МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологий
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _к.п.н. Бердибаев Рат Шынгалиевич_
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Обнаружения устройств несанкционированного съема информации»

Специальность Системы Информационной Безопасности_____

Выполнил(а) Даутпаев Даурен Талгатович_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель к.т.н., профессор Тынымбаев С.Т._____
(ученая степень, звание, Ф.И.О.)
Консультанты: старший преподаватель Мукашева Асель Коптлеуовна____
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич_____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: старший преподаватель Дмитриева Маргарита Валерьевна_
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: тех. дир. ТОО «Доктор Веб – Центральная Азия» Бугаев Виталий
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных Технологий
Кафедра «Системы информационной безопасности»
Специальность «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Даутпаеву Даурену Талгатовичу
(Ф.И.О.)
Тема проекта «Обнаружения устройств несанкционированного съема информации»

Утверждена приказом по университету № 147 от «11» 11 2019 г.

Срок сдачи законченного проекта «01» 06 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – радиоэфир помещения, радиозакладное устройство ручной сборки, сканиурющий приемник OSCOR OSC-500, модули передачи данных (WiFi, Bluetooth, Zigbee), математический редактор Smath Studio.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы - исследование методов обнаружения устройств несанкционированного съема информации.
Задачи исследования: библиографический обзор электронных устройств несанционированного съема информации, методы и технические средства для обнаружения радиоэлетронных устройств несанкционированного съема информации, алгоритмы обнаружения элетронных устройств несанкционированного съема информации.

Перечень графического материала (с точным указанием обязательных чертежей): блок схема алгоритма обнаружения закладных устройств на основе легальных передачи данных.

Основная рекомендуемая литература: Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам; Хорев, А.А. Оценка возможностей средств радиоразведки по перехвату информации.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н., доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Библиографический обзор закладных устройств негласного съема информации	17.12.2019 – 20.12.2019	
Систематизация и определения классификационных признаков закладных устройств	21.12.2019 – 28.12.2019	
Определение методов поиска и обнаружения закладных устройств	01.02.2020 – 08.02.2020	
Изучение методов радиомониторинга, приминяемых для процессов поиска радиозакладных устройств	09.02.2020 - 18.02.2020	
Формирование алгоритма для поиска устройств с передачей данных по легальным каналам	19.02.2020 – 27.02.2020	
Ознакомление со сканирующим приемником OSCOR OSC-500	28.02.2020 - 07.03.2020	
Формирование алгоритма для устройств с периодической передачей данных	08.03.2020 - 18.03.2020	
Проведение экспериментов	19.03.2020 - 30.03.2020	
Проведение сравнительного анализа сканирующих приемников по различным признакам	01.04.2020 - 09.04.2020	
Анализ рисков ИБ. БЖД	01.05.2020 - 09.05.2020	

Дата выдачи задания «_15_»___10___2019_г.

Заведующий кафедрой _____ (_Бердибаев Рат Шынгалиевич__)
(подпись) (ФИО)

Научный руководитель
проекта _____ (Тынымбаев Сахыбай Тынымбаевич)
(подпись) (ФИО)

Задание принял к
исполнению студент _____ (_Даутпаев Даурен Талгатович__)
(подпись) (ФИО)

Аннотация

В дипломном проекте разработаны алгоритмы обнаружения закладных устройств несанкционированного съема информации. Предложены две модели для идентификации закладных устройств с беспроводной передачей данных. Разработка моделей основывалась на особенностях конструирования и принципах передачи данных, которые являются слабым местом данных устройств. Произведено физическое моделирование процесса обнаружения закладных устройств при помощи радио мониторинга. Результаты представлены в четырех экспериментах. Данные модели могут являться фундаментом, для разработки автоматизированного комплекса обнаружения электронных устройств несанкционированного съема информации с беспроводной передачей данных. А также будет полезна в области пеленгации летательных аппаратов.

Annotation

In the graduation project developed algorithms for detecting embedded devices of secret information retrieval. Two models are proposed for identification of embedded devices with wireless data transmission, the development of which was based on the design features and principles of data transmission, which are the weak point of these devices. A physical simulation of the process of detecting embedded devices using radio monitoring has been performed. The results are presented in four experiments. These models can be the foundation for the development of an automated complex for detecting electronic devices of unauthorized information retrieval with wireless data transmission. It will also be useful in the field of aircraft direction finding.

Аңдатпа

Дипломдық жобада ақпаратты рұқсатсыз алу үшін салынатын құрылғыларды табу алгоритмдері әзірленген. Сымсыз деректерді беру арқылы ендірілген құрылғыларды анықтау үшін екі модель ұсынылды. Модельдерді әзірлеу осы құрылғылардың әлсіз орны болып табылатын деректерді беру принциптері мен құрастыру ерекшеліктеріне негізделді. Радио мониторинг көмегімен салынатын құрылғыларды анықтау процесін физикалық моделдеу жүргізілді. Нәтижелері төрт экспериментте ұсынылған. Бұл модельдер мәліметтерді сымсыз бере отырып, ақпаратты рұқсатсыз алудың электрондық құрылғыларын анықтаудың автоматтандырылған кешенін әзірлеу үшін іргетас болуы мүмкін. Сондай-ақ ұшу аппараттарын пеленгациялау саласында да пайдалы болады.

Содержание

Введение

С ростом доступности закладных устройств, предназначенных для негласного получения информации, возникает потребность в выявлении таких технических средств. Одним из методов выявления устройств негласного съема информации является радиомониторинг. В настоящее время основным средством радиомониторинга выступают многоканальные сканирующие приемники, которые позволяют осуществлять автоматически: постоянный контроль заранее заданных частот связи, а также поиск находящихся в эфире радиосигналов. Помимо сканеров в процессе ведения радиомониторинга используется и другая аппаратура, к ней относится: портативные частотомеры, анализаторы спектра, разного рода антенны, малошумящие антенные усилители и много другое. Эффект и результат радиомониторинга зависит не только от дорогостоящей аппаратуры и правильной установки измерительных приборов, но и от методов, применяемых к процессу, а также от квалификации и опыта специалистов, проводящих исследования в области радиомониторинга. Наблюдение за радио эфиром – очень длительный процесс. Довольно часто это занимает много времени. Квалифицированные специалисты осуществляют длительное наблюдение с помощью измерительных комплексов за радиодиапазонами, проводящих идентификацию и измерения параметров радиосигналов, запись, хранение и обработку информации, получаемой путем радиомониторинга и др.

Целью работы является исследование методов обнаружения устройств несанкционированного съема информации.

С учетом поставленной цели сформулированы основные задачи исследования:

- библиографический обзор электронных устройств несанкционированного съема информации;
- методы и технические средства для обнаружения радиоэлетронных устройств несанкционированного съема информации;
- алгоритмы обнаружения элетронных устройств несанкционированного съема информации.

Объект исследования – процесс поиска радиоэлектронных устройств негласного съема информации путем радиоманиторинга.

Предмет исследования – методы обнаружения радиэлектронных устройств негласного съема информации путем радиоманиторинга.

1 Теоретический обзор закладных устройств негласного съема информации

В век информации, когда действует принцип - кто владеет информацией, тот владеет миром, желающих таким образом овладеть миром предостаточно, а значит, существует устойчивый спрос на информацию, полученную несанкционированным путем.

Большая доля передачи информации приходится на речь. И в ближайшие десятилетия в этом плане не предвидится изменений. Сейчас, пожалуй, нет ни одного предприятия или организация, где конфиденциальная информация не передавалась бы при помощи речи на различных совещаниях. В связи с этим, утечка информации по речевому каналу будет оставаться актуальной проблемой.

Удаление информации с помощью радио-закладок является одним из самых распространенных способов получения информации по умолчанию. Он тайно устанавливается в месте, где секретная информация продолжает распространяться, и удаляется через канал акустической утечки и передается по электромагнитному (или другому: электрическому, оптическому и т. д.) каналу связи. Пока что нет способа предотвратить размещение радиоустройств. Поэтому для предотвращения использования закладок на радио необходимо знать их рабочие принципы, функции и функции, которые будут эффективно компенсировать такие устройства и облегчат их поиск.

Закладные устройства представляют собой организованный канал несанкционированного получения и передачи в пункт приема аудио и визуальной информации, а также информации передаваемой по сетям связи.

1.1 Классификация закладных устройств съема информации

Один из результативных путей внегласного извлечения коммерческих данных базируется на использовании так именуемых закладных устройств (ЗУ), тайно устанавливаемых в зонах вероятного пребывания предметов слежки (конкурентов) или подключаемых к применяемым ими каналам взаимосвязи. В наше время сформировано большое число видов подобных приборов, отличающихся принципом функционирования, методом передачи данных, дальностью воздействия, а кроме того, габаритом и наружным оформлением.

Наиболее мелкое запоминающее приспособление весит лишь 1,5 г и имеет линейный размер 2-5 миллиметров. Дистанция передачи данных с подобных приборов чуть выше 10 метров. Наиболее сильные приспособления имеют все шансы достигать величины не более нескольких см и могут транслировать перехваченные сведения в спектре от сотни вплоть до тысячи и более метров. Как правило приспособления хранения скрытно устанавливаются в зданиях и внутренних конструктивных элементах и

фиксируются под одеждой либо скрываются под персональные принадлежности.

С целью классифицировать понимание о подобных приборах, разумно внедрить 5 особенностей их систематизации:

- согласно каналу передачи данных;
- согласно методу восприятия данных;
- согласно присутствию приспособления управления;
- согласно наружному типу;
- согласно используемому ключу питания.

Рассмотрим отдельно каждый из классификационных признаков. В зависимости от канала передачи информации различают следующие типы ЗУ:

- радиозакладки;
- инфракрасные закладки;
- закладки с передачей информации по токоведущим линиям;
- закладки с записью на магнитофон.

В ходе передачи данных в радиокнигах применяется энергия электромагнитных волн, что никак не воздействует на чувства человека и имеет возможность охватывать крупные дистанции, справляясь с естественными и искусственными преградами. Благодаря этим двум функциям встроенные радиоустройства позволяют использовать стабильные приемные устройства для скрытого мониторинга объектов, представляющих интерес, практически из любой удаленной точки.

С технической точки зрения, закладки имеют все шансы трудиться буквально в каждом диапазоне радиоволн. Тем не менее из конструктивных суждений более применяемые частоты – с 100 вплоть до 1000 МГц.

В инфракрасных закладках энергия электромагнитных волн еще применяется с целью передачи данных, однако никак не данных в радиодиапазоне, а невидимой части оптической области диапазона данных в инфракрасном спектре. Из-за небольшой длины подобные волнения разносятся в узком луче в установленном направлении и их тяжело выявить в том числе и с поддержкой особого оснащения. Расстояние передачи данных с инфракрасной памяти доходит 500 м.

Однако высокая степень конфиденциальности такого оборудования значительно усложняет его использование. Поэтому инфракрасные закладки всегда должны находиться в пределах прямой видимости приемника оптического излучения, а объекты, люди или автомобили, которые случайно попадают в зону видимости, и изменение погодных условий могут привести к значительному снижению качества. Даже сигнал в записывающем устройстве теряется. Естественно, такие устройства хранения совершенно не подходят для движущихся объектов. Из-за этих недостатков инфракрасные закладки редко используются в промышленном шпионаже.

Закладки с передачей данных согласно токоведущим направлениям, применяют черту электро - сигналов охватывать в существенные дистанции

согласно проводникам. Подобные ЗУ владеют значимыми плюсами: высочайшей скрытностью передачи данных, высокий дальностью воздействия, неимением потребности в добавочных ключах кормления. помимо этого, они отлично камуфлируются под компоненты электро - цепей и токоприемники (розетки, тройники, гальванические удлинители, настольные лампы и т. д.). В свойстве токопроводящих направлений применяются или намеренно протоптанные кабель, или кабели электро и телефонных сеток. В силу упомянутых факторов ЗУ подобного вида зачастую используются бесчестными соперниками с целью извлечения данных секретного нрава. В зависимости от метода восприятия данных отличают 3 вида закладных приборов:

- микрофонного вида;
- массового вида;
- с включением к коммуникационным направлениям.

Принцип воздействия ЗУ микрофонного вида базируется в переустройстве звуковых погодных сомнений в гальванические сигналы и передаче их покупателю один с перечисленных выше методов. Закладные приспособления массового вида (стетоскопы) перехватывают звуковые сомнения жестких сфер (пульсации), появляющиеся из-за давления погодных звуковых волнений в сферы, показано в рисунке 1.1. В свойстве восприимчивых компонентов в подобных приборах как правило применяются пьезомикрофоны, электрические микрофоны либо детекторы акселерометрического вида. Они более результативны рядом регистрации в деликатных «площадных» поверхностях (межкомнатных перекладинах, стеклах, дверях и т. п.)

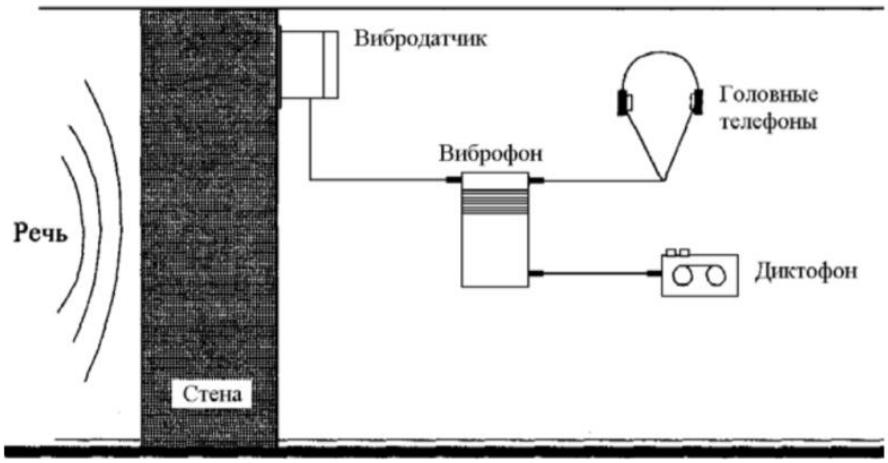

Рисунок 0.1 – Стетоскоп с передачей информации по специально проложенным проводным линиям

Для передачи информации потребителю, как правило, используется радиоканал, поэтому такие ЗУ обычно называют радиостетоскопами, представлено на рисунке 1.2.

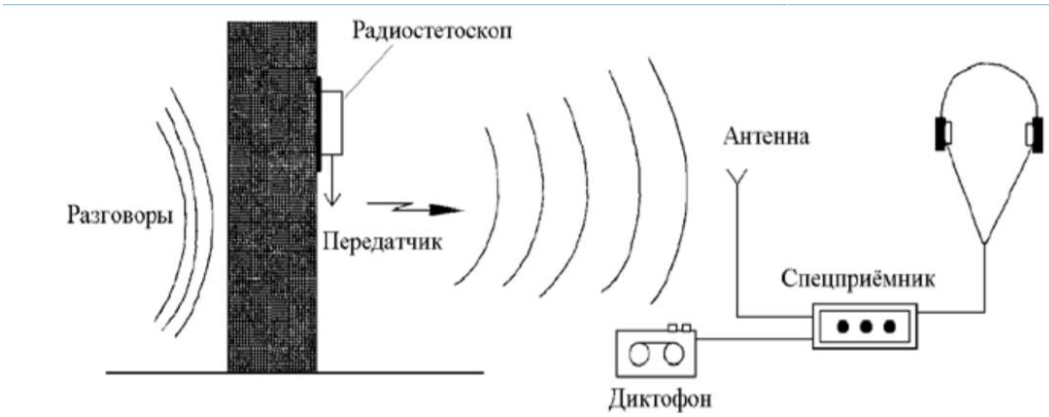

Рисунок 0.2 – Радиостетоскоп с передачей информации по радиоканалу

Ипотечное оборудование, подключенное к линии связи, предназначено для скрытого перехвата информации, распространяемой по телефону или по оптоволоконной линии. Такая память позволяет тайно получать информацию о содержании телефонных разговоров и текстовых сообщений (телеграмма, факс, электронная почта и т. д.). Радиоканал обычно используется для передачи информации из подключенной памяти. Эта память называется радио-ипотека (РЗУ).

По способу подключения к телефонным линиям радиозакладки делят на две группы: РЗУ с непосредственным подключением, и РЗУ с индукционным подключением, представлено на рисунке 1.3.

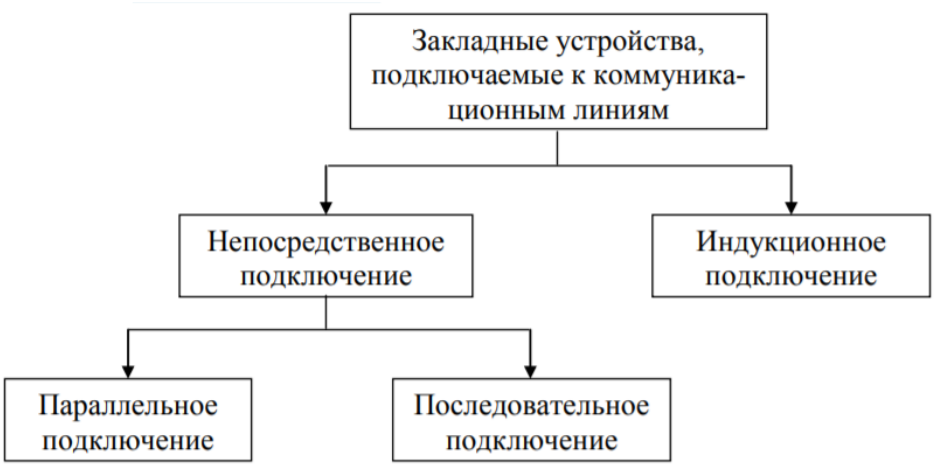

Рисунок 0.3 – Классификация ЗУ по способу подключения к токопроводящим коммуникационным линиям

Первая группа – радиозакладки с непосредственным подключением. Они подключаются либо одновременно к обоим проводам параллельно абоненту (параллельное подключение – рисунок 1.4.а), либо в разрыв одного из проводов (последовательное подключение – рисунок 1.4.б).

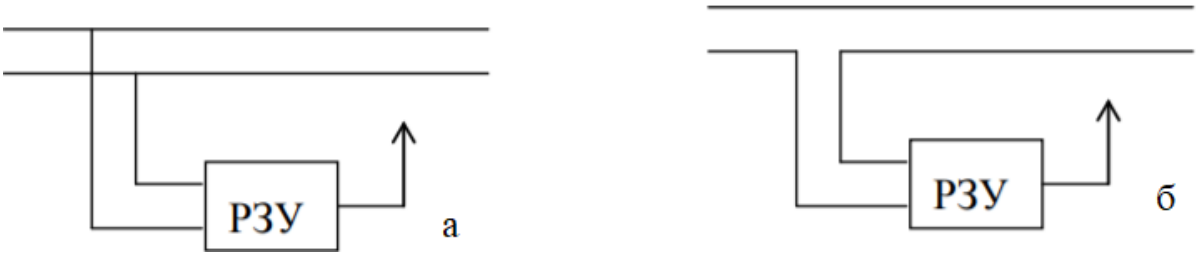

Рисунок 0.4 – Непосредственное подключение РЗУ: параллельное (а) и последовательное (б)

Подобные методы дают возможность приобрести хороший уровень сигнала (его превосходное свойство) на входе радиозакладки, а кроме того, возникает вероятность гарантировать ее питание с линии. Тем не менее закладки с прямым включением имеют все шансы быть легко обнаружены в связи с изменением характеристик направления

Этого недостатка в значительной степени лишены устройства второй группы – радиозакладки с индукционным подключением представлены на рисунке 1.5.

