаратов.

Обо всех нарушениях в работе аппаратов персонал немедленно сообщает лицу, ответственному за радиационную безопасность

При проведении контроля изделий микроэлектроники экономически целесообразно использовать установки с местной защитой имеющие санитарно-эпидемиологическое заключение и обеспечивающие безопасную работу персонала, что значительно снижает стоимость оборудования лаборатории.

Для сокращения времени необходимого для получения результатов контроля целесообразно укомплектовать лабораторию комплектом

оборудования необходимого для расшифровки рентгеновских снимков (негатоскопы, денситометры, измерительные лупы, средства автоматизации процесса расшифровки).

Производственный контроль за радиационной безопасностью в организации, в зависимости от объема и характера проводимых работ с источниками ионизирующего излучения, осуществляется специальной службой или лицом, ответственным за радиационную безопасность, прошедшим специальную подготовку.

При проведении рентгеновской дефектоскопии с использованием переносных дефектоскопов в производственных помещениях (цехах), на открытых площадках и в полевых условиях должны устанавливаться размеры радиационно-опасной зоны.

Радиационно-опасная зона ограждается и маркируется предупреждающими плакатами (надписями), отчетливо видимыми с расстояния не менее 3-х метров.

Для ограждения радиационно-опасной зоны должны использоваться стандартные металлические стойки, на которых навешивается шнур, либо другие виды четко видимых ограждений.

По возможности, просвечивание в производственных помещениях рекомендуется проводить в нерабочее время.

Работы по просвечиванию в производственных помещениях, на открытых площадках и в полевых условиях должны выполняются двумя работниками. Один из них наблюдает за отсутствием посторонних лиц в радиационно-опасной зоне.

При просвечивании персонал располагается в безопасном месте (на безопасном расстоянии от места просвечивания или за защитным устройством), обеспечивающем выполнение требования по ограничению годовых доз облучения персонала.

Для обеспечения радиационной безопасности персонала при проведении работ с переносными аппаратами необходимо:

- просвечивать изделия при минимально возможном угле расхождения рабочего пучка рентгеновского излучения, используя для этого входящие в комплект аппаратов коллиматоры, диафрагмы или тубусы;
- в случае необходимости устанавливать за просвечиваемым изделием защитный экран, перекрывающий прошедший пучок излучения;
- пучок излучения направлять в сторону от рабочих мест и мест, где могут появляться люди, по возможности в толстую стену или иное массивное препятствие;
- уменьшать время просвечивания изделий за счет использования высокочувствительных пленок, усиливающих экранов;
- пульт управления переносных аппаратов размещать на таком расстоянии от рентгеновского излучателя, которое обеспечивает безопасные условия труда персонала, но не менее 15 метров. При невозможности выполнения этого условия использовать специальные защитные экраны либо оснащать аппараты средствами автоматической задержки включения, дающими возможность персоналу отойти в безопасное место.

Во время проведения работ по рентгеновской дефектоскопии оператору запрещается оставлять без присмотра пульт управления аппарата.

3.2 Методика выявления устройств негласного съема информации

В зависимости от целей, задач и используемых средств при работе проектируемой испытательной лаборатории можно выделить следующие виды специальных проверок:

- специальное обследование выделенного помещения;
- визуальный осмотр выделенного помещения;
- комплексная специальная проверка помещения;
- визуальный осмотр и специальная проверка новых предметов (подарков, предметов интерьера, бытовых приборов) и мебели, размещаемых или устанавливаемых в выделенном помещении;

- специальная проверка радиоэлектронной аппаратуры, устанавливаемой в выделенном помещении;
- периодический радиоконтроль (радиомониторинг) выделенного помещения;
- постоянный (непрерывный) радиоконтроль помещения;
- специальные проверки проводных линий;
- проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем прохождения всех вызывных сигналов АТС.

Периодичность и виды проверок помещений с целью выявления в них закладных устройств зависят от степени важности помещений и порядка допуска в них посторонних лиц.

Специальное обследование и визуальный осмотр выделенного помещения проводятся без применения технических средств. Остальные же виды проверок требуют использования тех или иных специальных средств контроля.

Специальные обследования помещений проводятся после окончания строительства объекта или после проведения капитального ремонта в них, а также периодически. Для проведения специальных обследований должны привлекаться соответствующие специалисты.

С целью обнаружения звукозаписывающей и видеозаписывающей аппаратуры, а также радиозакладок может проводиться досмотр и специальная проверка посетителей и их вещей.

Специальная проверка радиоэлектронной аппаратуры, в том числе ПЭВМ и телефонных аппаратов, проводится после их закупки или ремонта. Для проведения проверки применяются рентгеновские комплексы, радиоизмерительная техника и специальные программно-аппаратные комплексы контроля.

Специальная проверка проводных линий осуществляется после окончания строительства объекта или после проведения его капитального

ремонта, а также периодически с целью обнаружения несанкционированных подключений к линиям средств съема информации. Для проведения проверки должны привлекаться соответствующие специалисты.

Радиоконтроль выделенных помещений проводится с целью обнаружения активных радиозакладок с использованием сканерных приемников или программно-аппаратных комплексов контроля. Он организуется периодически при проведении наиболее важных мероприятий (совещаний, заседаний) или непрерывно (постоянно). При этом средства контроля могут располагаться вне контролируемых помещений.

Тестовый «прозвон» телефонных аппаратов проводится при установке нового телефонного аппарата или телефонного аппарата после ремонта, а также периодически. «Прозвон» необходимо проводить с радиотелефона или телефонного аппарата, установленного в другом помещении. При наборе номера проверяемого телефонного аппарата осуществляется контроль (на слух) прохождения всех вызывных сигналов АТС.

Если обнаружено подавление (непрохождение) одного-двух вызывных звонков у контролируемого телефонного аппарата, то возможно, что в его корпусе или телефонной линии установлено закладное устройство и необходимо проводить специальную проверку телефонной линии и телефонного аппарата.

Комплексная специальная проверка помещений проводится после окончания строительства объекта или после проведения капитального ремонта в них, при проведении аттестации помещений, а также периодически. Это наиболее полный вид проверки. Для проведения таких специальных проверок используется весь арсенал технических средств контроля.

Обследование объектов информатизации проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств и систем требованиям по защите информации.

Таким образом, используя выше перечисленное оборудование, можно исследовать защищенное помещение на предмет наличия в нем несанкционированных радиопередающих устройств, любых посторонних радиоэлектронных устройств, а также фактов ВЧ-навязывания по проводным линиям, которые имеются в помещении.

Однако, кроме технической составляющей, обследование защищенных помещений имеет и организационную составляющую, так как очень важно даже после нахождения и устранения закладных устройств не позволить установить их вновь. Для этого необходимо соблюдать некоторые требования по обеспечению ограниченного доступа к защищаемым помещениям и сохранения тайны итогов поиска закладных устройств.

В ходе обследования проверяется:

- соблюдение организационно-режимных требований и установленных требований по звукоизоляции защищаемых помещений;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- наличие электробытовой, радио и телевизионной аппаратуры и устройств иностранного и непромышленного изготовления (пультов связи, устройств вызова и оповещения, усилителей, генераторов и других вспомогательных технических средств и систем), которые могут способствовать возникновению каналов утечки информации;
- выполнение требований предписаний на эксплуатацию на основные технические средства и системы по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;
- соответствие выполняемых на объекте информатизации мероприятий по защите информации данным, изложенным в техническом паспорте;

- выполнение требований по защите автоматизированных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите автоматизированных систем и средств вычислительной техники.

Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы;
- вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;
- проверить качество установки стеклопакетов оконных приемов;
- провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры).

Выше были рассмотрены основные разновидности закладных устройств. Очевидно, что для наиболее результативного поиска и полного обнаружения таких устройств необходимо применять комплекс средств, охватывающих все виды несанкционированных устройств, а также косвенные признаки их присутствия.

Такими признаками могут быть:

- электромагнитное излучение;
- физическое изменение размеров устройств приборов и устройств;

- изменение проводимости звука стен, столов, потолков и других поверхностей;
- изменение режимов работы различных устройств (к примеру, телефонов);
- посторонние провода питания или элементы радиоэлектронной аппаратуры.

Следовательно, для организации полноценного комплекса поисковых мероприятий в защищенных помещениях необходимо использовать устройства, которые могли бы оценивать и обеспечивать следующие факторы:

- наличие радиоэлектронных элементов в тех конструкциях, в которых их не должно быть;
- физическое (визуальное) обнаружение закладных устройств;
- посторонние излучения в проводных линиях;
- посторонние излучения в ИК-диапазоне;
- посторонние видеоустройства.

Кроме того, поиск активных радиоустройств необходимо осуществлять в диапазоне 33-2000 МГц, поиск радиоэлектронных устройств – в диапазоне 30-2500 МГц, поиск видеокамер на расстоянии не более 1,5 метра от места предполагаемого расположения, также обязательно необходимо использовать средства визуализации посторонних предметов.

Обнаружение РЗУ по излучению радиопередатчика решается известными методиками. Проблема возникла с переходом РЗУ в режим радиомолчания, например в случаях:

- обнаружения сигналов нелинейного радиолокатора поисковой группы;
- по сигналу телеуправления от потребителя;
- в случае разряда источника питания.

Основными признаками радиоприемника РЗУ являются трансформации зондирующего сигнала:

– затягивание длительности;

– уширение спектра сигнала;

– появление кратных гармоник резонансной частоте;

– фазовые сдвиги и др.

Всего обнаружено около двух десятков демаскирующих признаков и их комбинаций, однако перечисленные могут быть прогнозируемы. Методы обнаружения классифицируются по режимам работы поисковой аппаратуры на импульсные, непрерывные и комбинированные. Методика поиска радиоприемника приведена на рисунке 3.1.