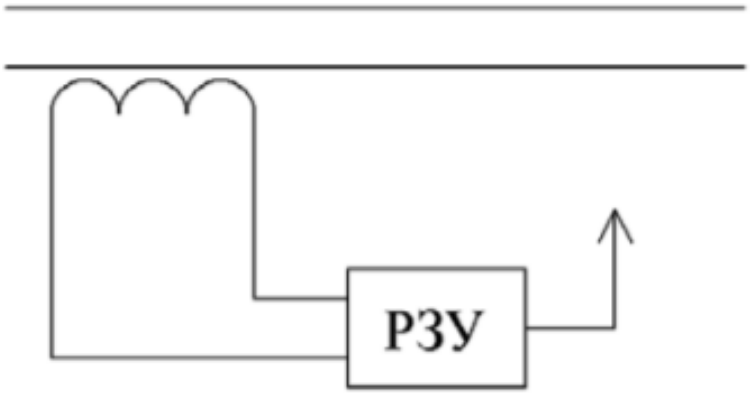

Рисунок 0.5 – Индукционное подключение РЗУ

В закладках данного вида чувствительный компонент выступает в роли специально сконструированной антенны, что определена вблизи с телефонной линией. Электромагнитное поле около телефонной линии индуцирует электричество в антенне, что содержит информацию о характере уведомления. Данные токи усиливаются, преобразуются, а потом направляют приобретенные сведение в раздел регистрации.

Закладные приспособления с целью снятия данных с волоконно-зрительных направлений сознательно различаются с пересмотренных ранее только лишь методом снятия данных. Для данных целей используются специализированные приспособления сжатия волоконных направлений, инициирующие интерференционные движения в плоскости зрительного волокна, что и считываются фотоприемником. По присутствию

приспособления управления закладные приспособления относительно делят в 3 категории:

- с постоянным излучением;
- с дображивающим правлением;
- с самодействующим включением при выходе в свет сигнала.

Непрерывная эмиссионная память является самой простой в изготовлении, дешевой и рассчитанной на получение информации в течение ограниченного времени. С момента включения питания изучается излучение этого типа памяти. Если источник питания автономен, рабочее время таких запоминающих устройств обычно не превышает 1-2 часа из-за большого энергопотребления при передаче сигнала. Время работы запоминающих устройств с питанием от линий (питания или телефона) практически не ограничено.

Тем не менее единым значимым минусом для абсолютно всех ЗУ с постоянным излучением является вероятность их выявления согласно излучению. значительно повысить период беспрерывной деятельность приборов с самостоятельным питанием и увеличить незаметность дает возможность применение дображивающего управления ЗУ. Оно дает возможность перечислять приспособление в порядок испускания только лишь в этих вариантах, если предмет исследования проводит диалог или сообщает сведение согласно каналам взаимосвязи. Время испускания имеет возможность являться в дополнение сжато, в случае если заполнение включает приспособление сбережения и сжатия сигнала. Другим методом повышения времени деятельность закладки представляется применение приборов механического введения передатчика рядом выходе в свет сигнала (звукового или электрического в направления). Голосовые триггеры называются акустическими индукторами. Их иногда называют системами VAS или VOX. Закладки, оснащенные этим устройством, могут использоваться в качестве приемников звука в обычном (резервном) режиме, потребляя небольшое количество тока. Например, когда появляется сигнал, в начале разговора между наблюдаемым объектом и кем-либо, на передатчик подается напряжение, и передатчик переключается в режим излучения. Если звуковой сигнал пропадает через определенный промежуток времени (обычно через несколько секунд) (разговор заканчивается), передатчик выключится, и закладка перейдет в режим ожидания. Использование акустомата дает возможность в некоторое количество единожды повысить период деятельность закладного приспособления. тем не менее их применение приводит к утрате первых слов при всяком подключении. По используемому ключу питания, равно как было указано ранее, ЗУ разделяются на 2 типа:

- с собственным источником;
- с питанием с наружного источника.

К первому типу причисляются всевозможные ЗУ, обладающие интегрированный батарея (батарейку). К другому – ЗУ с передачей данных

согласно токоведущим направлениям и ЗУ с прямым включением к коммуникационным направлениям. Период деятельности подобных приборов фактически безграничен. Согласно наружному типу отличают ЗУ: в обыкновенном выполнении; в закамуфлированном варианте. В обыкновенном выполнении приспособления обладают металлической оболочкой и фигуру параллелепипеда. Они довольно многофункциональны и используются в разных обстоятельствах ситуации. Такие ЗУ скрываются одеждой, объектами внутреннего убранства (пластмассовой коробкой, книгами, полотном и т. п.) или районными объектами, пропускающими звуковые и (либо) электромагнитные колебания (травой, сжатым хлопчатобумажным или пластмассовым фунтиком, фанеры и т. п.). В закамуфлированном варианте ЗУ используются только лишь в согласовании с определенной ситуацией. Таким образом, к примеру, в варианте электросиловой либо телефонной розетки только лишь в этом случае, в случае если прочие неприменяемые розетки в помещении обладают такого рода наружным типом, вроде индивидуальных предметов (часов, зажигалки, заколки), в случае если они отвечают единому стилю применяющего их лица.

1.2 Радиозакладные устройства

Более обширное использование в практике промышленного шпионажа определили приспособления с радиоканалом передачи перехватываемых данных, таким образом именуемые, радиозакладные устройства (РЗУ), либо попросту радиозакладки. Высокая заинтересованность к применению РЗУ сопряжена с их исключительно обширными способностями по надзору за подвижными предметами, пребывающими на значительной дистанции.

Встраиваемые в радио устройства как радиоустройства имеют особые функции, которых нет у многих других устройств хранения. В соответствии с этими функциями вы можете использовать следующие классификационные функции для классификации радио-закладок: принцип генерации сигнала, метод и объем закрытия передачи информации. По принципу формирования релейного сигнала он может быть активным, полуактивным и пассивным.

В соответствии с принципом формирования сигнала РЗУ могут быть активные, полуактивные и пассивные.

1.3 Схемы применения радиозакладных устройств

Схемы ретрансляции сигнала в телефонную линию и в УКВ радиоканал показаны на рисунках 1.6 и 1.7 соответственно. Схема приема сигналов от радиозакладок, закамуфлированных под личные вещи сотрудников и некоторые предметы, представлена на рисунке 1.8.

Схемы применения радиозакладных приборов с применением ретрансляторов сигналов с закладных приборов к пунктам приёма и сбора данных приведены в рисунках 1.9 и 1.10.

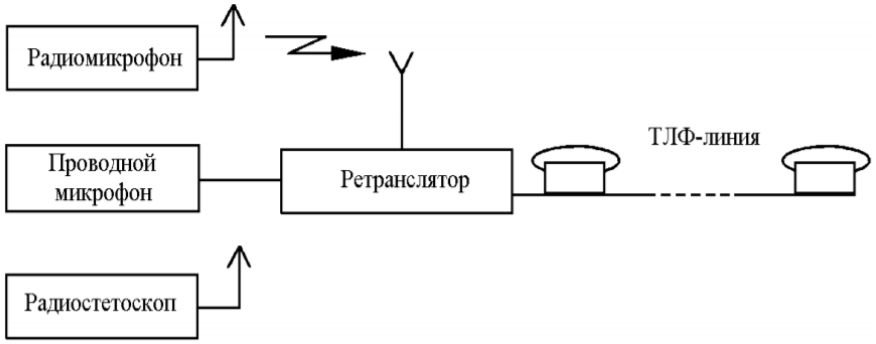

Рисунок 0.6 – Ретрансляция сигналов в телефонную линию

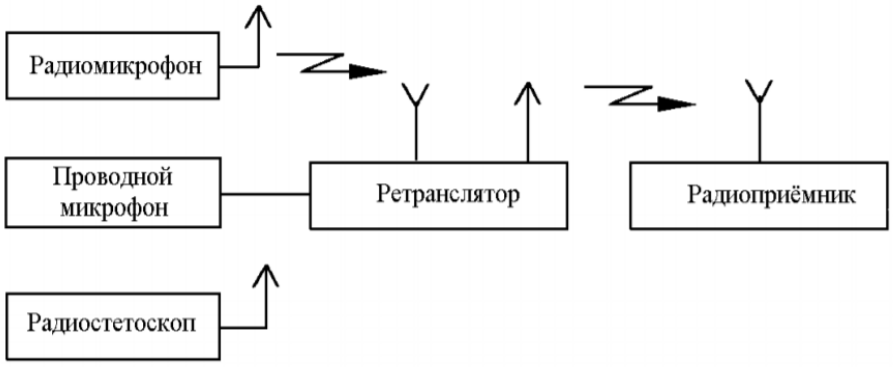

Рисунок 0.7 – Ретрансляция сигналов в УКВ радиоканал

На один приёмник допускается получать сигнал от нескольких радиозакладных приборов, в этой части закамуфлированных либо под персональные принадлежности, либо под элементы электроцепей. Схемы использования закамуфлированных радиозакладных устройств приведены на рисунках 1.11 и 1.12.

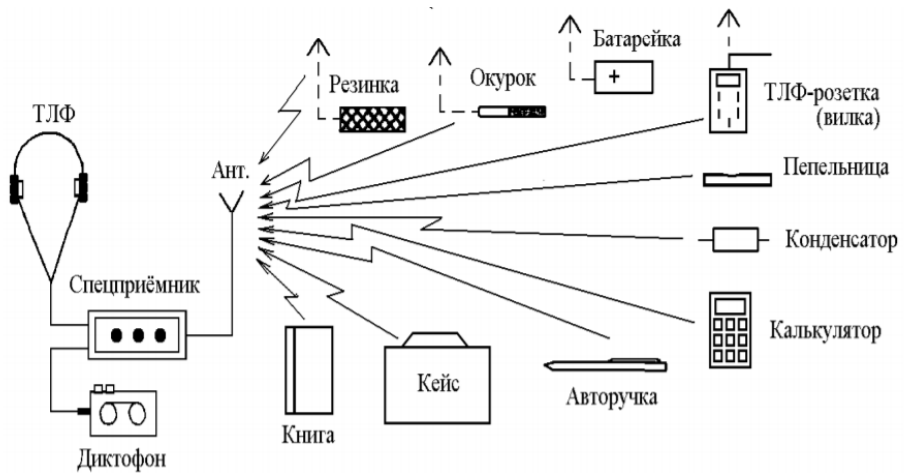

Рисунок 0.8 – Приём сигналов от радиозакладок, закамуфлированных под личные вещи сотрудников и некоторые предметы

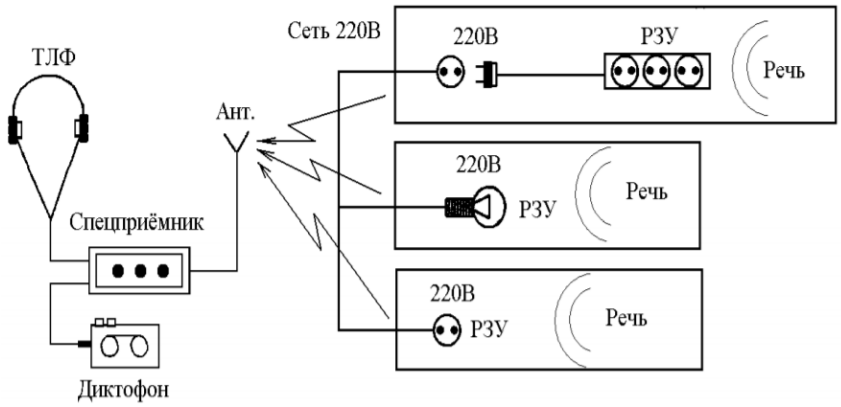

Рисунок 0.9 – Приём сигналов в контролируемых помещений, от нескольких радиозакладок которые закамуфлированы под элементы электросети 220В

1.4 Выводы по главе

В данной главе был произведен обзор закладных устройств негласного съема информации. Была представлена классификация закладных устройств по различным признакам. Описаны принципы их работы, а также принципы работы приемников закладных устройств.

2 Методы и средства выявления радиоэлектроных закладных устройств

2.1 Общие принципы выявления

Одним из элементов системы защиты информации является выявление возможно внедренных закладных устройств (ЗУ). Оно реализуется на основе двух групп методов, представлено на рисунке 2.1.

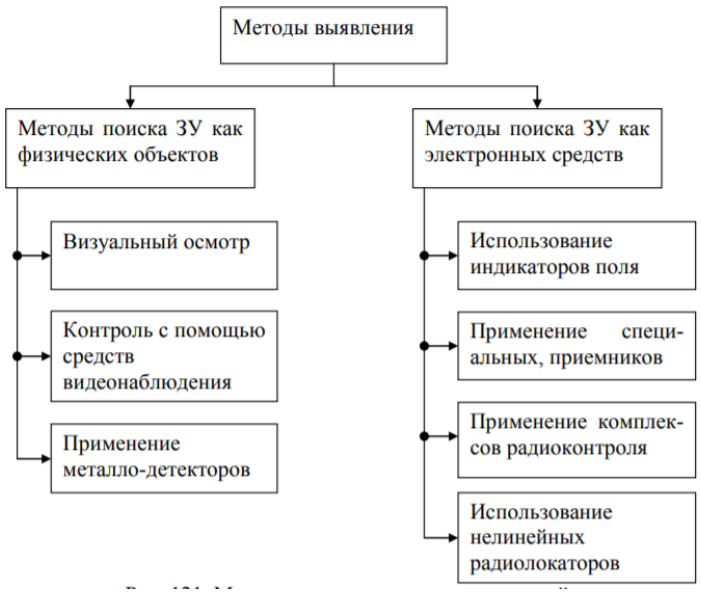

Рисунок 2.1 – Методы выявления закладных устройств

Первая группа – методы, основанные на поиске ЗУ как физических объектов с вполне определенными свойствами и массогабаритными характеристиками. К этой группе методов относятся:

- визуальный осмотр мест возможного размещения ЗУ, в том числе с применением увеличительных стекол, зеркал, средств специальной подсветки;
- контроль труднодоступных мест с помощью средств видеонаблюдения;
- применение металлодетекторов.

Вторая группа – методы, использующие свойства ЗУ как электронных систем. Она включает:

- использование индикаторов поля, реагирующих на наличие излучения радиозакладных устройств и позволяющих локализовать их месторасположение;
- применение специальных радиоприемных устройств, предназначенных для поиска сигналов по заданным характеристикам и анализа электромагнитной обстановки;
- применение комплексов радиоконтроля и выявления ЗУ;
- обследование помещений с помощью нелинейных радиолокаторов, позволяющих выявлять любые типы ЗУ.

Обнаружение ЗУ как физических объектов является наиболее общим случаем, попадающим под понятие осмотра или досмотра. Его основные методы и используемые технические средства будут рассмотрены ниже.

2.2 Методы поиска закладных устройств как физических объектов

Визуальный осмотр - это один из важнейших способов раскрытия, он никак не может быть заменен ни одним другим. Он нужен в целях выявления ЗУ равно как в обыкновенном выполнении, так и в закамуфлированном варианте. Осуществляется периодически, а еще перед проведением значимых событий в тех комнатах, где может быть расположение ЗУ.

При проведении зрительного осмотра особенное внимание необходимо уделять внутренним изменениям, появлению новых царапин, а кроме того, чистым либо разноцветным следам. В особенности подарки, персональные принадлежности либо прочие «случайные» объекты, позабытые путешественниками в последствии кропотливого осмотра (полной или частичной разборки). Неукоснительный осмотр полевых телефонных аппаратов и прочих линий связи от приспособления вплоть до распределительной коробки.

При проведении осмотра особенное внимание уделяется тайным и труднодоступным участкам, так как, собственно, они представляют максимальный интерес для персон, устанавливающих ЗУ. Для облегчения процедуры поиска используют специальные фонари и зеркала, представленные на рисунках 2.2 и 2.3.

Но подобные несложные устройства не всегда удобны и результативны, следовательно в практике, нередко, используют технические средства видеонаблюдения, намеренно адаптированные с целью осмотра труднодоступных зон.

Рисунок 2.2 – фонари Mag–Lite (оборудованы устройством, позволяющим изменять световой пучок от точечного до рассеянного)

Рисунок 2.3 – Зеркало, предназначенные для проведения осмотра в труднодоступных местах

Следующий метод – это контроль с помощью средств видеонаблюдения. К современным средствам видеонаблюдения относят оптикоэлектронные системы, которые условно можно разбить на две группы:

- эндоскопическое оборудование;
- досмотровые портативные телевизионные или видеоустановки.

Перечень эндоскопической продукции содержит в себе полную гамму волоконно–оптических фиброскопов, жестких бароскопов, а кроме того видеоскопов, дозволяющих реализовывать обследование труднодоступных зон. Приметной характерной чертой данных приборов представляется расположение микролинзы в конце мелкой эластичной трубки либо жесткой трубки, что работает как устремляющим компонентом, так и пучком волокон, специализированным с целью передачи. Изображение защитного рукава выводится с объектива в фотоокуляр либо ПЗС. В определенных видах эндоскопов матрица ПЗС находится напрямую на конце выявления канюли либо трубки. Сигнал передается с выхода матрицы на блок преобразования по кабелю либо радиоканалу, а потом на дисплей.

Гибкие фиброскопы предназначены для проникновения сквозь сложные изгибы различных каналов, представлены на рисунке 2.4.

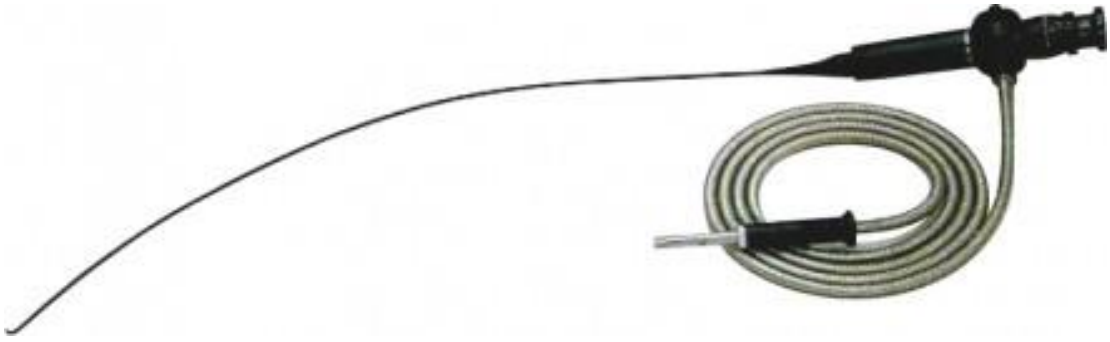

Рисунок 2.4 – Фиброскоп *PK* 1760

Барометры используются для проверки узлов, и узлы могут быть доступны через узкие прямые каналы. В отличие от фиброскопов, они оснащены жесткими стержнями вместо гибких рукавов. Функция видеоосциллографов заключается в том, что они позволяют выводить изображения в режиме реального времени на телевизионный монитор, предоставляя фотографии и / или видеофайлы, такие как устройства PK 1700. Видеоосциллографы позволяют отслеживать удаленные объекты на расстоянии до 22 м.

Общим минусом эндоскопических приборов является тот фактор, что они скорее рассчитаны на постоянное тщательное исследование, нежели в стремительный оперативный осмотр. Помимо этого, нередко данные концепции обладают многомодульной конфигурацией с кабельными соединениями, их многофункциональные блоки никак не минимизированы по весу и габаритам (PK 1765, PK 1700). Очевидны и трудности с скорой подготовкой к работе, переносом концепции и сохранением ее целостности. Вдобавок одно значительное свойство заключается в не всегда приемлемом качестве наблюдаемого при помощи фотоокуляра изображения.

Рисунок 2.5 – Бароскоп *PK* 1700–*S*

Сравнительный анализ разных видов эндоскопического оборудования выявляет, что лучшее свойство изображения можно получить с помощью

видеоэндоскопов, помимо этого, фактически безграничное число наблюдателей смогут смотреть и контролировать на телевизионном мониторе. В то же время подобное оборудование никак не может использоваться оператором и не годится для стремительной смены позиций контроля и обхода объектов. Для данных целей больше годится переносное эндоскопическое оборудование (к примеру, фиброскоп MR-660V, MM-013C либо PK 1760).

Следующий метод - досмотровые переносные телевизионные системы. Досмотровые переносные телевизионные системы дают возможность объединить плюсы высочайшего качества изображения с наибольшим удобством использования оборудованием при осмотре. Это достигается посредством конструктивного союза в едином устройстве миниатюрной телевизионной камеры, регулируемой штанги и телевизионного монитора.

Такое оборудование намеренно разрабатывается для нужд таможенных служб, однако довольно эффективно может быть применено и с целью отыскивания ЗУ.

В качестве примера можно привести носимое досмотровое видеоустройство Альфа–4, в комплект которого входят следующие основные компоненты:

- телескопическая штанга с черно–белой видеокамерой и источником инфракрасной подсветки, позволяющие досматривать объекты на удалении до 2,5 м;

- миниатюрный жидкокристаллический видеомонитор, размещаемый в руке оператора;

- специальный жилет, носимый поверх одежды.