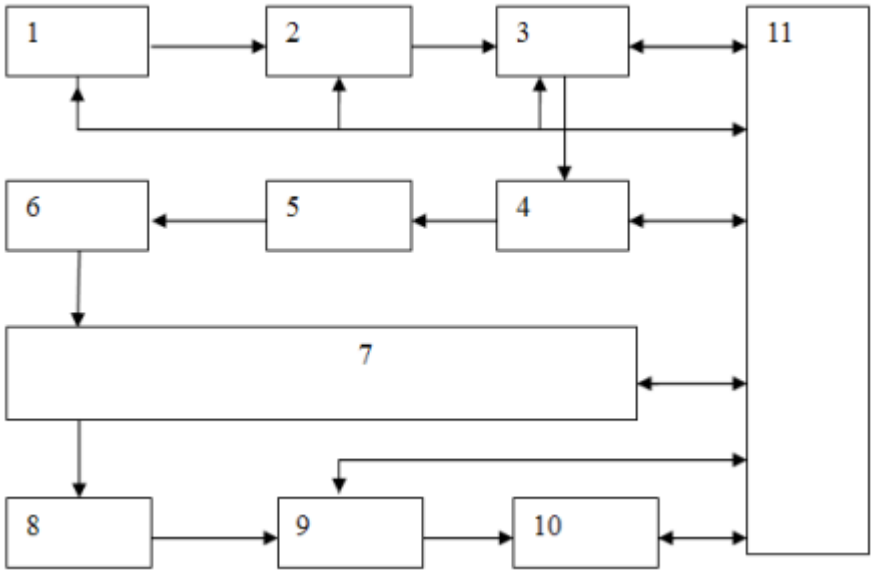

Рисунок 3.1 Методика поиска радиоприемника

На рисунке обозначены:

1 – анализ тактической и технической задачи поиска;

2 – прогнозирование ситуации и демаскирующих признаков;

3 – оценки степени угрозы наличия защитников РЗУ;

4 – результаты предварительного мониторинга (характеристики паспорта объекта);

5 – разработка альтернативных решений по проведению поискового мероприятия;

6 – согласование сил и средств для основной, обеспечивающей и контрольной функций;

7 – принятие решения о последовательности поиска, принятых мер безопасности и условий его приостановки или завершения;

8 – доведение решения до исполнителей;

9 – проведение поисковых мероприятий и документирование процессов и результатов;

10 – завершение поисковых мероприятий, анализ результатов с оценкой степени достижения требуемого результата, корректура основных элементов данной методики и значений демаскирующих признаков найденного приемника;

11 – база данных.

Упрощенное имитационное моделирование поиска позволило определить значимость демаскирующих признаков, которые расположились в следующей последовательности:

– затягивание эхо-сигнала;

– появление кратных гармоник резонансной частоты антенны;

– появление фазовых сдвигов;

– уменьшение интервала раскорреляции.

Применение четвертого и других признаков связаны с затратами, которые определяются ограниченностью поисковых аппаратно-программных средств. Поэтому наличие первых двух признаков позволяют гарантировать обнаружение. Появление еще и третьего демаскирующего признака характеризуют повышенную опасность и требует корректуры методики и проведение доразведки. Предлагаемая методика поиска радиоприемного устройства может иметь рекомендательный характер и адаптироваться по условия и ограничения реальной ситуации. Интересным является вариант применения доразведочных мероприятий с определением параметров и прогнозированием типа радиоприемного устройства. В случае применения приемника, построенного по супергетеродинному принципу, появляется

возможность поиска его обнаружения по сигналу излучения гетеродина. В этом случае методика поиска частично меняется и предусматривает прогнозирование возможных частот излучения РЗУ в активном режиме и частоты гетеродина. Для этого могут использоваться и непрерывный, и импульсный режимы. Эффективность их примерно одинакова, отличие заключается в используемых демаскирующих признаках, при этом применение непрерывного метода считается более безопасным. В дальнейшем поиск ведется в ближней зоне, поэтому обнаружение предусматривает определение местоположения другими методами.

Для работы с детектором электромагнитного поля «PROTECT 1203», необходимо при помощи отвертки в нижней части прибора открыть крышку батарейного отсека и соблюдая полярность, установить либо заменить любые батареи размера AAA или аккумуляторы, затем закрыть крышку. Установить в зависимости от условий стандартную или City антенну, закрутив ее по часовой стрелке до упора на задней части панели детектора. Включить прибор нажатием на передней части панели кнопку питания, слева от кнопки загорится светодиод, означающий работу устройства. Откручивание антенны при включенном приборе запрещается.

Перед тем, как войти в защищаемое помещение необходимо включить детектор поля «PROTECT 1203» и ориентируясь на показание шкалы индикатора настроить чувствительность таким образом, чтобы шкала показывала один сегмент или ничего, тогда все новые излучения будут обнаружены. При проведении лабораторной работы детектор поля необходимо перемещать в непосредственной близости от исследуемых предметов на расстоянии 0,1-0,5 м, обследуя помещение на предмет поиска «радиозакладки».

При приближении к передатчику уровень на индикаторе начинает расти. Если уровень сигнала очень большой следует уменьшить чувствительность до 1 сегмента. Чем ближе передатчик к антенне, тем

уровень выше. Когда уровень индикатора доходит до последних 3-х красных сегментов, прибор начинает вибрировать.

Важно не превышать максимально допустимый уровень входного сигнала. Никогда не подносить прибор слишком близко к антенне передатчика (особенно к радиостанциям мощностью 1-5 Вт) во избежание повреждения (сгорания) прибора. Если высокий уровень сегмента наблюдается в большей части помещения, следует использовать другую (городскую) антенну вместо стандартной длинной антенны. Данная антенна позволит избежать влияния помех от внешних источников в городах или вблизи вышек радиовещаний.

Для работы с частотомером «Roger RFM-32» необходимо слева на верхней панели прибора подсоединить в разъем телескопическую антенну и по часовой стрелке закрутить. При использовании антенны, частотомер будет иметь максимальную чувствительность при минимальной ее длине в диапазоне 450 МГц, выдвинутой наполовину в диапазоне 150 МГц и полностью выдвинутой в диапазоне 27-50 МГц. Для включения прибора нужно переключить «POWER» на «ON», загорится светодиод и раздастся звуковой сигнал.

При поиске источников сигнала в защищаемом помещении на индикаторе частотомера могут появляться случайные показания. Это происходит вследствие высокой чувствительности входного усилителя, который усиливает шум до значения, достаточного для счета.

Важно не превышать максимально допустимый уровень входного сигнала. В случае отсутствии сигнала необходимо включить фильтр хаотичных показаний индикатора нажатием переключателя «FILTER». Переключение ««RANGE» позволит произвести измерения в диапазоне частот 1-300 МГц или 10-3000 МГц. Для более точного измерения необходимо нажать кнопку «GATE» – переключение времени счета. Чем больше время счета, тем выше будет точность измерения.

Режим Авто-Захвата включается кнопкой «FUNCTION». В этом режиме, при обнаружении сигнала фиксируется значение частоты и раздается прерывистый звуковой сигнал.

В области обнаружения детектором поля многочисленного роста числа сегментов, частотомером определен четкий уровень сигнала.

Кнопка «FUNCTION» также служит для переключения между режимами из частоты, периода и режимом Авто-сигнала. Поэтому, если переключится из режима частоты в режим периода можно определить период повторений сигнала частоты.

Для продолжения поиска и измерения частоты зафиксированное значение нужно сбросить кнопкой «HOLD». Значение частоты обнаруженного сигнала отметить на схеме исследуемого объекта. По завершению поиска выключить прибор, переключив «POWER» на «OFF».

Прежде чем начать поиск необходимо выполнить ряд действий. Во-первых, необходимо правильно выбрать время поиска и создать подходящие условия. Существуют устройства, включаемые и выключаемые дистанционно, поэтому необходимо приложить все усилия для создания видимости реальной рабочей ситуации. Вы должны позаботиться о «звуковом сопровождении» поисковых мероприятий. Под «звуковым сопровождением» подразумевается проигрывание во время поисковых мероприятий музыкальных композиций. «Звуковое сопровождение» выполняет следующие функции:

- активизирует передатчики, активизируемые голосом;
- маскирует поисковые мероприятия.

Поиск в помещениях:

- закройте все окна и шторы в помещении. Включите освещение и офисное оборудование для создания обычных условий работы. Прежде чем входить в проверяемое помещение включите прибор. Настройте чувствительность прибора. Для этого вращайте ручку настройки до тех пор, пока не будет светиться или мигать только один сегмент на светоиндикаторе.

Если во время поиска Вы не хотите, или не имеете возможности наблюдать уровень РП при помощи светоиндикатора, Вы можете установить чувствительность, при которой горят все зеленые сегменты. В этом случае, если Вы приблизитесь к источнику излучения, загорятся красные сегменты и включиться встроенный вибратор. Ниже приведен один из возможных алгоритмов поиска:

- войдите в проверяемое помещение, держа Protect 1203 вертикально и наблюдая показания светоиндикатора. Включите и выключите свет, офисное оборудование и прочие электроприборы;
- наблюдайте изменения показаний прибора. Если они меняются синхронно с включением/выключением какого-либо оборудования, то это сигнал о возможном наличии в этом приборе устройства несанкционированного съема информации;
- обойдите всю комнату, наблюдая показания прибора. При приближении/удалении к источнику излучения будет соответственно увеличиваться/уменьшаться показываемый уровень излучения;
- определите места с наибольшим уровнем излучения перемещая прибор во всевозможных направлениях и наблюдая показания светоиндикатора;
- проверьте все объекты, которые могут содержать скрытые устройства негласного съема информации. Сигналом об обнаружении подобного рода передатчиков является опять-таки изменения показаний светового индикатора;
- пытайтесь точно определить местонахождение источника нелегального излучения. Для этого уменьшите до минимума чувствительность прибора. Если антенна выдвинута не полностью, то уровень РП, отображаемый на световом индикаторе, не будет зависеть от взаимного расположения антенны и передатчика, и Вы будете наблюдать постоянный уровень излучения вблизи передатчика. Иногда светоиндикатор

может показать увеличение уровня РП вблизи проводов или металлических объектов. Это связано с тем, что металлические объекты выступают как «продолжение» антенны и такие ситуации не обязательно сигнализируют о наличии передатчика;

– после определения точного местонахождения источника излучения приступайте к физическому поиску.

Произведите визуальный осмотр и проверку с помощью PROTECT 1203 каждого объекта, находящегося в «опасной» зоне. Разберите, если это возможно, осветительные приборы, телефоны, розетки питания, телефонные розетки и т.п. Очень тщательно осмотрите телефонные линии и линии 220 В. Просмотрите все книги, содержимое столов.

3.3 Описание выбранного автомобиля и размещение оборудования в нем

В качестве базового транспортного средства для разработки подъемного устройства выберем автобус категории М2 отечественного производства, а именно 13-местный ГАЗ-32213, который в ряду в ряду «ГАЗелей-автобусов» является наиболее вместительным. Годы эксплуатации «ГАЗелей» в режиме работы «на износ», который типичен для маршрутных автобусов, являются веским доказательством выносливости и неприхотливости этих автомобилей.