В жилете расположены пульт управления и индикации, малогабаритный микрофон, аккумуляторный источник питания и трансмиттер телевизионного сигнала с антенной. Последний применяется в том случае, если нужна передача изображения в неподвижную телевизионную станцию с целью наиболее кропотливого контроля и документирования.

Другим примером реализации переносной телевизионной аппаратуры осмотра может служить концепция S–1000 («Кальмар»), обладающая аналогичной сборкой. Ее характерными особенностями являются следующие:

- изделие оборудовано пылевлагозащитным и ударопрочным корпусом, предохраняющим приспособление от воздействия находящейся вокруг среды, а изоляция камеры дает возможность осуществлять осмотр в том числе и в жидких средах;

- цилиндрический корпус камеры с интегрированной инфракрасной подсветкой гарантирует предельно возможную для данного оборудования умение проникновения в труднодоступные зоны;

- угловое положение камеры изменяется с помощью гибкой концевой штанги или фиксируемого шарнира;

- телевизионный сигнал и питание передаются по кабелю, пропущенному изнутри телескопической штанги. Здесь же гарантируется машинальная подмотка лишнего кабеля на интегрированный подпружиненный барабан;

- компактный монитор с электронно–лучевой трубкой крепится на штанге с помощью регулируемого кронштейна.

Еще один немаловажный метод – применение металлодетекторов. Минусом визуального осмотра является потребность долгой повышенной концентрации внимания оператора, что не всякий раз предоставляет надежный результат. Следовательно, последующий этап в увеличении производительности раскрытия ЗУ связан с объединением возможностей визуального и детекторного исследований.

Исследование детекторов относится к использованию оборудования, которое определяет определенные физические характеристики контактным или бесконтактным способом. Это оборудование указывает на некоторые аномалии в зоне контроля в виде неоднородностей, характерного излучения или конкретных веществ. С точки зрения достоверности проверки с использованием детектора важно, чтобы, если параметры, используемые для проведения проверки, превышали указанный порог, они генерировали аудио или оптические сигналы. Следовательно, имеет место не только идентификация, но и желаемое позиционирование устройства или объекта. Все дальнейшие рассмотренные методы являются детекторами.

Металлоискатели предстают более легким видом детекторов ЗУ, функционирующим согласно принципу раскрытия металических объектов (компонентов ЗУ) в непроводящих и слабопроводящих средах (дерево, одежда, пластик и т. п.). Детекторы бывают равно как ручного, так и арочного вида. Безусловно, что для вышеопределенных целей годятся только лишь ручные приборы. В наше время знакомы сотни модификаций металлодетекторов. Тем не менее согласно принципу работы, они практически никак не различаются друг от друга, а их ключевые характерные черты составляют только лишь потребительские и эксплуатационные характеристики.

Почти все нынешние металлоискатели нужны с целью отыскивания предметов из черных и цветных металлов. В данном случае умение определения диапазона находится в диапазоне от 10 вплоть до 500 миллиметров и находится в зависимости от свойства предмета. Все приспособления имеют звуки и порой световые сигналы. Ниже перечислены последующие виды металлоискателей:

АКА 7202М – селективный металлодетектор, предствленный на рисунке 2.6, предназначенный для поиска металлических предметов в диэлектрических и слабопроводящих средах. Подает различные звуковые сигналы при приближении к предметам из черных и цветных металлов. Максимальная дальность обнаружения: 80 мм – винт М3×7; 100 мм – диск 15×1 мм. Питание – «Крона» 9 В.

Рисунок 2.6 – Металлодетектор АКА 7202М

МАРС – металлодетектор, представленный на рисунке 2.7, предназначенный для оперативного поиска предметов из черных и цветных металлов. Питание – «Крона» 9 В.

Рисунок 2.7 – Металлодетектор МАРС

СТЕРХ–92АР – металлодетектор, представленный на рисунок 2.8, предназначенный для поиска металлических предметов в диэлектрических и слабопроводящих средах. Максимальная дальность обнаружения металлических предметов: 250 мм – диск 20×1 мм; 600 мм – пластина 100×100×1 мм. Питание – «Крона» 9 В.

Рисунок 2.8 – Металлодетектор С*ТЕРХ*–92*АР*

МИНИСКАН – малогабаритный селективный металлодетектор, представленный на рисунке 2.9, предназначенный для оперативного обнаружения металлических предметов. Подает различные звуковые сигналы при приближении к предметам из черных и цветных металлов. Не нуждается в предватительных настройках. Питание – «Крона» 9 В.

Рисунок 2.9 – Металлодетектор МИНИСКАН

2.3 Методы поиска ЗУ как электронных средств

В соответствии с классификацией, ключевыми методами раскрытия радиозакладных приборов представлены: использование индикаторов поля; использование специализированных приемников; использование комплексов радиоконтроля.

Все эти методы основаны на существовании радиоволн в этом типе памяти, которые не только имеют скрытую функцию, но также имеют много функций, которые могут быть распознаны как сигналы радиомонтажа. Поэтому, с точки зрения поиска, встроенные в радио устройства являются очень удобными объектами. Обратите внимание на эти функции.

Необходимо рассмотреть основные признаки излучения радиозакладок.

Первый признак – сравнительно высокий уровень излучения, определенный потребностью передачи сигнала за пределы контролируемого здания. Данный уровень тем выше, чем ближе к ЗУ располагаются приборы поиска.

Второй – присутствие гармоник в излучении радиозакладок. Данное условие представляется результатом потребности минимизации объемов ЗУ, а, следовательно, невозможности гарантировать отличную фильтрацию выходящего испускания. В передовых радиозакладках ослабление излучений на гармониках является лишь 40–50 дБ, следовательно, выявление этих нежелательных излучений без специальных проблем возможно на удалении вплоть до 10 м, безусловно, в случае если позволяет радиочастотный спектр используемого приемника контролирования.

Третий – возникновение нового источника в как правило свободном частотном спектре. При этом диспетчер, выполняющий контроль, обязан весьма хорошо разбираться в общей радиоэлектронной обстановке и понимать, что и в каких спектрах имеет возможность работать.

Четвертый сопряжен с применением в ряде радиозакладок направленных антенн. Это приводит к мощной локализации испускания, то есть существенной неравномерности его степени в границах регулируемого предмета. На расстояниях в несколько метров этот эффект лучше всего проявляется для гармоник основного излучения.

Пятый признак связан с отличительными чертами поляризации излучения радиозакладок. Дело в том, что при изменении пространственного положения либо ориентации приемной антенны прослеживается модификация степени абсолютно всех ключей. тем не менее однотипные удаленные источники 1-го спектра ведут себя приблизительно одинаково, в то время как сигнал закладки изменяется отлично от остальных. На практике данный результат наверняка замечали те, кто именно осуществлял поиск ЗУ с применением анализаторов спектра.

Шестой признак заключается в изменении («размывании») диапазона излучений радиомикрофонов при происхождении каких–либо шумов в контролируемом помещении. Он выражается только в том случае, в случае если ЗУ функционирует без кодировки транслируемой информации.

Седьмой признак сопряжен с возможностью человека различать акустические сигналы. Таким образом, в случае если закладка функционирует без маскирования, то диспетчер, выполняющий поиск ЗУ, слышит шум помещения либо тот тестовый сигнал, что непосредственно сформировал. В аппаратном виде данный результат обыгрывается разного рода корреляторами и, таким образом именуемой, акустической завязкой. При выявлении закладок с маскированием передаваемой информации сигнал походит нечёткую речь либо какофонию, в случае если в свойстве тестовых используются, соответственно, речевой сигнал либо музыка. В конечном случае с целью аппаратного раскрытия нужны специализированные методы корреляции, однако, как правило можно обойтись и просто зондированием импульсными акустическими сигналами. В конечном итоге, при использовании кодировки, скорее всего, диспетчер будет слышать белый шум, и скорее всего практически никакая корреляция со звуком в этом случае не поможет.

Восьмой признак сопряжен с периодом работы радиозакладок. Таким образом, наиболее простые из них, то есть никак не оснащенные схемами дистанционного включения и VOX, станут работать постоянно в течение определенного времени. Для закладок с VOX свойственен неровный режим деятельность в дневное время и фактически абсолютное безмолвие в ночное время. Устройства с дистанционным включением обязательно имеют несколько коротких сеансов в течение дня и практически наверняка будут работать в период переговоров, важных с точки зрения установившего их лица.

Применительно к телефонным закладкам присутствие восьмого признака проверяется весьма просто: в случае если какое–либо радиоизлучение появляется параллельно с поднятием трубки и пропадает, когда трубка положена, в таком случае данное радиоизлучение непосредственно либо непрямо связано с утечкой данных.

Вышеприведенный список признаков не является исчерпывающим и может быть существенно расширен.

2.4 Методы, применяемые для поиска радиоустройств

Для поиска сигналов радиозакладок используют три метода – метод разности панорам, аудио–визуальный метод и экспертный метод. Они являются универсальными, т.е. предназначены для поиска любых сигналов.

Методы поиска различаются друг от друга по степени участия в них оператора. По степени автоматизации первейшим следует метод разности панорам. Аудио–визуальный метод и экспертный метод допускается считать автоматизированными методами.

Учитывая, что деятельность исполняется со слабыми сигналами, она обычно может быть распознана только одним человеком в соответствии с его интуицией и опытом, поэтому метод поиска может быть организован в обратном порядке автоматизации в соответствии с качеством полученных результатов. Наилучшие результаты могут быть получены экспертными методами. Аудиовизуальный метод работает хорошо, в то время как метод панорамного сравнения отключает числа.

Все методы на первом этапе требуют получить две панорамы сигналов – с выключенным тестовым сигналом и с включенным тестовым сигналом. Чтобы уменьшить уровень шумов в панорамах необходимо использовать алгоритмы усреднения.

Рассмотрим представленные методы.

Первый метод – это метод разности панорам. Для поиска сигналов радиозакладок методом разности панорам проводятся два измерения уровней. Первое измерение производится несколько раз вне исследуемого помещения, чтобы сформировать базовую модель частот. Второй замер производится внутри исследуемого помещения.

Затем вычтите базовое значение горизонтальной карты из горизонтальной карты исследуемой комнаты. Под порогом, заданным оператором, зарегистрированная частотная точка сигнала второго графика, превышающая сигнал первого графика, попадает в список частот возможных сигналов встроенного устройства.

Выводы по методу разности панорам:

- участие оператора: необходимо только для включения сканирования заданного диапазона частот и запуска процесса разности двух панорам частот;

- эффективность метода: хорошо обнаруживает только сильные сигналы, у которых отношение сигнал/шум превышает 6–10дБ;

- время поиска: 4 минуты.

Аудио–визуальный метод отыскивания сигналов радио–излучаемой закладки максимально прост. В добавление к отлично всем известному аудио контролю, что использовался при применении селективных микровольтметров, в данном методе применяется метод визуального контроля электромагнитного диапазона.

Первый этап метода включает в себя получение двух спектров электромагнитной среды - замыкание и размыкание тестовых сигналов (начиная с метода панорамного дифференциала). Далее оператор визуально проверяет полученную графику и проверяет наличие подозрительных сигналов.

Выводы по аудио–визуальному методу поиска:

- участие оператора: оператор участвует во всех этапах работ, степень автоматизации – высокая;

- эффективность метода: обнаруживает практически все сигналы с положительным отношением сигнал/шум для выбранной полосы пропускания;

- время работы. для типового технического средства «монитор ПЭВМ» время поиска составляет 3–10 минут.

Экспертный метод поиска является модификацией метода поиска сигналов на частотах гармоник. Любая периодическая последовательность цифровых сигналов образует в радиоэфире ряд гармоник.

Данный метод широко используется при ручных исследованиях для сокращения времени работы.

К минусам метода ручного поиска сигналов по гармоникам относится тот факт, что диспетчер не ведает верную частоту сигнала первой гармоники, что отличается для каждого случая исследуемых технических средств (как правило расширяется от основной частоты вплоть до 10 -5 кварцевый генератор). следовательно в последствии настройки на примерную частоту следующей гармоники диспетчер обязан искать сигнал вблизи этой частоты. всякий сигнал в радиоэфире имеет оптимальные для приема полосы пропускания. Они находятся в зависимости от полосы занимаемых частот сигналом и степени шума. При ручных исследованиях искать сигнал и его подходящие условия приема трудно, так как это занимает весьма немало времени.

Метод экспертного поиска возместит последующие минусы: частота первой гармоники измеряется весьма четко, а затем частота каждой субгармоники не ищется, а прогнозируется. в последствии настройки на данную частоту будут обнаружены наилучшие условия приема, а частота первой гармоники будет улучшена частотой обнаруженного сигнала.

Выводы по экспертному методу обнаружения:

- участие оператора: оператор участвует во всех этапах работ, степень автоматизации – высокая;

- эффективность метода: самая высокая эффективность из всех методов, обнаруживает все сигналы, которые можно обнаружить с предельно

достижимой чувствительностью измерительного прибора. Обнаруживаются те сигналы, которые невозможно обнаружить ни одним другим методом, включая исследование в ручном режиме;

- время работы: для типового технического средства «монитор ПЭВМ» время поиска составляет 8–15 минут.

2.5 Выводы по главе

В данной главе были приведены методы обнаружения закладных устройств. Методы обнаружения закладных устройств были определены, как обнаружение ЗУ по физическим признакам и электронных признакам. Приведены рекомендации к каждому из методов. Также приведены три основных метода радиозакладок путем радиосканирования.

Методы поиска различаются друг от друга по степени участия в них оператора. По степени автоматизации первейшим следует метод разности панорам. Аудио–визуальный метод и экспертный метод допускается считать автоматизированными методами.

Все методы на первом этапе должны получить две панорамы сигнала - отключить тестовый сигнал и включить тестовый сигнал. Чтобы снизить уровень шума в панораме, необходимо использовать алгоритм усреднения.

Был проведен анализ сканирующих приемников по различным признакам и представлен в приложении А.

3 Алгоритмы поиска и требования к аппаратуре при поиске радиоэлектронных устройств

В сегодняшнем сверхтехнологичном мире поиск радиоканалов средств не санкционированного съёма информации усугубляется некоторыми факторами. Во–первых, создатели средств не санкционированного съёма данных используют всё наиболее непростые способы, а также алгоритмы скрытия излучения своих приборов. На этапе установки закладных девайсов также используются специфические способы маскирования, к примеру, формируется канал съёма данных вместе с учётом излучения действующих возле объекта легальных устройств, препятствующих работе поисковой техники.

Во–вторых, не прекращается рост использования радиоэфира в целях организации связи, обмена данными, а также команд управления, сегодня уже фактически весь частотный диапазон задействован под работу легальных радиопередатчиков. Данное провоцирует запутывание эфирной обстановки, в особенности в больших населенных пунктах. К примеру, в Столице в спектре вплоть до 3000 МГц, в зависимости от района, а также критерий приёма, можно определить больше 4000 радиосигналов.

В наше время период проблемы улучшения способов отыскивания неразрешенных радиопередающих и радиозакладных приборов (закладок) представлены важными по причине настойчивого возрастания значимости информативной защищенности в общегосударственной и обыкновенной областях работы, а кроме того перспектив промышленных денег поиска. нынешние закладки разумно различаются товарищ с товарища, однако имеют все шансы пользоваться последующие единые способы сокрытия подделывала передачи сведений:

- метод накопления данных с последующей их передачей в течение заданного промежутка времени (до нескольких миллисекунд);
- метод накопления информации с последующей многократной передачей через определенные интервалы времени или после получения внешней команды;
- передача с возможной перестройкой частоты канала;
- использование широкополосных шумоподобных сигналов, когда энергия сигнала сосредоточена в широкой полосе частот и не имеет выраженного превышения над шумами;
- выбор диапазона частот излучения сигнала рядом с сильным источником легитимных сигналов, которые перегружают прием поиска сканирующего устройства при недостаточном диапазоне сканирования;
- маскировка под стандартные каналы связи.

Перечисленные выше способы никак не обхватывают всегда вероятные основы конспирации, применяемые закладками. сведения способы имеют все шансы таким (образом ведь и сочетаться товарищ с ином. Какие б трудные методы сокрытия подделывала передачи сведений никак не

применяли закладки, они всегда в равной мере имеют все шансы обнаружить себе установленной периодичностью передачи сведений либо применением узкого спектра частот. сведения особенности выявляются оператором рядом скоротечном разборе частотного диапазона. собственно частотно–временной периодичностью закладки различаются с ненамеренного гула, что допускается утвердить из-за закладку.

При поиске источников излучения такого типа не стоит полагаться на их мгновенное обнаружение. Чтобы найти закладку необходим радиомониторинг в течение длительного времени: до суток или более с последующим анализом всех найденных сигналов в представлении спектрограммы.

Исходя из этого и предъявляются требования к алгоритмам, которые должны быть реализованы в программном обеспечении комплекса.

Одними из основных характеристик сканирующего приемника являются диапазон частот сканирования и скорость сканирования.

Для поиска закладок наиболее часто используется режим автоматического сканирования приемника в заданном диапазоне частот. При этом режиме устанавливаются начальная и конечная частоты сканирования исходя из возможностей сканирующего приемника, шаг перестройки по частоте, вид модуляции и порог чувствительности для обнаружения закладок с низким уровнем сигнала.

Для скрытия канала передачи информации разработчики закладок используют множество методов и алгоритмов, среди которых выделяется использование стандартных каналов связи. Это значит, что нелегально установленные закладочные устройства передают перехваченную информацию в частотных диапазонах легальных стандартов, используют их протоколы передачи информации, имеют ту же самую частотную характеристику – являются по сути такими же легальными устройствами и отличаются от них только фактом нелегальной установки для негласного получения информации. Под стандартными каналами передачи информации понимаются широко распространённые, повседневно используемые большим количеством устройств стандарты, к которым можно отнести Wi–Fi, Bluetooth, ZigBee .

3.1 Алгоритм поиска радиозакладок основанных на легальных протоколах передачи данных

Как ранее упоминалось, гаджеты негласного съема информации не редко маскируют под бытовые каналы передачи данных , в частности – Wi–Fi, Bluetooth, ZigBee.

Маскировка под подобные протоколы кажутся на первый взгляд преимуществом, но все же метод имеет весомый изъян, по причине которого профессионал не будет его использовать. Но попричине того, что в обыденности нам приходится иметь дело с новичками, следует рассматривать данную методику, как угрозу, и искать алгоритмы и средства противодействия.

Главной слабостью ЗУ основанных на передаче данных легальными каналами связи является то , что известны протоколы по которым осуществляется обмен информацией. Для идентификации и локализации устройств необходимо произвести ряд мероприятий, описанных ниже.

Сначала необходимо произвести развертывание и определить зону сканирования (зону уверенного приема) комплекса предназначенного для обнаружения ЗУ. Выполнить определенные организационные мер, направленные на упрощение задачи по выявлению ЗУ , путем отключения всех устройств, излучающих сигнал в зоне сканирования антены, для выявления ЭУНПИ. Лишние сигналы «засоряют» панорамы полученные в результате радиоманиторинга. При наличии такой вазможности, отключить устройства в диапазоне 2,4 ГГц, в обратном случае производим «маневр временем», т.е. выбирается подходящий промежуток времени, когда представится возможностьреализовать данные действия, чаще всего ночное время.

Затем подключаем в произвольной последовательности, легальные устройства передачи данных, в режим опроса. А именно подключение устройств Wi–Fi, Bluetooth, ZigBee , с целью идентификации устройств работающих не в замаскированном режиме и дают отклик на сигнал опроса. Приналичии отклика можно сделать вывод , что в зоне поиска имеется ЭУНПИ. Далее выполняем последовательность действий для лаколизации по демаскирующим признакам. Поиск ЭУНПИ методом опроса через устройство беспроводной коммуникации Wi–Fi реализуетсяпри помощи специального ПО, например MacAddress Scaner, формируя полученные данные и сравнивая их с о списком запрашиваемых Mac-адресов , находящихся в зоне опроса Wi–Fi модуля, что дает возможность определить физические адреса всех опрошенных устройств.