Немаловажно, что салон всех вариантов микроавтобусов оснащен дополнительным отопителем. Для обеспечения комфортного микроклимата в теплое время года боковые окна автобусов имеют сдвижные стекла. Стандартно устанавливается и люк в крыше.

Как и любая другая модель семейства «ГАЗель», микроавтобусы имеют полноприводные модификации.

Рисунок 3.2 ГАЗ-32213

Основные характеристики автобуса приведены в таблице 3.1.

Таблица 3.1 – Основные характеристики Газ-322113

Габаритные размеры	Показатели
Длина, мм	5540
Ширина, мм	2380
Высота, мм	2274
Колесная база, мм	2900
Колея передних/задних колес, мм	1700 / 1560
Масса автомобиля, кг	
Снаряженная	2340
Полная	3500
Коробка передач	Пятиступенчатая механическая
Подвеска колес	
Передняя	Зависимая, на двух продольных полуэллиптических рессорах с гидравлическими телескопическими амортизаторами
Задняя	Зависимая, на двух продольных полуэллиптических рессорах с дополнительными рессорами, со стабилизатором поперечной устойчивости (по заказу), с гидравлическими телескопическими амортизаторами
Тормоза	
Рабочая тормозная система	Двухконтурная со схемой разделения перед-зад, с гидравлическим приводом и вакуумным усилителем
Передние	Дисковые
Задние	Барабанные

Характеристики двигателя ЗМЗ-40522 приведены в таблице 3.2.

Таблица 3.2 – Характеристики двигателя ЗМЗ-40522

4-цилиндровый, рядный, бензиновый с распределенным впрыском топлива, 4-тактный, 16-клапанный	
Система зажигания	микропроцессорная
Рабочий объем, л	2.46
Степень сжатия	9,3
Мощность брутто, л.с. (кВт) / об/мин	152 (111,8) / 5200
Максимальный крутящий момент брутто, кГс*м (Н*м) / об/мин	21,5(210,9) / 4000
Топливо	Аи-92

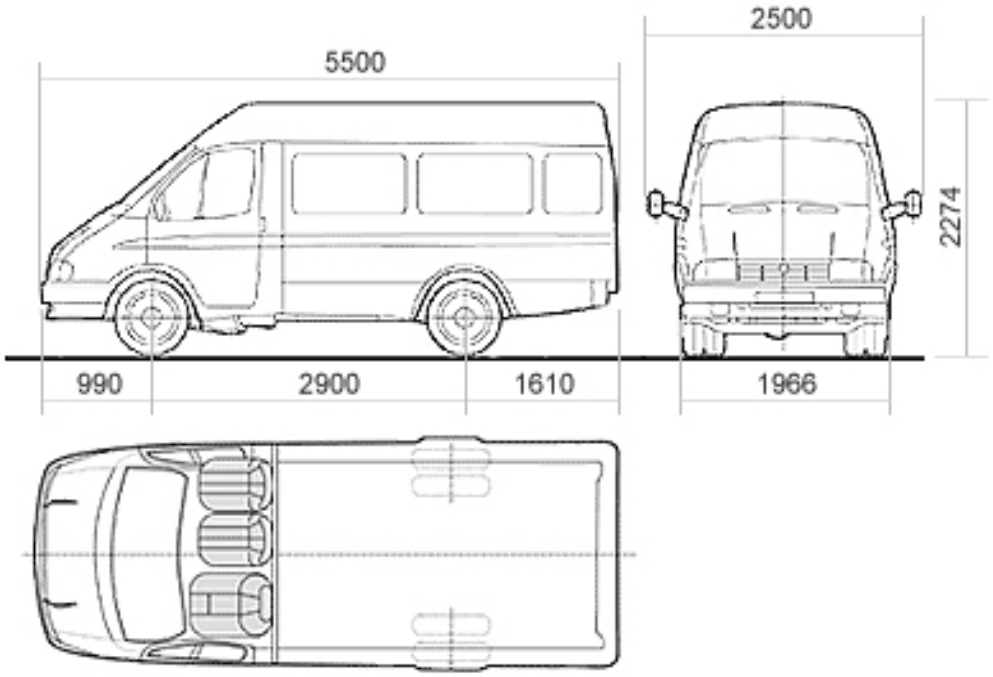

Рисунок 3.3 – Габаритные размеры Газ-322113

Все выбранное оборудование имеет транспортировочную упаковку и будет перемещаться в составе лаборатории в своей упаковке. Использование оборудования будет осуществляться непосредственно в испытуемых помещениях или, в автомобиле на оборудованном столе.

Для зарядки аккумуляторов используемого оборудования, а также обеспечения энергопитания необходимо использовать бензиновый (так как выбранный автомобиль также имеет бензиновый двигатель) генератор электропитания. Предлагается использовать Бензиновый генератор MITSUI Power ECO ZM 10000 E-3, который показан на рисунке 3.4.

Рисунок 3.4 – Бензиновый генератор MITSUI Power ECO ZM 10000 E-3

Бензиновый генератор MitsuiPower ECO ZM10000 E-3, как и генераторы всей линейки, обладает пониженным уровнем выбросов, вредных для экологии. Данная модель может применяться в качестве резервного или основного источника питания для любой техник, в том числе для чувствительной к перепадам тока. В генераторе используется обмотка стопроцентной медью, чем достигается высокий класс изоляции. Поэтому к этой модели можно смело подключать чувствительное и сложное оборудование.

Технические характеристики MITSUI ECO ZM 10000 E-3:

- номинальная мощность 10 кВт;
- максимальная мощность 11 кВт;
- вид топлива Бензин АИ-92;
- тип запуска электрический стартер;
- топливный бак 35 л;
- расход топлива 3,5 л/ч;
- напряжение 380 В;
- двигатель Mitsui ZX680;
- объем двигателя 420 куб.см;
- кол-во оборотов двигателя 3000 об./мин.;

- кол-во цилиндров два;
- тип охлаждения воздушное;
- уровень шума на расстоянии 7 м 82 дБ;
- вес 135 кг;
- габариты 785х625х795 мм.

Конструкция бензиновой электростанции MitsuiPower ECO ZM10000 E-3 отличается удобством и легкостью в использовании. А пара колес и ручка, которыми оснащен генератор, делает его максимально удобным в транспортировке.

На рисунке 3.5 представлена схема автономного питания технических средств подвижной испытательной лаборатории.

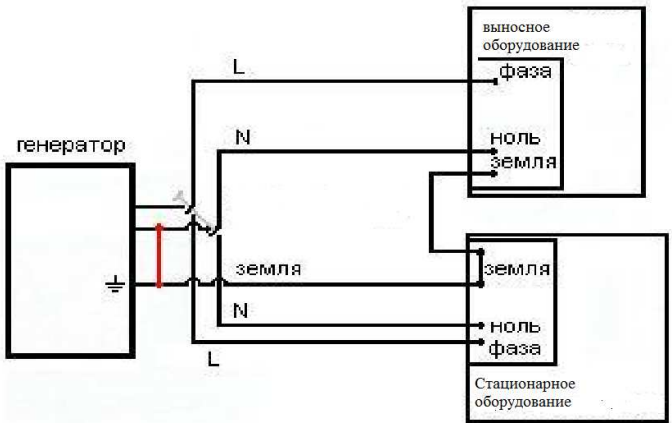

Рисунок 3.5 – Схема автономного питания технических средств подвижной лаборатории

3.4 Требования к рабочему месту оператора

Рабочее место является частью пространства, в котором сотрудник ведет свою трудовую деятельность и так или иначе проводит значительное количество рабочего времени. Само рабочее место, правильно приспособленное к трудовой деятельности, грамотно и точно организованное в плане свободного пространства, формы и размера дает сотруднику удобное положение в процессе работы и повышенную производительность труда при минимальном психологическом и физическом напряжении.

Если рабочее место организовано правильно, производительность труда человека увеличивается с 8 до 20 процентов.

Положение «сидя» в процессе работы вызывает минимальное утомление сотрудника. Грамотная планировка рабочего места включает в себя определенный порядок и постоянство размещения предметов, документов и средств труда. Все, что постоянно необходимо для выполнения работ чаще, должно находиться в зоне легкой досягаемости рабочего пространства.

Под моторным полем понимается пространство рабочего места, в рамках которого могут быть реализованы двигательные действия человека.

Максимальная зона досягаемости рук включает в себя часть моторного поля рабочего места, которое ограничено дугами, описываемыми максимально вытянутыми руками при их движении в плечевом суставе.

Рассмотрим оптимальное размещение предметов труда и документации в зонах досягаемости рук: дисплей размещается в зоне а (в центре); клавиатура; в зоне г/д; системный блок размещается в зоне б (слева); принтер находится в зоне а (справа);

Документация: в зоне легкой досягаемости ладони; литература и документация, необходимая при работе; выдвижных ящиках стола, а также в шкафах; литература, неиспользуемая постоянно.

Главными элементами рабочего места пользователя являются письменный стол и кресло. Основным рабочим положением является положение сидя. Рабочее место для выполнения работ в положении сидя организуется в соответствии с Санитарными нормами и правилами СанПиН.

Рабочее место по отношению к световым проемам должно располагаться так, чтобы естественный свет падал сбоку, преимущественно слева. Оконные проемы в помещении должны быть оборудованы регулируемыми устройствами типа жалюзи, занавесей, внешних козырьков и др.

При планировании рабочего места необходимо обеспечить нормальные условия обзора. Зону обзора описывает угол, вершина которого находится в центре глаз, а стороны составляют границы, в которых человек, при

фиксированном положении глаз, хорошо различает предметы и их местоположение. Величина этого угла равна 30°.

Клавиатуру следует располагать на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю, или на специальной регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

В помещениях с ПЭВМ ежедневно должна проводиться влажная уборка.

Важным моментом является также рациональное размещение на рабочем месте документации, канцелярских принадлежностей, что должно обеспечить работающему удобную рабочую позу, наиболее экономичные движения и минимальные траектории перемещения работающего и предмета труда на данном рабочем месте.

Создание благоприятных условий труда и правильное эстетическое оформление рабочих мест на производстве имеет большое значение как для облегчения труда, так и для повышения его привлекательности, положительно влияющей на производительность труда. Окраска помещений и мебели должна способствовать созданию благоприятных условий для зрительного восприятия, хорошего настроения. В служебных помещениях, в которых выполняется однообразная умственная работа, требующая значительного нервного напряжения и большого сосредоточения, окраска должна быть спокойных тонов – малонасыщенные оттенки холодного зеленого или голубого цветов

При разработке оптимальных условий труда пользователя необходимо учитывать освещенность, шум и микроклимат.