Поиск устройств, основанных на принципе передачи данных по Bluetooth, осуществляется с помощью любых устройств, имеющих Bluetooth–модуль (телефоны, ноутбуки) Принцип метода довольно банален и реализуется на включении функции «Поиск устройств». В случе, если ЭУНПИ работает не в скрытом режиме, на опрашивающем утройстве отображается сетевое имя или же MAC-адрес.

ЭУНПИ на основе ZigBee рекомендуется опрашивать с устройства работающего в режиме координатора, при которой отправляется команда «определение узла». В следствии такой команды ЭУНПИ в ответ отправит пакет, содержащий 16-битовый сетевой адрес и 64-битовый физический адрес. Начало алгоритма поиска ЭУНПИ представлено на рисунке Рисунок 3.1.

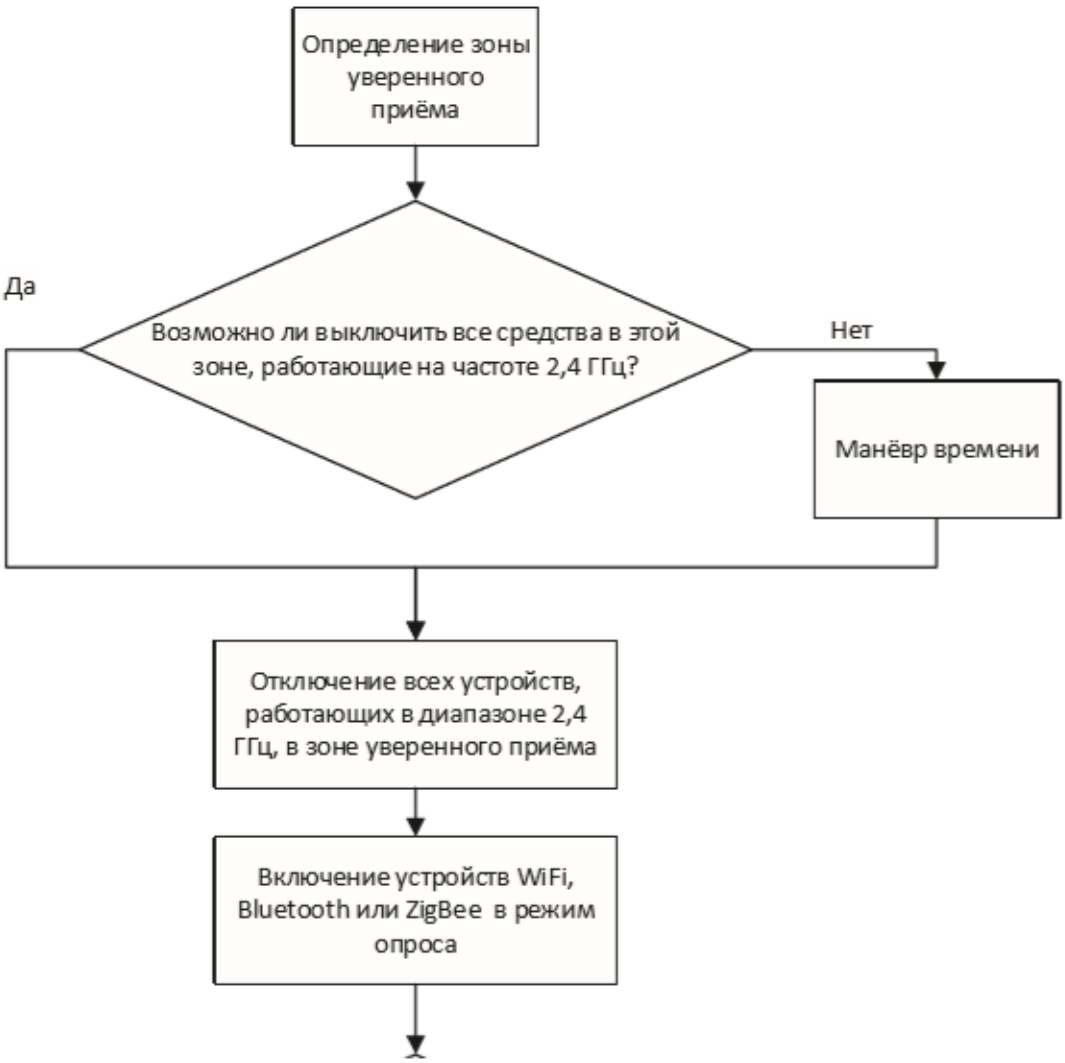

Рисунок 3.1 – Алгоритм методики выявления ЭУНПИ построенных на базе средств беспроводной связи (часть 1)

В случае, когда злоумышленник понимает, что в режиме работы не скрытом от опроса, устройство будет обнаружено даже без применения специального оборудования, а в скрытом режиме вероятность растяжение времени до обнаружения больше и всё же скрывает, тогда необходимо применять специальные устройства для радиомониторинга.

Нужно применять методы радио сканирования непосредственно в частотном диапазоне около 2,4 ГГц.Если же радиомониторинг не дал результата необходимо выполнить два следующих шага.

Далее необходимо произвести отключение всех электронных устройств в области сканирования. Исходными данными на данном этапе являются предположение, что источником питания ЭУНПИ является какой-либо электронный прибор. Затем фиксируется панорама при отключенных устройствах, далее произвольно включается устройство и зоны уверенного приема, и до включения каждого устройства панорама также фиксируется. Анализируя протоколы устройств беспроводной связи, можем определить, что

такие устройства выдают сигнал при включении. в случае обнаружения сигнала проводит мероприятия по локализации.

Данный этап основан на включении тестового (акустического) сигнала. Основан на предположении, что ЭУНПИ управляется системой VAS и выходит в эфир при подаче возбуждающего сигнала на микрофон. Для реализации необходимо добиться максимально возможная тишины. к Дарье подается возбуждающий акустический сигнал, соответственно параллельны фиксируется панорама до и после подачи сигнала. Далее после обнаружения сигнала локализуется ЭУНПИ. Продолжение алгоритма по обнаружению ЭУНПИ, на базе легальных устройств передачи данных представленна на рисунке 3.2.

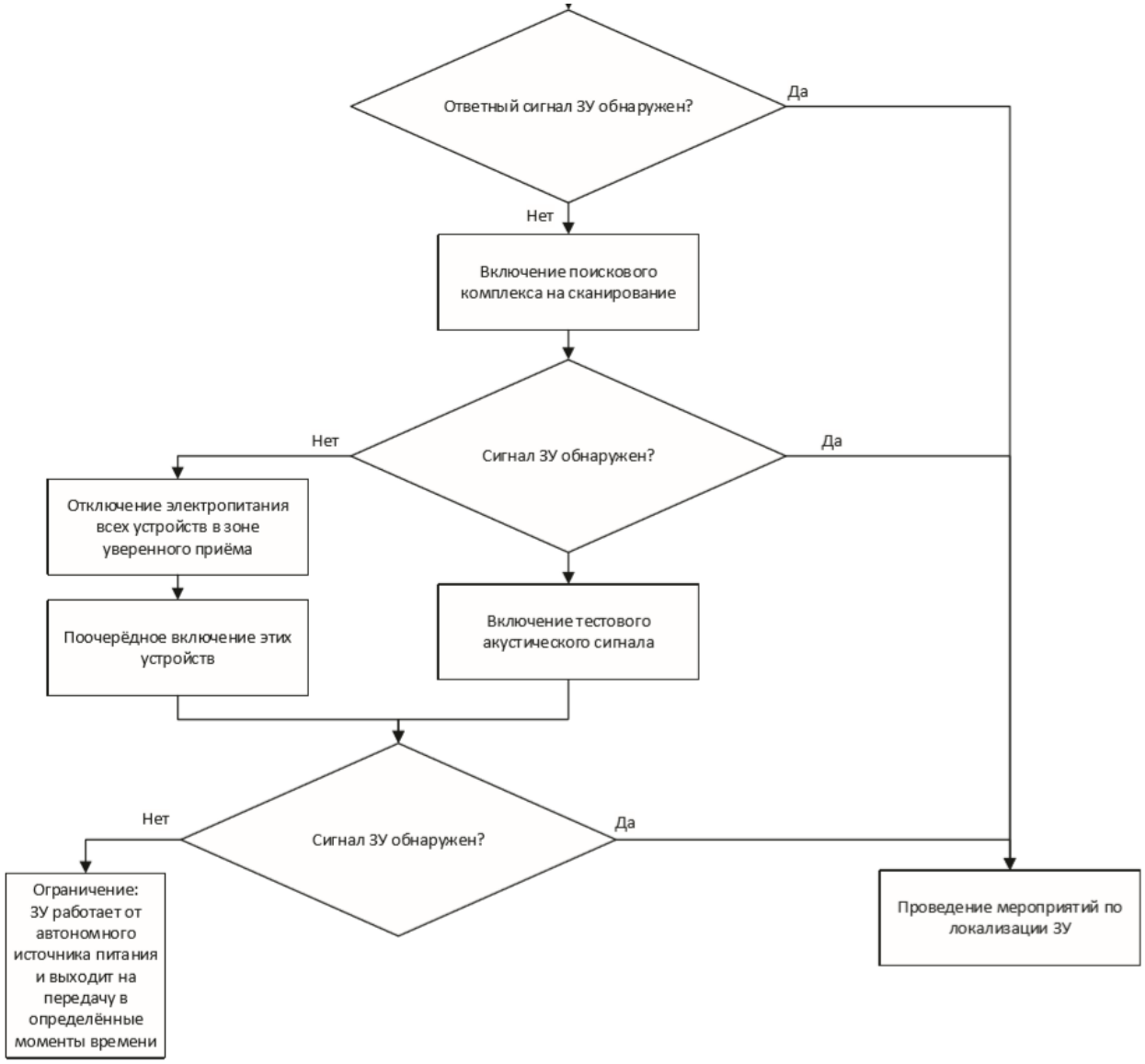

Рисунок 3.2 – Алгоритм методики выявления ЭУНПИ построенных на базе средств беспроводной связи (часть 2)

Стоит отметить, что данный алгоритм, позволяет лишь определить наличие (присутствие) ЗУ, а обнаружения необходимо производить другими устройствами (нелинейные локаторы, индикаторы поля и т.д.).

Данный алгоритм следует применять в самом начале процесса обнаружения ЗУ. Так, в случае если устройство работало подданным протоколом, это сократит время обнаружения. А также бывали случаи, когда подобное устройство была установлена для отвода глаз, и скрывала основное устройство. В случае если не удалось обнаружить устройство при сканировании вероятно передача данных происходит в ней периодически.

3.2 Алгоритм обнаружения периодически передающих радиозакладных устройств

Методы моделирования процесса обнаружения ЗУ, периодической передачей сигнала предложены в данной работе. В основном при поиске радиозакладок используются специальные приемники для радио сканирования, в котором задаются диапазоны сканируемых частот и устанавливают в автоматический режим. Предложенная модель дает возможность выработать рекомендации, которые позволяют оптимизировать процесс поиска во временной области, также повышает вероятность идентификации ЗУ.

При автоматическом режиме радио сканирующих приемников в зависимости от их характеристик устанавливаются определенные физические величины, которые представлены в таблице 3.1, также там представлены величины характеризующие ЗУ.

Таблица 3.1 – Расшифровка обозначений

Сканирующий приемник	
Диапазон частот, МГц	[a;b]
Шаг сканирования, МГц	H
Скорость сканирования, шагов/с	V
Порог чувствительности приемника, В	S
Количество шагов сканирования	N
Максимальное количество периодов поиска	M
Время прохождения одного периода поиска, с	$t_{рабСП}$
Закладное устройство	
Несущая частота, МГц	F
Ширина полосы, МГц	Δf
Период повтора, с	T
Время работы, с	$t_{раб}$ЗУ

Амплитуда излучаемого сигнала, В	U

Выполнена процедура имитации процесса обнаружения, которая позволила вносить изменение в параметры сканирования и ЗУ. Определялось влияние сканирования приёмника в промежутках времени (число периодов поиска необходимых для обнаружения) от скорости сканирования в определённых указанных частотных диапазонах до момента идентификации ЗУ с установленными временем и периодичностью передачи данных на определенной несущей частоте.

Упрощённая блок-схема алгоритма поиска закладных устройств представлена на рисунке 3.3

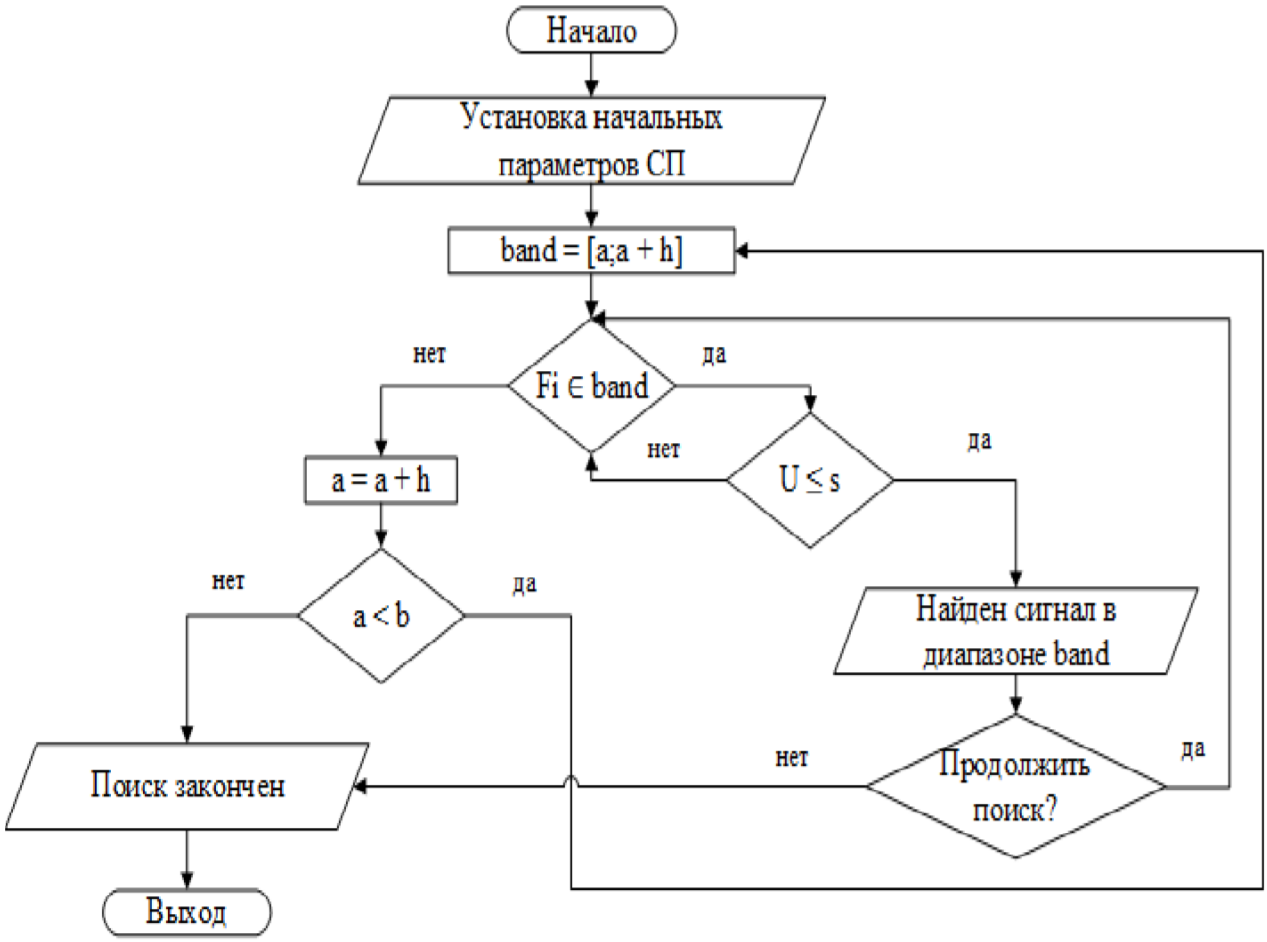

Рисунок 3.3 – Упрощенная блок–схема поиска СП

Данный алгоритм позволяет определить необходимое число периодов поиска в зависимости от исходных параметров, заданных в ЗУ и СП.

Устанавливая границы частотного диапазона от a до b и имея шага сканирования h, вычисляются количество шагов (3.1):

$$N = \frac{b-a}{h}, \qquad (0.1)$$

В параметрах СП устанавливается значение сканирование, определяющая количественное значение шагов, обработанных за одну секунду. Из этого следует выражение, позволяющее определить затраченное время за один период сканирования (3.2):

$$t_{рабСП} = \frac{N}{V} \tag{0.2}$$

Оперируя значением, полученным в (4.2) и характеристиками ЗУ, имеется возможность вычислить интервал времени, когда СП обработает частотный промежуток передачи ЗУ. Определи время необходимое на сканирование одного шага (3.3):

$$t_h = \frac{t_{рабСП}}{N} \tag{0.3}$$

После определяется необходимых промежуток времени по формулам (3.4) и (3.5):

$$t_1 = t_h \times floor\left(\frac{f - \frac{\Delta f}{2}}{h}\right), \tag{0.4}$$

$$t_2 = t_h \times ceil\left(\frac{f + \frac{\Delta f}{2}}{h}\right) \tag{0.5}$$

Таким образом, чтобы определить необходимое количество периодов, необходимых для идентификации ЗУ, нужно определить момент времени, при котором закладное устройство будет включаться тогда, когда сканирующий приемник будет сканировать частоту, на которой работает ЗУ. Вычислить этот промежуток времени можно, я найдя время начала работы ЗУ ($t_{нач.рабЗУ}$), изменяя значение периодов и времени ожидания (i), по отношению к началу работы СП:

$$t_{нач.рабЗУ} = \left[\sum_{1}^{i}(t+T)\right] \bmod t_{рабСП}, i = 1,2,3...M \tag{0.6}$$

При помощи формулы (3.6), изменяя значение i на 1, сравнивая полученные значения применяем выражение:

$$\left[t_{нач.рабЗУ}; t_{нач.рабЗУ} + t_{рабЗУ}\right] \in \left[t_1; t_2;\right] \quad (0.7)$$

В момент, когда закладное устройство попадает, в рабочем режиме в данный промежуток времени, его можно считать раскрытым. После, чтобы найти необходимое количество периодов сканирования (затраченное время), применяя вычисленное i необходимо:

$$T_{поиска} = \left[\sum_{1}^{i} t + T\right] div\, t_{рабСП} \quad (0.8)$$

Значение параметров i, вариативно до момента окончания заданных периодов сканирования.

Если ЗУ не было идентифицировано, то вероятнее всего произошёл процесс синхронизации закладного устройства и сканирующего приемника. Следовательно, необходимо изменить исходные параметры сканирующего приемника.

Было произведено 4 эксперимента, результаты которых были отражены на соответствующих графиках. Каждый эксперимент имел скорость сканирования от 10 до 100 каналов в секунду. Отличие 1, 3, 4 экспериментов заключается в сканируем диапазоне. Вервый, второй эксперимент различны во времени работы закладного устройства, параметры моделирования представлены в таблице 3.2.

Таблица 3.2 – Параметры моделирования

№	Диапазон сканирования, МГц	Шаг перестройки частоты, МГц	Скорость сканирования, каналов/с	Время работы закладки, с	Период работы закладки, с	Полоса частот закладки, МГц
1	0–1000	1	от 10 до 100	1	5	99,5–100,5
2	0–1000	1	от 10 до 100	0.5	5	99,5–100,5
3	0–500	1	от 10 до 100	1	5	99,5–100,5
4	0–200	1	от 10 до 100	1	5	99,5–100,5

Результаты первого эксперимента представлены на графиках на рисунке 3.4.

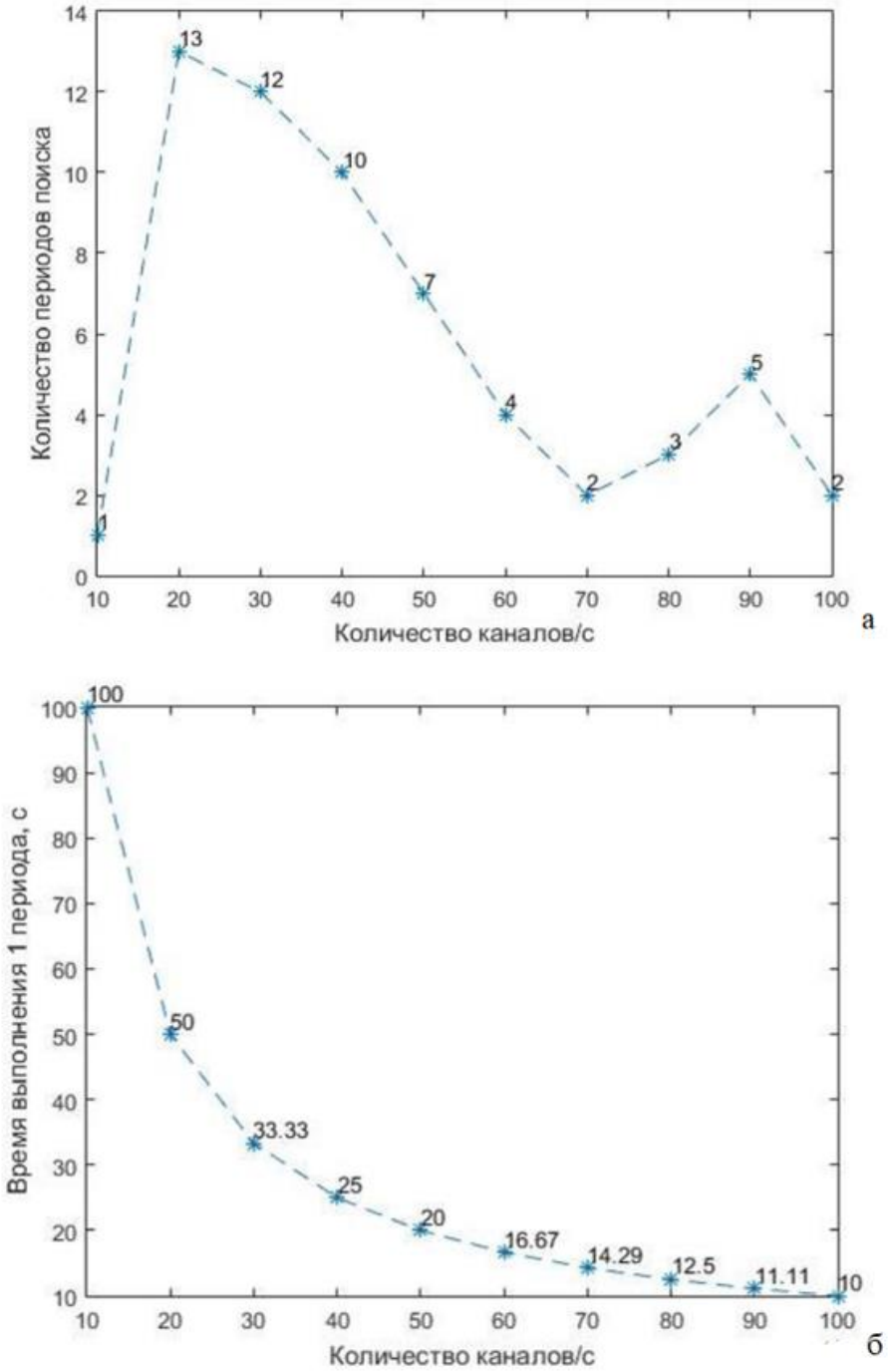

Рисунок 3.4 – График зависимости количества периодов поиска от скорости сканирования (а); Время выполнения одного периода в зависимости от скорости сканирования (б) (эксперимент №1)

Из графиков следует, что при росте скорости сканирования, число необходимых для обнаружения периодов поиска изменяются по разному не всегда убывает. к для 10 каналов/с было затрачено меньше всего периодов и сканирующее устройство обнаружило ЗУ при первом периоде. несмотря на это общее время понадобившееся для поиска при 10 каналах/с составила 100 секунд, что больше чем при скорости сканирования 60-100 каналов/с, это

связано с тем, что при росте скорости сканирования уменьшается время необходимое на один период. При скорости 60-100 каналов/с общее время составила от 68 с до до 20 с, соответственно. Несмотря на аналогичный исходные данные с первым экспериментом во втором эксперименте было изменено время работы ЗУ с 1 секунды до 0,5 секунд.

Результаты второго эксперимента представлены на рисунке 3.5.

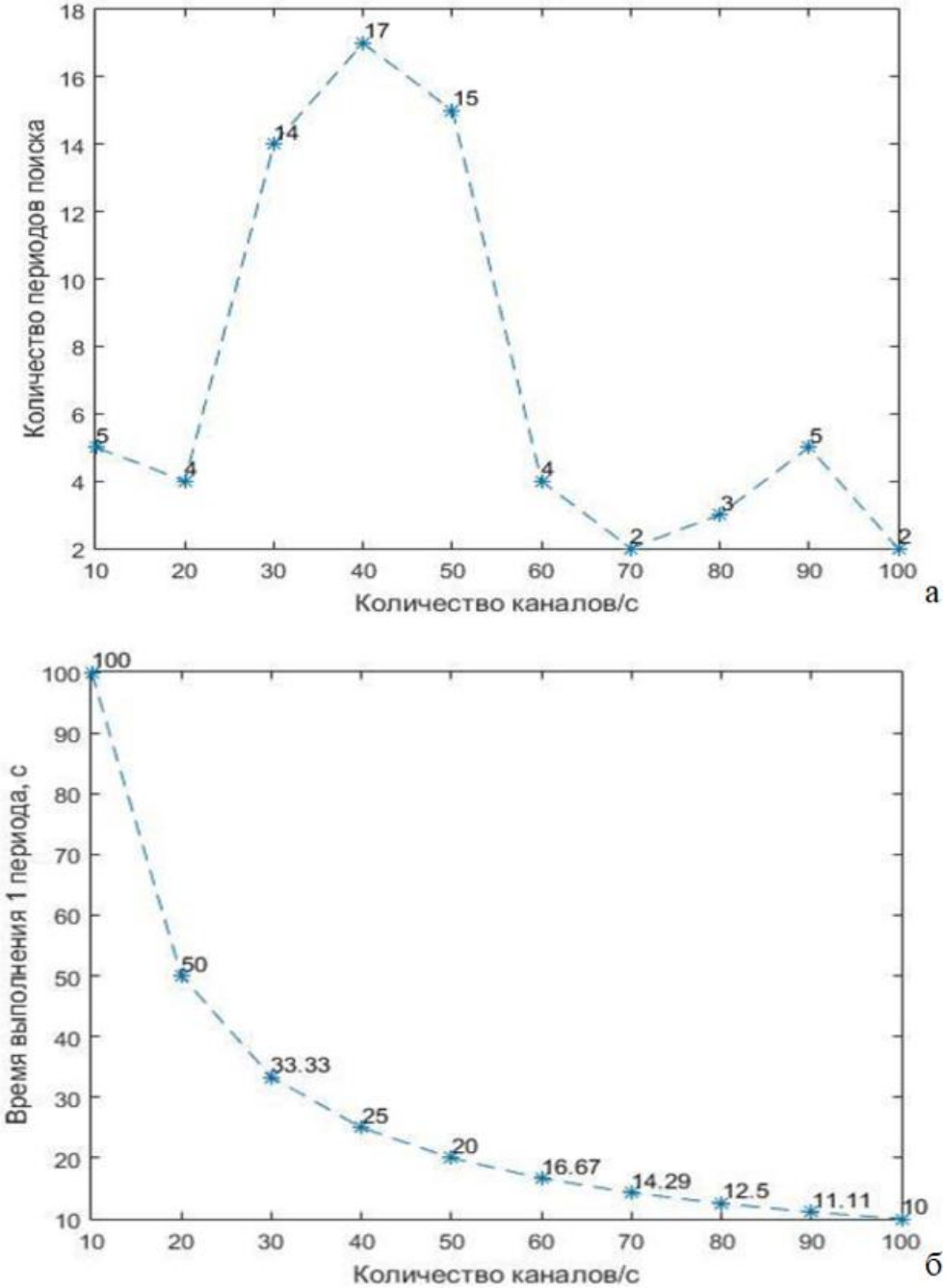

Рисунок 3.5 –График зависимости количества периодов поиска от скорости сканирования(а); Время выполнения одного периода в зависимости от скорости сканирования (б) (эксперимент №2)

Если сравнивать результаты второго эксперимента с первым экспериментом, можно определить тенденцию роста числа необходимых периодов при некоторых скоростях сканирования. Максимальное число периодов поиска в 1-ом при 20 каналах/с (13 периодов), во 2-ом при 40 каналах/с (17 периодов). Встретим эксперименте сокращён диапазон частот от от 0 до 500 МГц. Результаты представлены на графиках, изображённых на рисунке 3.6.

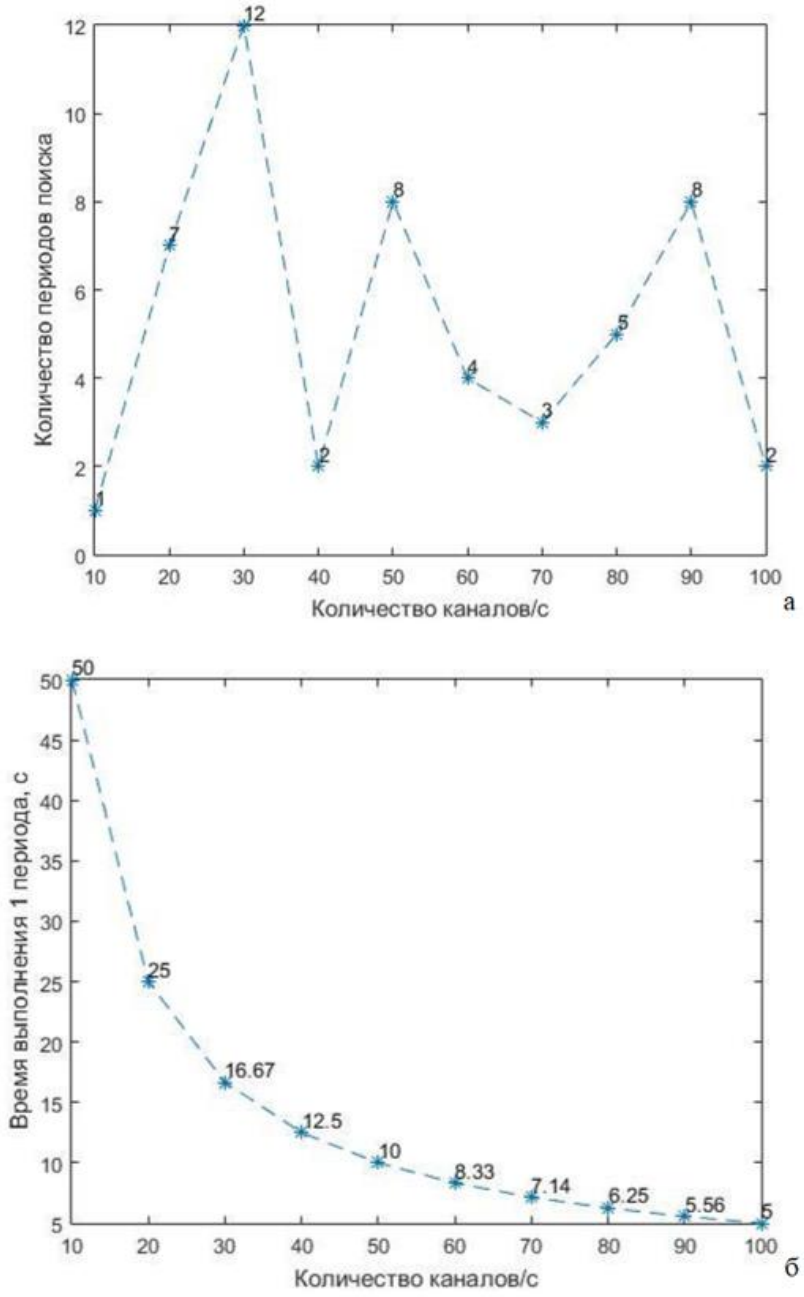

Рисунок 3.6 – График зависимости количества периодов поиска от скорости сканирования (а); Время выполнения одного периода в зависимости от скорости сканирования (б) (эксперимент №3)

Сокращение частотного диапазона сократило время, затраченное на один период сканирования. При данном эксперименте, также увеличение скорости сканирования не является гарантом того, что сократится необходимое количество периодов. В четвёртом эксперименте диапазон частот был сокращён в 2.5 раза по сравнению с третьим экспериментом, другие параметры остались неизменными. Результаты 4 эксперимента представлены на рисунке 3.7.

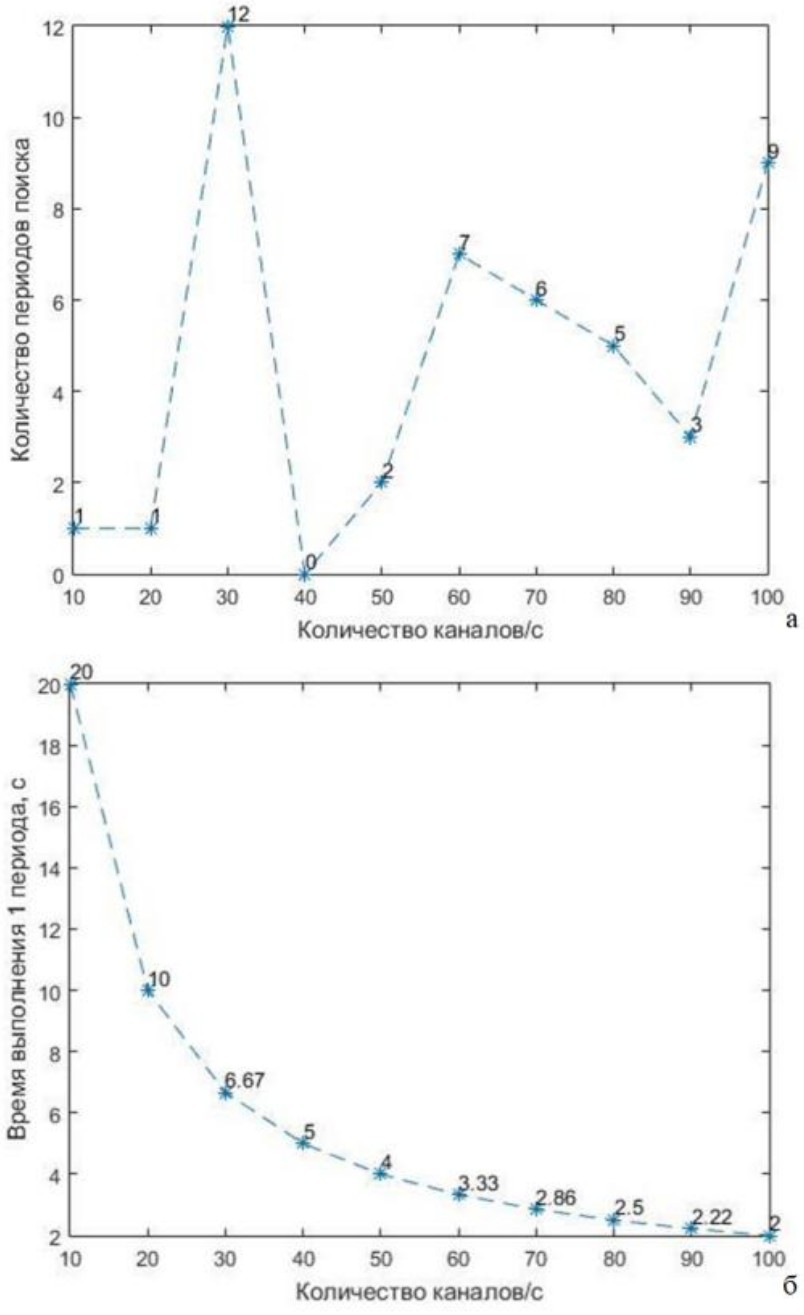

Рисунок 3.7 –График зависимости количества периодов поиска от скорости сканирования (а); Время выполнения одного периода в зависимости от скорости сканирования (б) (эксперимент №4)

Диапазон частот процесса сканирования в данном эксперименте был установлен в пределах от 0 до 200 МГц, что увеличило скорость сканирования в 2,5 раза по сравнению с предыдущим экспериментом. Также как и в предыдущих экспериментах видим, что нет прямой зависимости числа периодов поиска от скорости сканирования. Особенностью данного эксперимента является то, что при скорости сканирования 40 каналов/с закладное устройство обнаружено не было, это связано с тем, что время затраченное на один период сканирование и периодичность срабатывания закладных устройств кратны, что провоцируй синхронизацию данных объектов, т.е. момент времени сканирования необходимой частоты не совпадает с моментом времени, когда срабатывает закладное устройство. Основываясь на результатах полученных экспериментах 1-4, можно сделать следующие выводы:

- увеличение параметров скорости сканирования не всегда дает сокращение числа периодов, затраченных до момента обнаружения ЗУ. причиной этому является различие между периодами сканирования рабочего промежутка закладного устройства;
- на значение скорости сканирования оказывают влияние частотный диапазон сканируемого полосы шаг перестройки в ней;
- в 4-ом эксперименте при скорости сканирования 40 каналов/с, произошла синхронизация периодичности сканирование СП и периодичности срабатывания ЗУ, что составило 5 секунд, я по этой причине устройство не было обнаружено;
- значение периодов необходимых для обнаружения закладного устройства и аналитический счёт и примерно совпали, из этого следует, что можно использовать данные выражения и алгоритмы, как фундамент при формировании своих алгоритмов;
- чтобы повысить шансы для обнаружения закладных устройств, излучающих сигнал периодический, необходимо производить сканирование в несколько этапов с небольшой шириной частотного диапазона, а лучше всего использовать несколько сканирующих приемников.

Данные результаты получены в ходе проведения физического моделирования процесса поиска ЗУ. В качестве технической базы для проведения моделирования использовались – сканирующий приемник, соответствующий характеристикам, отраженным в таблице, а также ЗУ с характеристиками, представленными в таблице 4.2. Внешний облик ЗУ и сканирующего приемника, представлены на рисунке 3.8.

Рисунок 3.8 – Использованные в ходе эксперимента а) ЗУ и б) сканирующий приемник OSCOR OSC-500

3.3 Выводы по главе

В данной главе были предложены алгоритмы по противодействию устройствам негласного съема информации. Определены два алгоритма, для обнаружения закладных устройств, первое – как устройств, замаскированных под стандартные каналы связи. Второе – как устройств с периодической передачей данных.

Таким образом, исходя из результатов исследования можно дать рекомендации по реализации поисковой программы по обнаружению ЗУ, полагаясь на следующие выводы:

- увеличение параметров скорости сканирования не всегда дает сокращение числа периодов, затраченных до момента обнаружения ЗУ. причиной этому является различие между периодами сканирования рабочего промежутка закладного устройства;
- на значение скорости сканирования оказывают влияние частотный диапазон сканируемого полосы шаг перестройки в ней;
- в 4-ом эксперименте при скорости сканирования 40 каналов/с, произошла синхронизация периодичности сканирование СП и периодичности срабатывания ЗУ, что составило 5 секунд, я по этой причине устройство не было обнаружено;
- значение периодов необходимых для обнаружения закладного устройства и аналитический счёт и примерно совпали, из этого следует, что можно использовать данные выражения и алгоритмы, как фундамент при формировании своих алгоритмов;

- чтобы повысить шансы для обнаружения закладных устройств излучающих сигнал периодический, необходимо производить сканирование в несколько этапов с небольшой шириной частотного диапазона, а лучше всего использовать несколько сканирующих приемников.

Основываясь на два предложенных алгоритма, появляется возможность разработать автоматизированный комплекс по обнаружению ЗУ с беспроводной передачей данных. Корректируя указанные параметры, можно повысить вероятность обнаружения устройств негласного съема данных.

Данные результаты могут быть полезны не только в отрасли противодействия шпионажу, но и в области пеленгования летательных аппаратов.

4 Безопасность жизнедеятельности

Решение проблемы БЖД состоит в обеспечении нормальных и комфортных условий труда для людей в их жизни, в защите человека и окружающей его среды от воздействия вредных факторов, превышающих нормативно-допустимые уровни. Обеспечение и поддержание оптимальных и даже хороших условий деятельности и отдыха человека способствует его высшей работоспособности и продуктивности.

Обеспечение безопасности труда и отдыха способствует сохранению жизни и здоровья человека за счет снижения травматизма и заболеваемости.