3.5 Программа проведения специальной проверки

Специальные проверки представляют собой проверки технических средств и систем (ТСС) объекта защиты с целью выявления и изъятия специально установленных закладных устройств съема информации непосредственно с ТСС, выявление технических доработок по изменению

свойств ТСС, облегчающих умышленный или неумышленный съем информации, выявление различного рода программных закладок съема информации. При проведении специальных проверок применяются специализированные технические средства.

Данный вид работ лицензируется, контролируется и проводится на основании нормативно-методических документов. Специальная проверка предшествует специальным исследованиям и состоит из нескольких последовательно выполняемых действий:

- прием-передача проверяемого технического средства представителям исследовательских лабораторий или сертификационных центров, формирование исходных данных для программы проверки;
- составление программы проведения специальной проверки технического средства;
- проведение проверки;
- анализ результатов проверки, составление отчетных протоколов.

На специальную проверку технические средства должны предъявляться в исправном состоянии, в штатной упаковке и в полной комплектации по акту приема-передачи. Акт приема-передачи подписывается только после проверки работоспособности технического средства. В случае неисправности технического средства специальная проверка не производится.

Кроме технического средства, представители организации, которой оно принадлежит, обязаны предоставить для разработки программы проверки информацию следующего вида:

- данные о техническом средстве;
- сведения о его планируемом применении;
- данные о месте размещения технического средства.

Данные о техническом средстве должны содержать сведения о его назначении и полной комплектации, комплект документов на техническое

средство, способ приобретения с указанием сведений об организации-поставщике.

Данные о планируемом применении должны содержать сведения:

- планируется ли техническое средство для обработки закрытой информации;
- есть ли высший гриф секретности у обрабатываемой или обсуждаемой информации;
- в составе какой информационной системы планируется работа технического средства;
- к каким коммуникационным системам планируется подключение технического средства.

Сведения о планируемом размещении технического средства должны содержать:

- описание объекта информатизации, на котором планируется использовать техническое средство;
- перечень охраняемых сведений объекта информатизации;
- минимальное расстояние до границы контролируемой зоны;
- наличие посольств, представительств и мест пребывания иностранных граждан с указанием расстояния до контролируемой зоны;
- возможность и периодичность пребывания иностранных делегаций на объекте.

Программа проведения специальной проверки должна учитывать, что возможно установленные электронные закладные устройства или программные закладки ориентированы на получение вполне конкретной информации или на выведение из строя технических средств обработки информации.

По имеющимся документам проводится анализ схемотехнических особенностей электронного технического средства и источника его питания с целью выявления мест циркуляции обрабатываемой информации.

Итогом анализа исходных данных, схемотехнических особенностей и иных необходимых сведений с учетом классификации электронного устройства должен явиться перечень каналов утечки информации и возможно внедренных аппаратных закладных устройств.

Далее на основании перечня естественных каналов утечки информации и возможно внедренных закладных устройств составляется программа проведения специальной проверки технического средства, определяющая порядок выявления демаскирующих признаков закладного устройства и самого устройства. Результаты оформляются в журнале проведения специальных проверок и заверяются подписью руководителя рабочей группы.

Типовой перечень операций проведения специальных технических проверок состоит из:

- дозиметрического контроля изделия в упаковке для обнаружения радиоактивных меток и радиоизотопных источников питания;
- контроля упаковки, которая по назначению не должна иметь полупроводниковых приборов, нелинейным локатором для выявления специального электронного устройства, выполняющего роль маяка для определения местоположения технического средства;
- проведения радиоконтроля для выявления активных закладных устройств передачи информации по радиоканалу и проверки возможности съема информации методом высокочастотного навязывания;
- проведение инфракрасного контроля для выявления специального электронного устройства, использующий для передачи информации ИК-диапазон;
- проведение специального программного контроля для СВТ на базе Windows, для выявления устройств беспроводных средств доступа;

- выявление беспроводных средств и устройств сотовой связи, использующие для передачи информации стандарты беспроводных средств доступа и GSM стандарты;
- проведение активного контроля цепей питания, использующие для выявления пультов дистанционного управления и акустоэлектрических преобразований;
- разборки технического средства с последующим осмотром его узлов для выявления отклонения от схемотехнических и конструкторских решений;
- рентгенографии или рентгеноскопии неразборных узлов и элементов технических средств с целью выявления схемных изменений;
- рентгенотелевизионного и визуально-оптического контроля внешнего вида и внутренней структуры узлов и элементов технических средств.

Сложные виды контроля (визуально-оптический контроль, рентгеновский контроль, контроль методами нелинейной локации, радиоконтроля и высокочастотного «навязывания») проводятся по специальным методикам.

Проверенные технические средства и оборудование маркируются по специальной методике.

По результатам проведения специальной проверки руководитель проверяющей группы делает вывод о наличии или отсутствии закладных электронных устройств и оформляет акт с перечислением проверенных элементов, видов технических проверок и фамилий и инициалов проводивших отдельные виды проверок лиц. Акт оформляется в единственном экземпляре и хранится у исполнителя. Заключение составляется в двух экземплярах (для исполнителя и заказчика). Акт и заключение утверждаются руководителем организации-исполнителя.