Вопросы безопасной жизнедеятельности человека необходимо решать на всех стадиях жизненного цикла, будь то разработка, эксперимент или применение разработанной методики на практике.

Работа с вычислительной техникой по вредности относится к безопасным (риск смерти на человека в год составляет менее 0.0001). Тяжесть труда у работника вычислительной техники также минимальна, так как уровень психической нагрузки по этому роду деятельности предусматривает энергозатраты 2000...2400 ккал в сутки.

Однако сотрудник при работе с вычислительной техникой подвергается воздействию комплекса неблагоприятных факторов, обусловленных характером производственного процесса условий труда:

- повышенная интенсивность работы и ее монотонность;
- специфический характер зрительной работы;
- тепловыделение от оборудования;
- воздействие шума;
- воздействие ионизирующих и неионизирующих излучений, вредных;
- неудовлетворительные условия световой среды в помещении и освещения на рабочем месте.

4.1 Определение категории тяжести труда через интегральную бальную оценку

Условия труда – это совокупность факторов внешней производственной среды, влияющих на здоровье и работоспособность человека во время выполнения работы. Эти факторы делятся на 4 группы.

Санитарно-гигиенические факторы характеризуют производственную среду рабочей зоны (влажность, температура воздуха, освещенность, наличие шума и вибраций, электромагнитных излучений). Воздействие применяемого оборудования и технологических процессов определяет наличие этих факторов в процессе труда. Все показатели санитарно-гигиенических факторов нормированы и оцениваются количественно.

Психофизиологические факторы (тяжесть труда) обусловлены самим процессом труда. Они характеризуются физической нагрузкой, нервным напряжением, темпом работы и ее монотонностью.

Эстетические факторы (элементы) характеризуются цветовым оформлением рабочих мест и помещений, эстетизацией трудового процесса, продуктом труда, окружающей средой рабочей среды и определяющим восприятие рабочей среды и ее элементов трудящимися.

Социально-психологические факторы характеризуются сплоченностью команды, межгрупповыми отношениями в коллективе. Эти факторы определяют психологический климат в рабочей силе.

Условия труда оказывают большое влияние на здоровье персонала и его работоспособность.

Чтобы избежать негативного воздействия вредных производственных факторов, снизить производительность труда, предотвратить возникновение профессиональных заболеваний, необходимо планировать и осуществлять мероприятия по улучшению условий труда. Для этого необходимо проанализировать условия труда и определить уровень выполняемой работы.

Для оценки влияния вредных факторов на здоровье и производительность труда можно нивелировать используемые категории работ, что учитывает суммарный эффект всех факторов производственной среды.

4.2 Разделение работ по тяжести и напряженности

Из-за влияния вредных факторов производства в трудовом процессе можно сформировать три функциональных состояний организма: нормальное, пограничное (между нормой и патологией) и патологическое.

Согласно существующей классификации, условия труда можно разделить на 6 категорий тяжести работы.

Первая категория тяжести должна включать те виды работ, которые могут быть выполнены в оптимальных условиях внешней производственной среды и при оптимальной физической, умственной и нейро-эмоциональной нагрузке. В этом случае рабочая нагрузка будет соответствовать физиологическим возможностям человеческого тела и его способностям.

Вторая категория тяжести включает те работы, в результате которых уровни вредных и опасных производственных факторов не превышают оптимальных или максимально допустимых значений. В то же время работоспособность не ухудшается, нет никаких отклонений в состоянии здоровья, которые могут быть связаны с профессиональной деятельностью. Возможные функциональные изменения исчезают во время отдыха.

Третью категорию тяжести следует отнести к работе, выполняемой в условиях, когда практически здоровые люди испытывают реакции, характерные для пограничного состояния организма. Наблюдается небольшое снижение показателей труда (производительность труда). Использование рациональных режимов работы и отдыха может быстро устранить эти негативные последствия.

Четвертая категория тяжести включает в себя работу, в результате которой организм может сформировать достаточно глубокое пограничное

состояние даже у практически здоровых людей. Большинство физиологических показателей ухудшаются (реакции замедляются), особенно в конце смены или рабочей недели. Могут появиться характерные состояния, обусловленные производством.

Пятая категория тяжести включает работу, которая в конце смены и / или рабочей недели формирует реакции, характерные для патологического состояния организма у практически здоровых людей и которые, как правило, исчезают у большинства рабочих после полного отдыха. Но у некоторых людей изменения могут привести к производственным и профессиональным заболеваниям.

Шестая категория тяжести включает работу, в результате которой четко проявляются признаки патологического состояния в организме человека. Эти работы выполняются в особо опасных (критических) условиях работы. В то же время патологические реакции могут развиваться достаточно быстро, могут быть необратимыми и часто сопровождаются серьезным нарушением функций жизненно важных организмов и систем.

4.3 Параметры микроклимата

Характеристики микроклимата имеют все шансы меняться в широких пределах, в то время как важным обстоятельством жизнедеятельности человека считается поддержание постоянства температуры тела вследствие терморегуляции, т.е. возможности организма корректировать ответную реакцию тепла в окружающую среду. Принцип нормирования микроклимата – создание оптимальных обстоятельств с целью теплообмена тела человека с окружающей средой.

Вычислительная оборудование считается основой значительных тепловыделений, что способен послужить причиной к увеличению температуры и уменьшению относительной влаги в помещении. В комнатах, где определены ПК, обязаны соблюдаться конкретные характеристики микроклимата. В санитарных нормах СН-245-71 определены величины характеристик микроклимата, формирующие удобные условия. Эти нормы устанавливаются в связи с периода года, характера трудового процесса и характера производственного помещения. Представлены в таблице 4.1.

Объем комнат, в каковых расположены сотрудники вычислительных центров, не должен быть меньше 19,5м3/человека с учетом максимального числа одновременно работающих в смену. Общепризнанных мерок подачи свежего воздуха в помещения, где находятся ПК [1], приведены в таблице 4.2.

Таблица 4.1 - Параметры микроклимата для помещений

Период года	Параметр микроклимата	Величина
Холодный	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	22…24°С 40…60% до 0,1м/с
Теплый	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	23…25°С 40…60% 0,1…0,2м/с

Таблица 4.2 - Нормы подачи свежего воздуха в помещения [1]

Характеристика помещения	Объемный расход подаваемого в помещение свежего воздуха, $м^3$ /на одного человека в час
Объем до 20$м^3$ на человека 20…40$м^3$ на человека Более 40$м^3$ на человека	Не менее 30 Не менее 20 Естественная вентиляция

С целью предоставления удобных условий применяются как организационные методы (здравая предприятие выполнения работ в зависимости от времени и дней, смена работы и отдыха), таким образом и технические средства (вентиляция, кондиционирование воздуха, отопительная система).

4.4 Количественный анализ тяжести и напряженности труда

Условия работы оказывают прямое влияние на состояние тела, которое характеризуется определенными реакциями. Чтобы оценить негативное воздействие на людей внешних условий, необходимо определить категорию тяжести работы.

При проведении количественного анализа тяжести труда должны учитываться санитарно-гигиенические и психофизиологические факторы производственной среды, характеризующие условия труда.

К санитарно-гигиеническим факторам производственной среды в соответствии с ГОСТ следует отнести [2]:

- микроклимат в рабочей зоне;
- наличие и концентрацию вредных веществ различных классов опасности;
- наличие и концентрацию производственной пыли;
- вибро-акустические факторы и ультразвук;
- интенсивность теплового излучения;
- электромагнитные излучения различных диапазонов частот;
- ионизирующие излучения (рентгеновское, гамма-, α-β-излучения);

- биологические факторы.

К психофизиологическим факторам соответствии с ГОСТ следует отнести:

- физическую, динамическую и статическую нагрузки;
- рабочую позу и перемещения в пространстве;
- сменность, продолжительность непрерывной работы в течение суток;
- разряд зрительных работ;
- число важных объектов наблюдения;
- темп работы, монотонность работы;
- объем получаемой и перерабатываемой информации;
- режим труда и отдыха;
- нервно-эмоциональная нагрузка;
- интеллектуальная нагрузка.

В ходе проведения анализа учитываются факторы рабочей среды, которые характерны для конкретного рабочего места и профессии. Как правило условия труда определяются совокупностью факторов рабочей среды, поэтому каждому показателю или фактору среды необходимо выставить оценку в баллах от 1 до 6 в зависимости от их численного значения.

Категория тяжести и напряженности труда непосредственно связана с интегральной бальной оценкой [3], которую можно определить по формуле (4.1):

$$U_r = \left[X_{max} + \frac{\sum_{i=1}^{n} X_i}{n-1} \times \frac{6 - X_{max}}{6}\right] \times 10, \quad (4.1)$$

где X_{max} - самая большая из полученных частных балльных оценок;

X_i - балльная оценка по i-му из учитываемых факторов;

n - общее число факторов без учета одного фактора X_{max};

N - общее количество факторов.

Зависимость категории тяжести от интегральной балльной оценки приведена в таблице 4.3. [3]

Таблица 4.3 - Категории тяжести труда

Категория тяжести труда	1	2	3	4	5	6
Интегральная оценка элементов условий труда, U_T, баллы	до 18	18,1- 33	33,1- 45	45,1- 53	53,1- 59	59,1- 60

Если вредный фактор оказывает воздействие не в течение всей рабочей смены, то оценка факторов и показателей условий труда должна быть определена в зависимости от времени их воздействия [4] на работника по формуле (4.2):

$$X_{iфакт} = X_i \frac{t}{t_{см}}, \quad (4.2)$$

где X_i - оценка i-го элемента условий труда в баллах;

t- фактическая длительность действия фактора, мин.;

$t_{см}$- продолжительность смены, мин.

Повышение тяжести труда будет влиять на работоспособность человека. Снижение работоспособности непосредственно связано с состоянием утомления, которое количественно можно оценить при помощи показателя утомления, выраженного в условных единицах. Зависимость между интегральным показателем тяжести труда и степенью утомлением [4] можно выразить уравнением (4.3):

$$У = \frac{U_T - 15,6}{0,64}, \quad (4.3)$$

где У - показатель утомления в условных единицах;

U_T - интегральный показатель категории тяжести труда в баллах.

Если знать степень утомления, то можно определить уровень работоспособности по формуле (4.4):

$$R = 100 – У, \quad (4.4)$$

где R - уровень работоспособности в относительных единицах.

По значениям работоспособности, которые определили до и после проведения мероприятий по улучшению условий труда, теперь можно рассчитать изменение производительности труда (прирост производительности) по формуле (4.5):

$$П_{пт} = \left[\frac{R_2}{R_1} - 1\right] \times 100 \times 0.2, \quad (4.5)$$

где $П_{пт}$ - прирост производительности труда;

R_2 и R_1 - работоспособность в условных единицах до и после проведения мероприятий по улучшению и оздоровлению условий труда;

0,2 - поправочный коэффициент, который отражает зависимость между увеличением работоспособности и ростом производительности труда.

Тяжесть и напряженность труда оказывает влияние на рост производственного травматизма. Так как интегральная балльная оценка дает возможность определить категорию тяжести труда, то величину производственного травматизма [5] можно рассчитать по формуле (4.6):

$$К = \frac{1}{1,3 - 0,0185 \cdot U_T}, \quad (4.6)$$

где К - рост производственного травматизма, количество раз;

U_T - интегральный показатель категории тяжести труда в баллах.

На рабочих местах необходимо предусмотреть создание благоприятной производственной среды и формирование условий труда, относящихся к первой категории тяжести труда (оптимальные). Если оборудование имеет малую травмоопасность и большую производительность, то величину травматизма можно принять равной единице, и в данном случае, интегральный показатель тяжести труда [5] будет равен:

$$U_T = (1{,}3 - 1{,}0) / 0{,}0185 = 16{,}2 \qquad (4.7)$$

что характеризует наилучшую травмобезопасность данного рабочего места.

4.5 Расчет допустимого уровня шума в офисе

Шум на рабочем месте оказывает раздражающее влияние на работника, повышает его утомляемость, а при выполнении задач, требующих внимания и сосредоточенности, способен привести к росту ошибок и увеличению продолжительности выполнения задания. Длительное воздействие шума влечет тугоухость работника вплоть до его полной глухоты.

Внезапные шумы высокой интенсивности, даже кратковременные (взрывы, удары и т.п.), могут вызвать как острые нейросенсорные эффекты (головокружение, звон в ушах, снижение слуха), так и физические повреждения (разрыв барабанной перепонки с кровотечением, поражения среднего уха и улитки).

Кроме общих требований, существуют критерии, применимые к конкретным видам работ, в зависимости от их содержания. Для офисных рабочих также рассчитаны свои показатели:

- для физической работы, требующей точности и аккуратности, воздействие не должно превышать 80 дБ;
- для творческих натур, руководящих должностей и персонала — не выше 50 дб;
- умственная деятельность, требующая слухового контроля и постоянной концентрации, не выше 65 дБ;
- создание новых программ, преподавательская деятельность — не свыше 40 дБ;
- деятельность, связанная сведением переговоров посредством телекоммуникации — не выше 55 дБ.

Основной характеристикой звукового поля [8] является уровень его звукового давления L_p, определяемый по формуле (4.8):

$$Lp = 20\lg\frac{p}{p_0}db, \qquad (4.8)$$

где p – эффективное звуковое давление дин/см^2;

p_0 – 2 10-4 дин/см^2 (звуковое давление, принятое за нулевой уровень).

Уровень звукового давления, создаваемого отдельным вентилятором Ni обычно задается в характеристиках вентилятора. Параметр обозначается там как “Noise”.

Для этого значения по формуле (4.9) можно вычислить эффективное звуковое давление pi. Здесь Ni и pi параметры i-го источника шума, а i=1, 2, … n.

$$p_i = 10(\frac{N_i}{20})\, p_0, \qquad (4.9)$$

где $p_0 = 2*10^{-4}$ дин/м^2.

Звуковое давление нескольких источников N суммируется по формуле (3). Поскольку в системном блоке все вентиляторы – источники шума расположены на расстоянии много меньшем контрольного расстояния для замера уровня шума (1м) можно считать, что формула (4.10) выполняется с достаточной точностью.

$$Lp = 20\lg\frac{p_1+p_2+p_3}{p_0}db, \qquad (4.10)$$

где p_1, p_2, p_3 – эффективное звуковое давление, его можно получить из (4.8) для каждого значения L_{p1}, L_{p2}, L_{p3};

N – суммарный уровень звукового давления.

Рассчитаем сколько шума производят несколько компьютеров в одном помещении.

Допустим в отделе разработки 4 компьютера. Каждый из них находится в 50см друг от друга. Вентиляторы с уровнем шума 53дб, 46дб, 36дб, 19дб.

Вычисляем эффективное звуковое давление каждого по формуле (4.9).

$p_1 = 10(\frac{53}{20})*2*10^{-4} = 0.0053$ дин/м^2.

$p_2 = 10(\frac{46}{20})*2*10^{-4} = 0.0046$ дин/м^2.

$p_3 = 10(\frac{36}{20})*2*10^{-4} = 0.0036$ дин/м^2.

$p_4 = 10(\frac{19}{20})*2*10^{-4} = 0.0019$ дин/м^2.

$p_{1+}\ p_{2+}\ p_{3+}\ p_4 = 0.0053+0.0046+0.0036+0.0019 = 0.0154$ дин/м^2.

По формуле (4.10) вычисляем результирующий уровень шума для этих вентиляторов.

$Lp = 20lg\ \frac{0.0154}{2*10^{-4}} = 37.7$дб.

Теперь рассчитаем уровень звука в 9-часовой рабочий день.

Эквивалентный уровень звука за 9-часовой рабочий день L_{ex9h}, ДБ: Величина, используемая в целях нормирования и оценки шума на рабочем месте [8] и определяемая по формуле (4.11):

$$L_{ex9h} = L_p + 10[\frac{T_e}{T_0}], \quad (4.11)$$

где Lp - 37.7, дБ;

T_e - эффективная длительность номинального рабочего дня (т.е. интервал времени, в течение которого наблюдается воздействие шума, существенного и представительного для данного рабочего места), час; убрав обеденный перерыв и периодические выходы их помещения получится примерно 6 часов;

T_0 - базовая длительность рабочего дня, равная 9 часов.

$L_{ex9h} = 37.7 + 10\ [\frac{6}{9}] = 44.4$ дб.

4.6 Определение расчета кратности воздухообмена

Кратность воздухообмена — санитарный показатель состояния воздушной массы в помещении. От этого параметра зависит безопасность и комфорт людей. Допустимые значения регулирует государство — в строительных нормах и правилах (СНиП), сводах правил (СП), санитарных правилах и нормах (СанПиН) и ГОСТах. Кратность воздушного обмена показывает, сколько раз в течение часа воздух заменялся на новый.

Есть 2 типа воздухообмена: естественный и искусственный. Естественный способ обмена заключается в движении воздушных масс за счет разницы давления. Из точек с большим давлением — в места с меньшим. Искусственный воздухообмен подразумевает работу вентиляторов, кондиционеров и других электрических устройств.

Формула кратности воздухообмена [7] выглядит так:

$$N = Q\ /\ V, \quad (4.12)$$

где: N — кратность (раз в час);

Q - нужное количество свежего воздуха в час, м³/ч;

V - объем помещения, м³; если у комнаты сложная форма, объем нужно определять вместе со специалистами.

Естественное замещение воздуха ограничивается 3-4-кратным показателем, поэтому его движение иногда приходится усиливать механической вентиляцией.

Вентиляционные системы работают по 2 схемам: вытесняют старый воздух новым или перемешивают обе эти массы.

Для систем, работающих только на удаление воздуха, основная формула кратности [7] выглядит следующим образом:

$$N = V\ у.\ в. / V\ пом, \quad (4.13)$$

где V у. в. — объем удаляемого воздуха, м³/ч;

V пом — объем помещения, м³.

В удаляемый объем следует включать тепловые выделения и летучие вредные вещества.

Для приточной и вытяжной вентиляции рассчитывают также отдельные показатели кратности.

К примеру, для приточной системы [7] его определяют так:

$$N\ пр = L\ пр / V\ пом, \quad (4.14)$$

где L пр — производительность приточной системы, м³/ч;

V пом — объем помещения, м³.

На одного сотрудника следует отводить 60 м³/ч, а на временного посетителя — 20 м³/ч. Удельная кратность выступает как информативный показатель при условии, что размеры помещения приближаются к стандартным.

В офисах и административных учреждениях требуется больше свежего воздуха, чем в индивидуальном жилье. Причина этому — большое количество офисной техники, напряженная умственная деятельность и стандарты обслуживания клиентов.

Новый воздух должен эффективно удалять испарения. Стоит уделить внимание увлажнению и очистке воздуха, его охлаждению или прогреву перед подачей в помещения.

В рабочей комнате на 1 сотрудника нужно не меньше 20 м³/ч. В конференц-залах столько же отводят на каждого посетителя. Интенсивный воздухообмен следует обеспечивать в умывальных и санитарных комнатах — до 15 обновлений воздуха в час.

Возьмем для примера помещение высотой 3,5 м и площадью 60 м², где работает 15 человек. Считаем, что воздух загрязняется только от роста концентрации углекислого газа из-за дыхания.

Сначала находим объем помещения: V = 3,5 м × 60 м² = 210 м³.

Учитываем, что 1 среднестатистический человек выделяет 22,6 л углекислого газа в час [8].

Получаем, что вредные выделения можно рассчитать формулой

B = 22,6 × n, где n соответствует количеству людей в помещении.

B = 22,6 л/ч × 15 = 339 л/ч

Для помещений максимально допустимая концентрация углекислого газа равняется 1/1000, или же 0,1 %. Переведем это в 1 л/м³. В чистом воздухе углекислого газа есть около 0,035 %. Переводим в 0,35 л/м³.

Рассчитаем по формуле 10.6, сколько свежего воздуха понадобится для всех 15 человек:

Q = 339 л/ч: 1 л/м³ – 0,35 л/м³ = 339 л/ч : 0,65 л/м³ = 521,5 м³/ч. Кубические метры в данном случае перешли в числитель, а часы — напротив, в знаменатель.

Определяем кратность воздухообмена (формула 4.13):

N = 521,5 м³/ч : 210 м³ = 2,48 раз в час. Выходит, при сменяемости воздуха на уровне 2,48 раз в час концентрация углекислого газа останется в пределах нормы.

Найдем теперь удельную кратность воздухозамещения на 1 человека и на 1 м². Объем помещения при этом должен быть не меньше 210 м³, а высота потолка — от 3,5 м.

521,5 м³/ч : 15 чел. = 34,7 м³/ч на 1 человека

521,5 м³/ч : 60 м² = 8,7 м³/ч на 1 м² площади

Таким образом, в помещении удельная кратность воздухозамещения на 1 человека 34,7 м³/ч, при том, что в рабочей комнате на 1 сотрудника необходимо не меньше 20 м³/ч.

4.7 Вывод по главе

В данной главе анализируются оптимальные условия труда для разработки программного обеспечения, а также определяются необходимые меры безопасности.

При анализе тяжести труда на рабочем месте специалиста выполнен расчет интегральной балльной оценки. В результате расчета определяются сроки и условия работы специалиста, относящегося к пятой категории сложности, что негативно скажется на работоспособности и состоянии здоровья. Для этого необходимо было ввести в действие меры по улучшению условий труда: сокращение продолжительности воздействия шума и нервно-эмоциональной нагрузки. После введения мероприятий категория тяжести труда повышается с пятого на второй уровень. Коэффициент производительности был увеличен с 38 в относительных единицах до 77, производительность рабочей силы составил 20,5%.

5 Анализ и оценка рисков

Целью анализа рисков, в данной работе, является оценка угроз и уязвимых зон объектов информации, также определение мер противодействия и препятствия доступа к ним. При оценке рисков учитывались все определяющие факторы, такие как: значимость ресурсов, степень угроз и уязвимостей, эффективность мер и средств имеющихся и планируемых для защиты объекта и другое. Анализ рисков коррелирует с тематикой затронутой в дипломной работе.

В ходе управления особое внимание направлено на выявление событий, что могут различным образом сказаться на предприятии, а также управлении, имеющих связь с этими событиями, рисками. Но также учитывается и контролируется допустимый уровень риска при рациональных гарантиях достижения целей предприятия.

В процессе управления рисками охвачено все предприятие и требует вовлеченности всех сотрудников не зависимо от принадлежности к каой-либо должностной иерархии.

В качестве объекта анализа принимаем здание Научно-исследовательского института по разработке радиоэлектронных комплексов, в частности 3-ех технических лабораторий, расположенных на территории института в непосредственной близости друг от друга, также имеющих статус режимных объектов. Вход на территорию НИИ осуществляется через контрольно-пропускную систему, на территории имеется дежурная смена охраны. Доступ в помещение лабораторий, имеет узкий круг лиц, за исключением нештатных ситуаций, и мероприятий связанных с защитой отчетных документов.

Рассматривается оценка рисков для трех лабораторий на предмет установки закладных устройств негласного съема информации (текстовой, речевой, видео) с беспроводной передачей данных. К мерам по управлению рисками относятся: пропускной контроль, и контроль за перемещением по территории; обеспечение сохранности и безопасности устройств и документации, находящихся на территории объектов; контроль сотрудников НИИ; контроль территории на наличие несанкционированных устройств. Необходимо определить объект защиты по средствам определения информационных активов, оценивается их уровень критичности для предприятия. Затем необходимо определить источники, от которых осуществляется защита. Для этого проводится анализ уязвимых зон объектов, степень критичности – вероятности того, что они могут провалиться.

Активы, рассмотренные в данной работе:

- схемы и чертежи разрабатываемых комплексов;
- испытательные макеты;
- математические и виртуальные модели разрабатываемых устройств;
- конфиденциальная информация о сотрудниках НИИ;

- информация о паролях-доступа в системы сбора и передачи данных.

Для анализа рисков был выбран алгоритм из стандарта ISO-27005. Расчет по первому алгоритму (по двум шкалам) производится на основе приложения Е стандарта ISO-27005 и представлен в таблице 1.5.

Таблица 5.1 - Ценность активов, уровни угроз и уязвимостей

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Простой общий рейтинг рисков:

- низкий риск: 0-2;
- средний риск: 3-5;
- высокий риск: 6-8.

Остаточный риск – это риск, который остается после мер по контролю над рисками. Расчет остаточного риска осуществляется по формуле, представленной на рисунке 5.1.

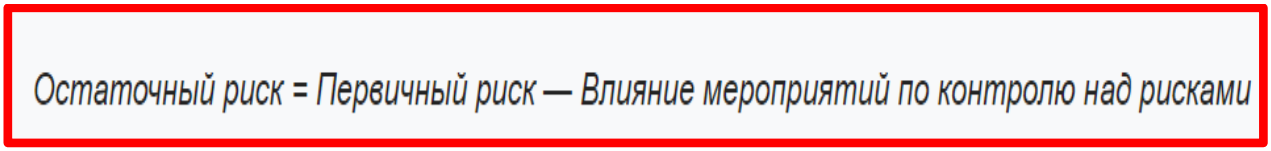

Рисунок 5.1 – Формула расчета остаточного риска

Табличная форма анализа рисков информационной безопасности представлена в таблице 5.2.

Таблица 5.2 – Анализ рисков информационной безопасности

Угрозы	**Уязвимости**	**Максимальн**	**Меры по обработке риска**	**Остаточный**	**Комментарии, ресурсы, ответственный**
Актив 1. Техническая документация и испытательные модели					
1 Установка аудио-визуальных закладных устройств в лабораторий (АВЗУ)	Допуск в помещения посторонних лиц. Обилие различных электронных устройств под которые могут быть замаскированы закладные устройства; Редкие проведение мероприятий для поиска ЗУ	6	Выстроить СКУД на территории НИИ; Систематизация и упорядочивание расположение электронных устройств; Проведение мероприятий по радио-мониторингу на наличие закладных устройств по разработанным алгоритмам	2	Старший специалист СБ
2 Съем информации через текстовые закладные устройства (ТЗУ)	Обслуживание ЭВМ подрядной организацией. Редкие проведение мероприятий для поиска ЗУ.	6	Организовать отдел по ремонту и обслуживанию ЭВМ; Регулярная проверка электронных устройств визуальным осмотром и нелинейными локаторами;	2	Старший специалист СБ

3 Диверсия по похищению технической документации и и испытательных моделей	Уязвимость перед закладными устройствами; Отсутствие тревожной сигнализации при взломе и проникновении ; Отсутствие дополнительных средств защиты (сейфы; специальные, охраняемые помещения).	8	Разработать автоматизированную систему по обнаружению закладных устройств на основе имеющихся алгоритмов. Установка охранной сигнализации; Усиление охранных мер при наличии важной, секретной документации и оборудования;	3	Старший специалист СБ
Актив 2. Конфиденциальная информация о сотрудниках НИИ					
4 Установка через вибро-акустических закладных устройств (ВАЗУ)	Устаревшие системы отопления и канализации; Мертвые зоны по территории у камер видеонаблюдения ; Редкое проведение мероприятий для поиска ЗУ.	7	Замена отопительных и канализационных магистралей поглощающих вибро-акустические колебания; Реконструкция имеющейся системы видеонаблюдения; Применение видеоскопов для поиска закладных устройств в трудно доступных местах;	2	Старший специалист СБ

Продолжение таблицы 5.2

5 Установка аудиовизуальных-закладок в административные помещения (АВЗ)	Допуск в помещения посторонних лиц; Редкое проведение мероприятий для поиска ЗУ;	7	Применение металодетекторов, периодический визуальный осмотр помещений, Блокирование радиоэлектронных устройств во время экстренных и важных совещаний; Применение радио-мониторинга.	2	Старший специалист СБ
Актив 3. Системы Базы данных					
6 Установка видео закладных устройств (ВЗУ)	Слабые защиты допуска в СУБД; Редкая смена паролей; Отсутствие СКУД в соседних зданиях; Редкие проведение мероприятий для поиска ЗУ	7	Усовершенствование защит допуска в СУБД; Оснащение СКУД всех зданий; Организовать смену пароля каждые три месяца, на программном уровне; Разработать автоматизированную систему по обнаружению закладных устройств на основе имеющихся алгоритмов.	2	Старший специалист СБ

7 Установка закладных устройств взлома и управления (ЗУВУ)	Редкие проведение мероприятий для поиска ЗУ; Слабые система противодействия взлому; Применение сомнительных устройств телекоммуникации.	7	Покупка устройств телекоммуникаций у официальных представителей; Организовать рабочую группу по противодействию от взлома СУБД; Постоянные мероприятия по идентификации закладных устройств.	2	Старший специалист СБ

Первичная оценка риской дала неприемлемые результаты (6-8 по шкале из 8 баллов), следовательно, для всех рисков были предусмотрены защитные меры. Затем, после внедрения защитных мер, риски были пересчитаны и получены остаточные риски, что дали благоприятные результаты (0-3 по 8-ми бальной шкале).

Связь компонентов по проведенному анализу рисков были выполнены в программном продукте CORAS.

На рисунке 5.2 представлены защищаемые активы в виде диаграммы взаимосвязей. Активы были разделены на три категории: «Оборудование и аппаратура», «информационные ресурсы», «Программные ресурсы».

Диаграмма модели угроз отображена на рисунке 5.3. Читать схему необходимо слева на право, где указаны: источники угроз, уязвимости, этапы реализации угроз, последствия реализации угроз (инциденты), понесшие от реализации угрозы ущерб активы.

На рисунке 5.3 представлена диаграмма модели угроз. Элементы диаграммы слева направо: источники угроз, уязвимости, этапы реализации угроз, последствия реализации угроз (инциденты), понесшие от реализации угрозы ущерб активы. Например, из-за обслуживания ЭВМ в подрядных организациях устанавливают текстовое закладное устройство, что приводит к получению доступа к оборудованию, происходит утечка информации, и в итоге оказывает негативное влияние на актив-1 (Техническая документация и испытательные модели). Источник угрозы злоумышленник.

Диаграмму модели угроз с учетом вероятности возникновения, читается также, как диаграмму, изображенную на рисунке 5.3, но с учетом вероятности возникновения (низкая, средняя, высокая), и представлена на рисунке 5.4.

На рисунке 5.5 представлена диаграмма рисков с характеристиками влияния угроз. Элементы диаграммы слева направо: источники угроз, уязвимости, способы реализации угроз, степень влияния реализации угроз,

понесшие от реализации угрозы ущерб активы. Например, злоумышленник по причине полученных данных о уязвимости сигнализации проникает в лабораторию, тем самым нанося ущерб активу-1.

На рисунке 5.6 представлена диаграмма модели угроз с учетом защитных мер. Ее следует читать так же, как и диаграмму, представленную на рисунке 5.3, с единственным отличием: между уязвимостями и способами реализации угроз добавлены защитные меры для уменьшения рисков. Например, защитными средствами от уязвимости при проникновении в лабораторию, будет правильно выстроенная система контроля и учета допуска на территорию НИИ.

На рисунке 5.7 представлена диаграмма недопустимых рисков. Она построена на базе диаграммы, представленной на рисунке 5.5, однако на данной диаграмме показаны только те риски, которые имеют высокую степень влияния угроз.