ЗАКЛЮЧЕНИЕ

В процессе проектирования были проанализированы и описаны стандарты и нормативно-методические документы, на которые опирается подвижная испытательная лаборатория в своей деятельности, изучены основные методики обнаружения и выявления технических каналов утечки информации, проанализированы специальные требования и рекомендации по технической защите информации. В ходе проектирования была разработана и описана структура подвижной испытательной лаборатории, выбрано оборудование, используемое подвижной испытательной лабораторией для осуществления своей деятельности, а также разработана и описана схема его питания. Были разработаны методические рекомендации оператору, а также методические рекомендации по проведению специальной проверки с использованием подвижной испытательной лаборатории.

В результате проектирования была разработана подвижная испытательная лаборатория, предназначенная для проведения специальных проверок.

Использование спроектированной подвижной лаборатории для проведения специальных проверок позволяет выявить и успешно бороться с различными видами закладных устройств.

Таким образом, выполненная работа полностью соответствует ТЗ на ВКР.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Руководящий документ Ростехкомиссии РФ «Классификация автоматизированных систем и требования по защите информации» [Текст].

2 Руководящий документ Ростехкомиссии РФ «Критерии оценки безопасности информационных технологий» [Текст].

3 Руководящий документ Ростехкомиссии РФ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [Текст].

4 Руководящий документ Ростехкомиссии РФ «Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам» [Текст].

5 Стандарт ЦБ РФ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», (принят и введен в действие распоряжением ЦБ РФ от 18 ноября 2004 г. N Р-609) [Текст].

6 Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных» от 27 июля 2006 года [Текст].

7 Автоматизированные информационные технологии в экономике [Текст]: учебник / Под ред. проф. Г.А. Титоренко. – М.: ЮНИТИ, 2005. – 399 с.

8 Болдырев, А.И. Методические рекомендации по поиску и нейтрализации средств негласного съема информации [Текст] / А.И. Болдырев, И.В. Василевский, С.Е. Сталенков. – М.: Нелк, 2001. – 224 с.

9 Бузов, Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Текст] / Г.А. Бузов. – М.: Горячая Линия – Телеком, 2010. – 240 с.

10 Домарев, В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – К.: ООО ТИД «Диасофт», 2004. – 992 с.

11 Кнорринг, Г.М. Справочная книга для проектирования электрического освещения [Текст] / Г.М. Кнорринг, И.М. Фадин, Сидоров В.Н. – 2-е изд., перераб. и доп. – СПб.: Энергоатомиздат, 1992. – 448с.

12 Лапонина, О.Р. Межсетевое экранирование [Текст] / О.Р. Лапонина. – М.: Бином, 2007. – 354 с.

13 Моисеева, Н.К. Практикум по проведению функционально. Компьютерные сети. Принципы, технологии, протоколы [Текст] / Н.К. Моисеева. – СПб.: Питер-пресс, 2002. – 465 с.

14 Павликов, С.Н. Формирование направления развития систем мобильной связи [Текст] / С.Н. Павликов, С.С. Веселова // Вестник Морского государственного университета. – Владивосток: Мор. Гос. Ун-т., 2010. – Вып. 43. С. 131-140.

15 Павликов, С.Н. Перспективы развития радиозакладных устройств с повышенным уровнем интеллекта и технологии защиты [Текст] / С.Н. Павликов, Л.Н. Дымова, О.В. Клева // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. Гос. Ун-т., 2013. – Вып. 58/2013. С. 61-64.

16 Петраков, А.В. Основы практической защиты информации [Текст]: учебное пособие / А.В. Петраков. – М.: Радио и связь, 2001. – 368 с.

17 Рудометов, Е.А. Электронные средства коммерческой разведки и защиты информации [Текст] / Е.А. Рудометов, В.Е. Рудометов. – М.: ООО «Фирма «Издательство АСТ», 2000. – 224 с.

18 Селезнева, Н.Н. Финансовый анализ. Управление финансами [Текст]: учеб. пособие для вузов / Н.Н. Селезнева, А.Ф. Ионова. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2007. – 639 с.

19 Скиба, В.Ю. Руководство по защите от внутренних угроз информационной безопасности [Текст] / В.Ю. Скиба, В.А. Курбатов. – СПб.: Питер, 2008. – 320 с.

20 Халяпин, Д.Б. Радиомониторинг защищаемого объекта с помощью индикаторов поля [Текст]: учебное пособие / Д.Б. Халяпин. – М.: Академия, 2010. – 212 с.

21 Хорев, А.А. Классификация электронных устройств перехвата информации [Текст] / А.А. Хорев. – М.: Спецтехника и связь. 2009. – №1. – С.46-50.

22 Хорев, А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации [Текст]: учебное пособие / А.А. Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

23 Хорошко, В.А. Методы и средства защиты информации [Текст] / Под ред. Ковтанюка П.В.; В.А. Хорошко, А.А. Чекатков. – М.: Юниор, 2003. – 504 с.

24 Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А.Ю. Щеглов. М.: Наука и техника, 2004. – 384 с.

25 Яковлев, В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта [Текст] / В.В. Яковлев, А.А. Корниенко. – М.: Маршрут, 2002. – 327 с.

26 Ярочкин, В.И. Информационная безопасность [Текст]: учебное пособие / В.И. Ярочкин. – М.: Междунар. отношения, 2000. – 400 с.