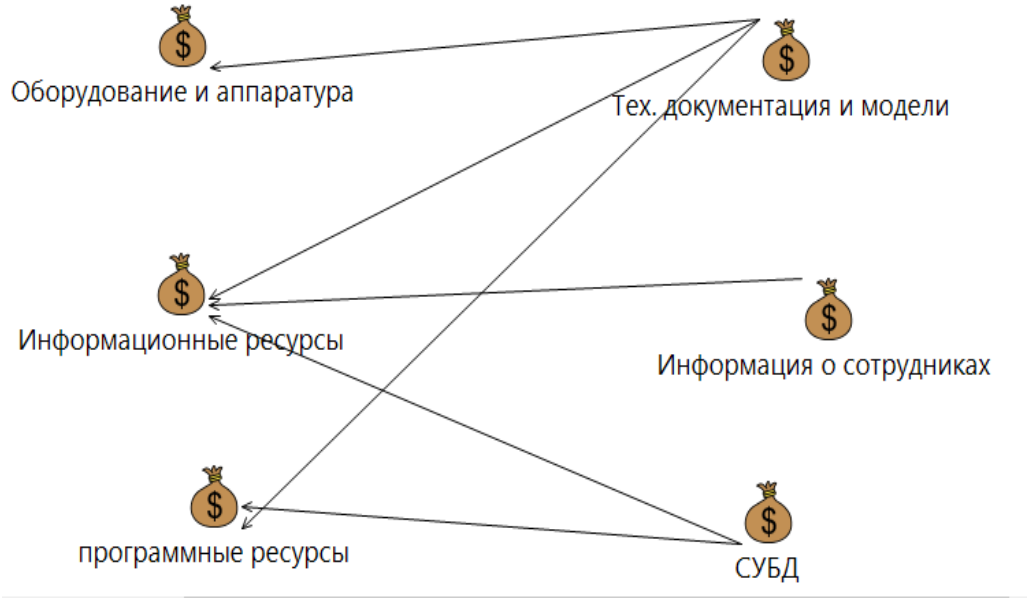

Рисунок 5.2 – Список защищаемых активов

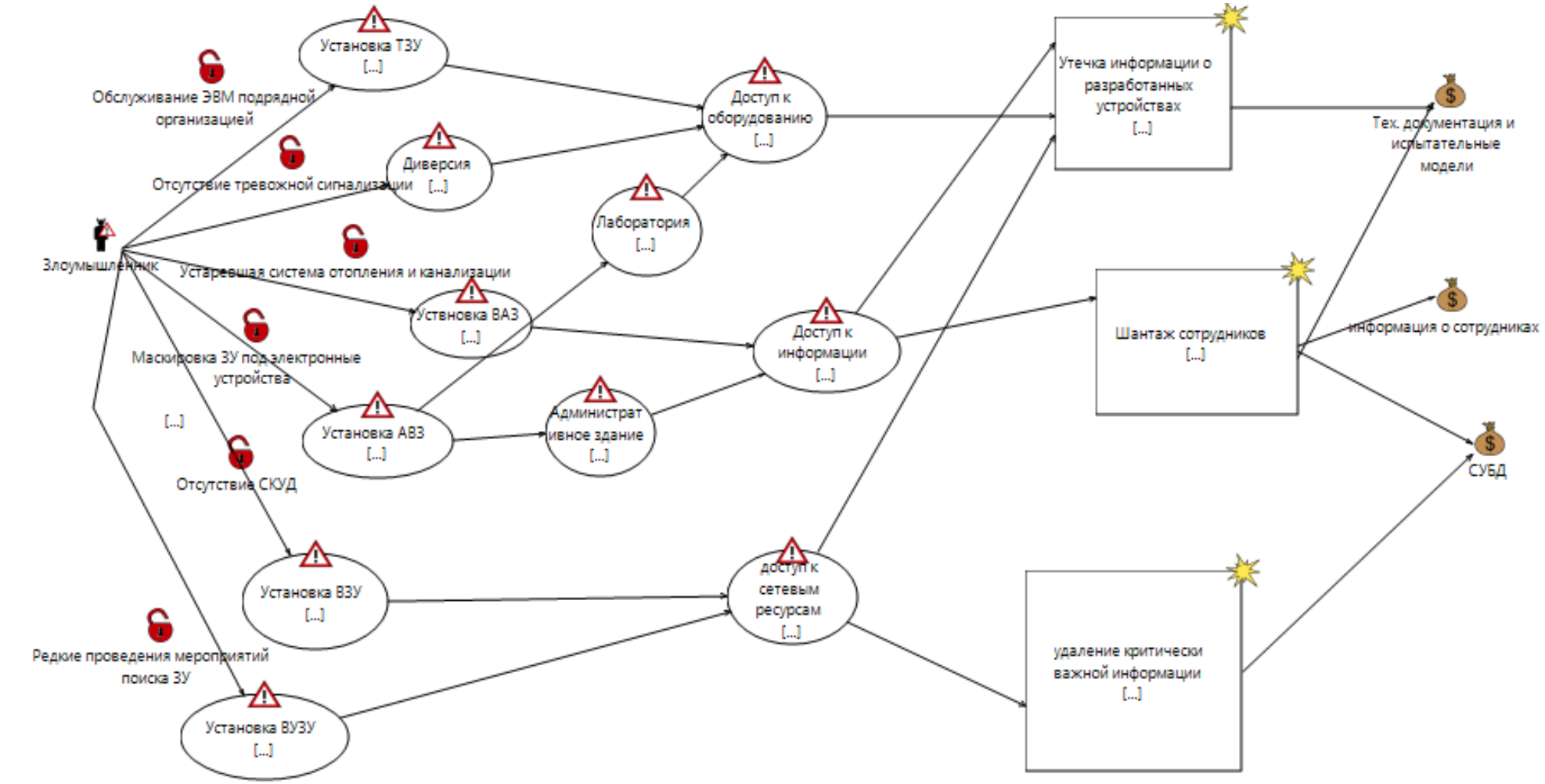

Рисунок 5.3 – Диаграмма модели угроз

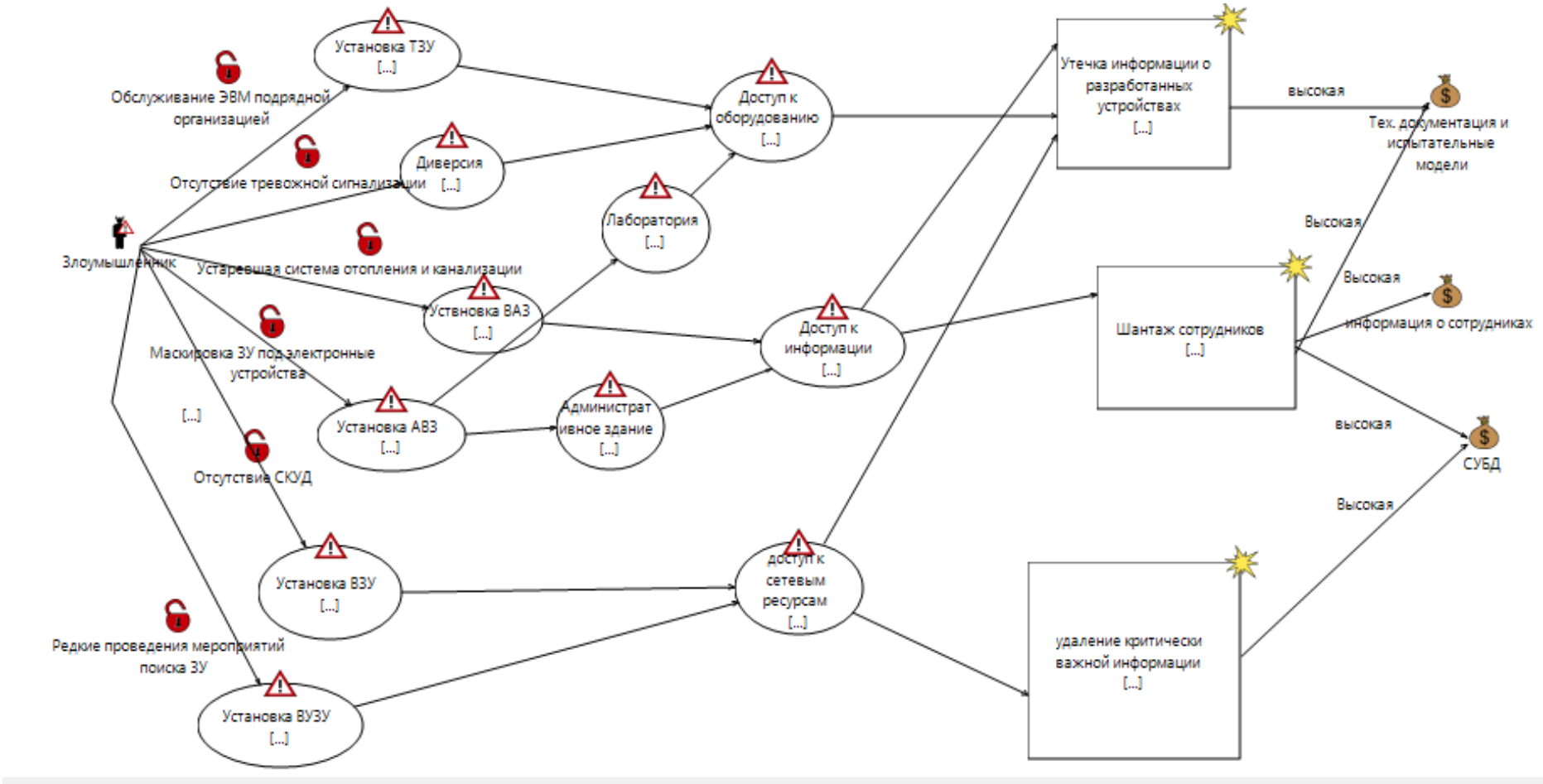

Рисунок 5.4 – Диаграмму модели угроз с учетом вероятности возникновения

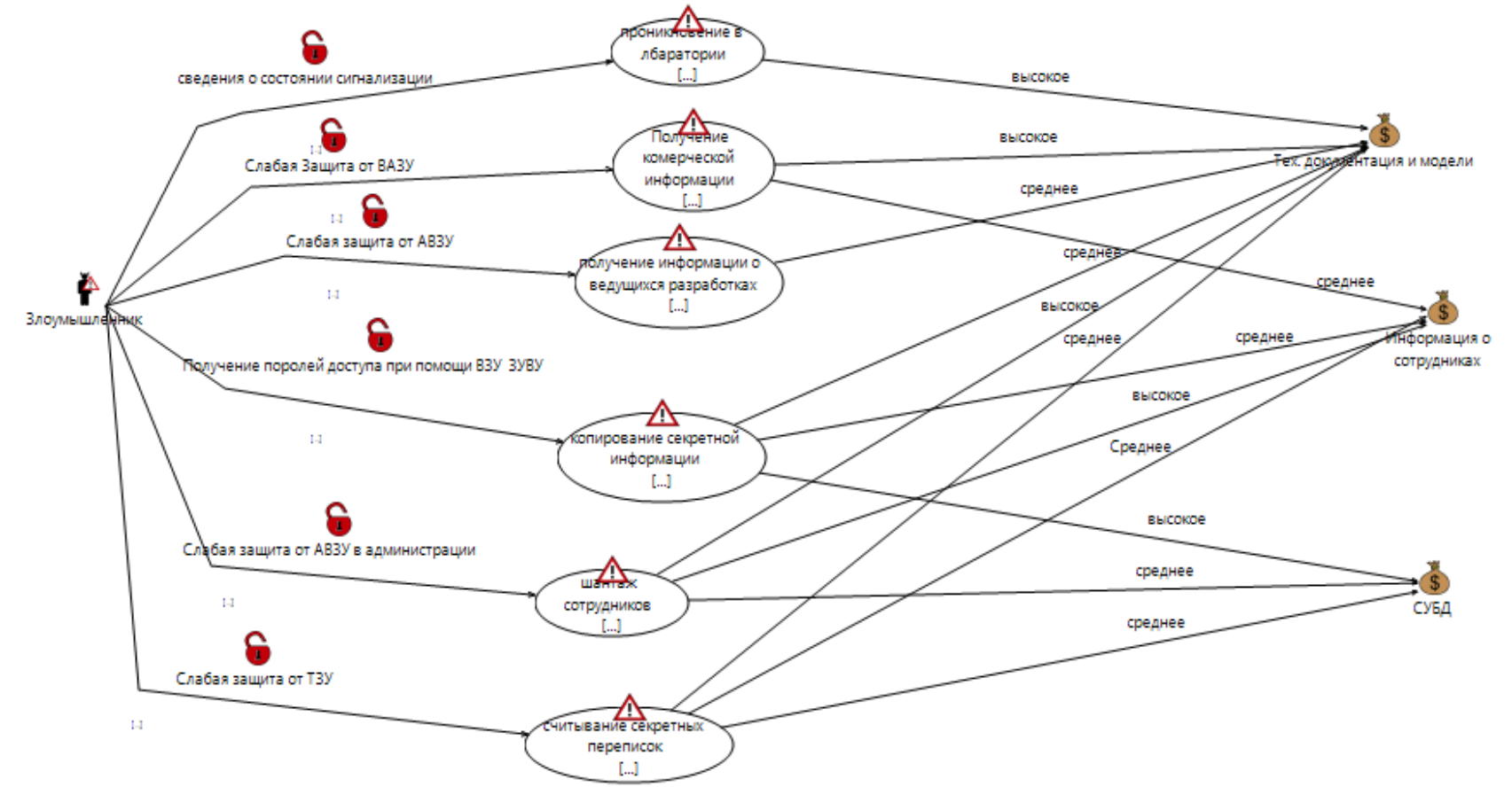

Рисунок 5.5 – Диаграмма рисков с характеристиками влияния угроз

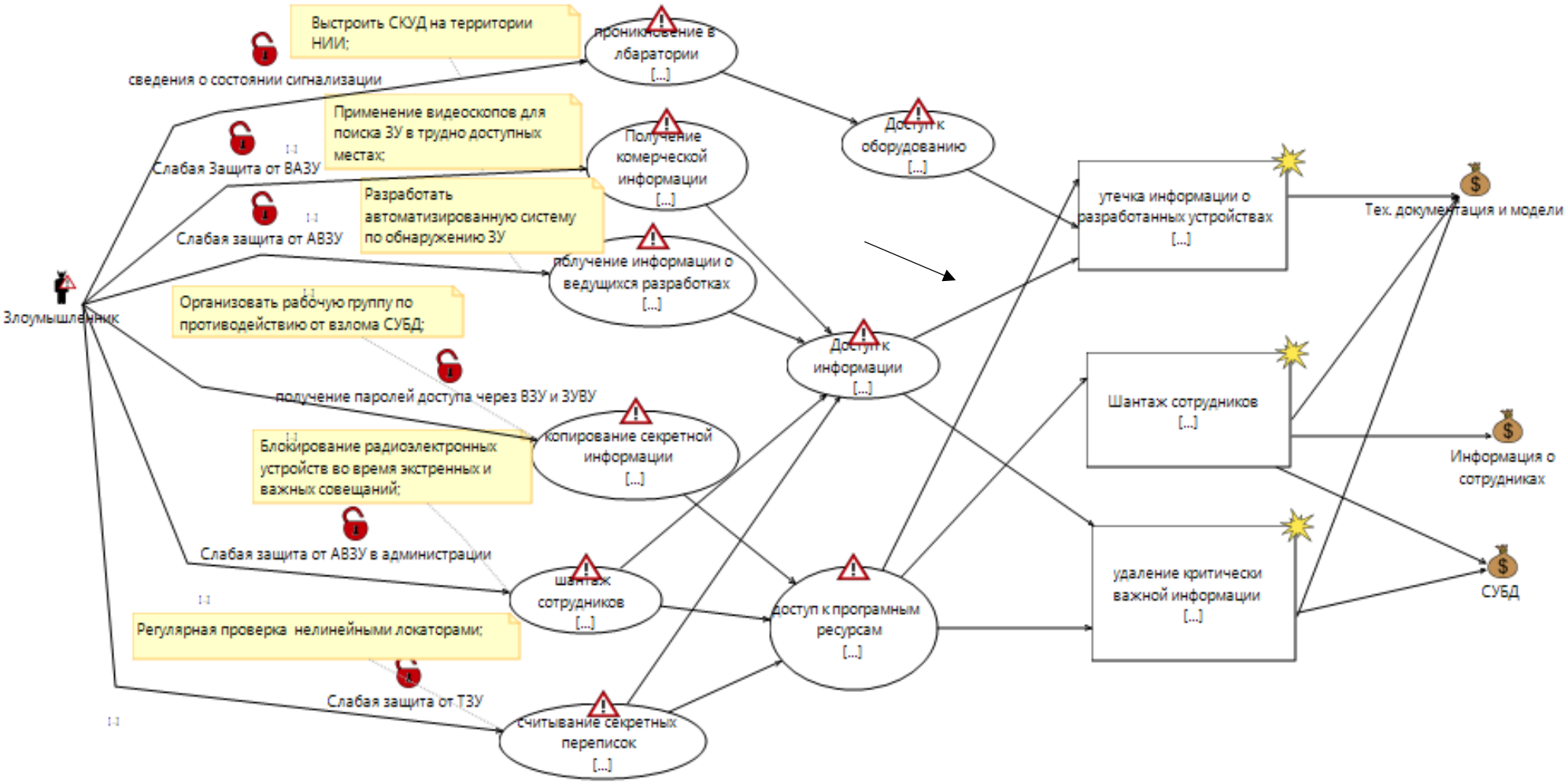

Рисунок 5.6 – Модель угроз с учетом защитных мер

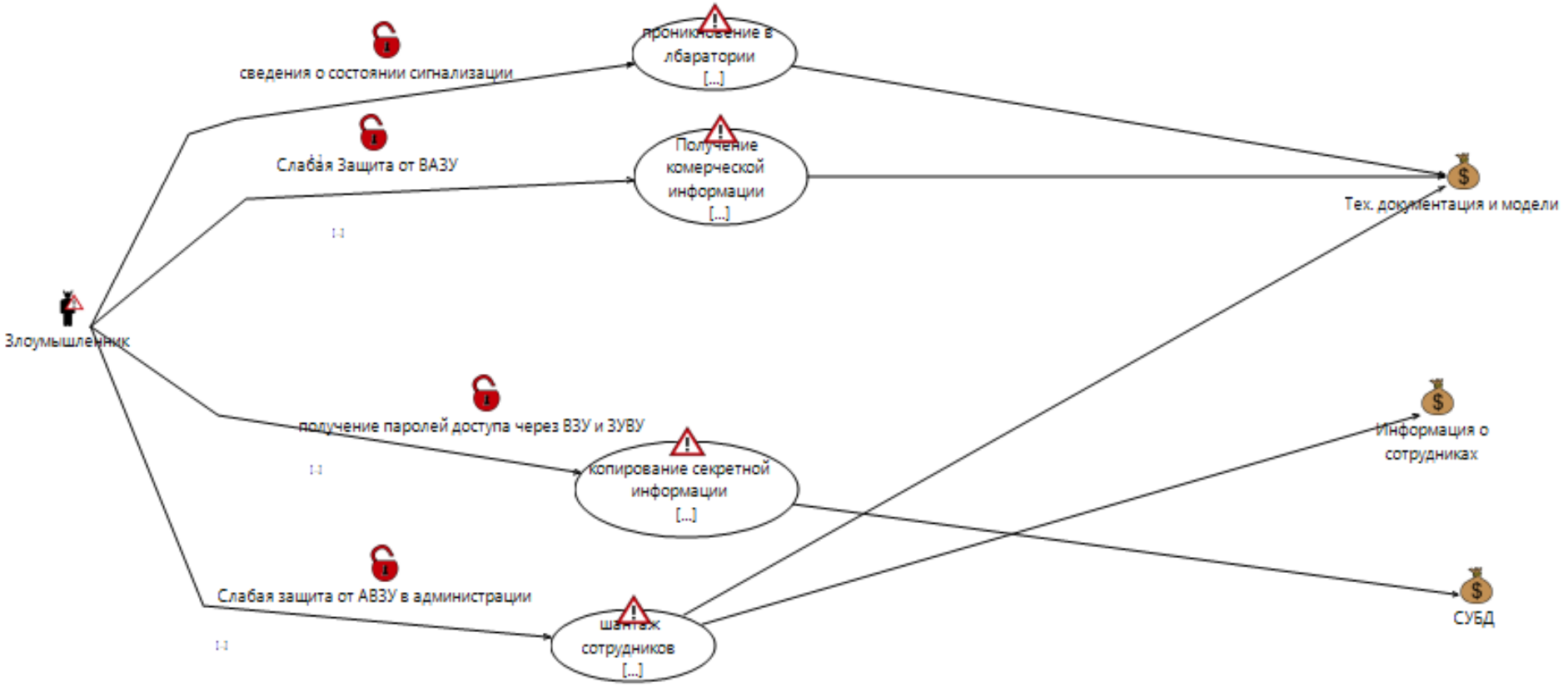

Рисунок 5.7 – Диаграмма недопустимых рисков

5.1 Вывод по главе

В данном разделе были произведены расчёты рисков. Целью данных методик расчёты рисков, понимание реальных угроз и рисков, а также выбора контрмер направленных на минимизацию рисков и защитных мер. Результаты расчетов дают возможность четко понять, что все риски оказались неприемлемыми (6-8 по шкале из 8 баллов). Вслед за тем были рекомендованы к внедрению защитные меры, направленные на снижение рисков, что были рассчитаны раньше. После выявления системы защиты данных необходимых для снижения рисков был совершен перерасчет рисков согласно этому методу. В результате перерасчета рисков с учетом рекомендованных защитных мер произошло их снижение до приемлемого уровня, а собственно уровень риска снизился в 2 раза (0-3 по 8-ми бальной шкале).

Заключение

Таким образом, в данной работе рассматривалась проблема противодействия шпионажу, основанного на получении информации через, так называемые закладные устройства. Были проведены исследования для определения основных характеристик устройств негласного съема информации, с целью разработки методов противодействия. Рассматривались устройства с беспроводной передачей данных, по причине преобладания этих устройств на рынке, их доступности и простоте исполнения.

В первой главе дана классификация закладных устройств негласного съема информации, по различным признакам. Определены принципы работы и реализации данных устройств., каналы передачи данных.

Во второй главе определены основные методы для обнаружения ЗУ. Их классифицировали, как методы обнаружения ЗУ по физическим и электронным признакам объектов. Выявили, что фундаментальное значение в процессах обнаружения ЗУ имеет «радиомониторинг» обстановки. Описали три основных метода, которые применяются в области противодействия техническому шпионажу, по средствам радиомониторинга.

В третьей главе разработаны и описаны два алгоритма для выявления ЗУ. Один из которых полезен в случаях, когда ЗУ использует легальные протоколы передачи данных, другой – для обнаружения устройств с периодическим выходом в эфир с целью передачи, полученной информации. Было произведено физическое моделирование процесса обнаружения ЗУ, результаты которых представлены в 4 экспериментах. Исходя из полученных данных, в результате проведенных экспериментов, можно сделать следующие выводы:

- увеличение параметров скорости сканирования не всегда дает сокращение числа периодов, затраченных до момента обнаружения ЗУ. причиной этому является различие между периодами сканирования рабочего промежутка закладного устройства;
- на значение скорости сканирования оказывают влияние частотный диапазон сканируемого полосы шаг перестройки в ней;
- в 4-ом эксперименте при скорости сканирования 40 каналов/с, произошла синхронизация периодичности сканирование СП и периодичности срабатывания ЗУ, что составило 5 секунд, я по этой причине устройство не было обнаружено;
- значение периодов необходимых для обнаружения закладного устройства и аналитический счёт и примерно совпали, из этого следует, что можно использовать данные выражения и алгоритмы, как фундамент при формировании своих алгоритмов;
- чтобы повысить шансы для обнаружения закладных устройств, излучающих сигнал периодический, необходимо производить сканирование в несколько этапов с небольшой шириной частотного диапазона, а лучше всего использовать несколько сканирующих приемников.

Основываясь на два предложенных алгоритма, появляется возможность разработать автоматизированный комплекс по обнаружению ЗУ с беспроводной передачей данных. Корректируя указанные параметры, можно повысить вероятность обнаружения устройств негласного съема данных.

Данные результаты могут быть полезны не только в отрасли противодействия шпионажу, но и в области пеленгования летательных аппаратов.

Также хотелось бы отметить, что современные методы радиомониторинга требуют прямого участия человека, и полностью автоматизировать процесс поиска на данном этапе не является возможным.

Список литературы

1 Хорев, А.А. Оценка возможностей средств радиоразведки по перехвату информации / А.А. Хорев // Специальная техника. – М.: 2009. – № 2. – С. 54–64.

2 Торокин, А.А. Основы инженерно-технической защиты информации / А.А. Торокин// Ось – М.: 1989. – 365 с.

3 Хорев, А.А. Средства перехвата информации с проводных линий связи/ А.А. Хорев //Защита информации. Инсайд. – С. Петербург: 2011. – № 1 – С. 22 –32.

4 Хорев, А.А. Способы и средства подавления электронных устройств перехвата информации, подключаемых к двухпроводным телефонным линиям / А.А. Хорев // Защита информации. Инсайд. – С. Петербург: 2013. – № 1. – С. 12–19.

5 Железняк, В.К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В.К. Железняк, Ю.К. Макаров, А.А. Хорев // Спецтехника. – 2000. – № 4.

6 Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие / В. К. Железняк // ГУАП. – СПб., 2006. – 188 с.

7 Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие для вузов /П.Б. Хорев // ФОРУМ. – М.: 2015.

8 Зайцев, А.П. Технические средства и методы защиты информации: учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. // Горячая линия-Телеком. – М: 2012.

9 Воробьев, Е.Г. Специалист объекта информатизации по технической защите информации. / Е.Г. Воробьев, С.В. Войцеховский, А.С. Марковский // ООО «Издательский дом «Афина». – СПб.: 2006.

10 Бабурин, А.В. Физические основы защиты информации от технических средств разведки / А.В. Бабурин, Е.А. Чайкина, Е.И. Воробьева // учеб. пособие. гос. техн. ун-т Воронеж. – Воронеж: 2006. – 193 с.

11 Акимов, В.П. Блокировка акустоэлектрических преобразователей в электронных технических средствах и системах общего применения: сборник рекомендаций «Z9» / В.П. Акимов, И.В. Коровин, В.И. Рыбальченко // Гелиос АРВ. – М.: 2010.

12 Хорев, А.А. Оценка возможностей средств акустической (речевой) разведки / А.А. Хорев //Специальная техника. – М.: 2009. – № 4 – С. 49-63.

13 Хорев, А.А. Средства акустической разведки: проводные микрофонные системы и электронные стетоскопы / А.А. Хорев //Специальная техника. – М.: 2010. – № 5 – С. 2–15.

14 Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А Бузов // Горячая линия-Телеком. – М.: 2017. – 636 с.

15 Ефремова О.С. Документация по охране труда в организации. Практическое пособие /О.С. Ефремова 5-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2015 г. – 152 с.

16 ГОСТ IEC 61140-2012. Защита от поражения электрическим током. Общие положения безопасности установок и оборудования / М.: Стандартинформ, 2012 – 30с.

17 Белов С.В. Безопасность жизнедеятельности. – М.: Издательство Высшая школа 1999. – 29 с.

18 СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений / Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.

19 ГОСТ 12.1.038-82. Система стандартов безопасности труда. Электробезопасность. Предельно допустимые значения напряжений и токов / М.: ИПК издательство стандартов, 2001-15с.

20 Ефремова О.С. Документация по охране труда в организации. Практическое пособие /О.С. Ефремова 5-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2015 г. – 152 с.

21 Ефремов О.С. Охрана труда в организации в схемах и таблицах. / О.С. Ефремова 7-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2018 г. – 124 с.

22 СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений / Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.

Приложение А

Сравнительный анализ сканирующих приемников

Таблица А.1 - Сравнительный анализ сканирующих приборов

Тип	Изготовитель	Функциональные возможности	Диапазон частот	Отображаемый средний уровень шума (DANL)	Максимальная полоса анализа	Нестабильность частоты	Погрешность измерения уровня	Интерфейсы для работы с ПК	Мобиль-ность	Анализ сигналов различных стандартов
FSW	Rohde&Schwarz	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; импульсные измерения; измерение параметров антенн; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерение фазового шума; измерения параметров систем беспроводной связи различных стандартов; запись поступающих данных; автоматическое обнаружение активных каналов и декодирование полезной информации; измерение занятости каналов; измерения MIMO.	от 2 Гц до 67 ГГц	- 169 дБ (мВт)	4 ГГц	1×10^{-7} / год (опционально 3×10^{-8} / год)	0,4 дБ	USB, LAN (Ethernet), GPIB	стационарн.	WCDMA/HSPA/HSPA+ 3GPP LTE GSM/EGPRS/EDGE Evolution/VAMOS CDMA2000® 1xEV-DO CDMA2000® 1xRTT TD-SCDMA GSM-R TETRA cdmaOne DECT WLAN IEEE 802.11 a/b/g/j/p/n/ac ZigBee™ IEEE 802.15.4 RFID WRAN IEEE 802.22 WWAN IEEE 802.20
FPS	Rohde&Schwarz	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; импульсные измерения; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерение фазового шума; измерения параметров систем беспроводной связи различных стандартов; запись поступающих данных.	от 10 Гц до 40 ГГц	- 155 дБ (мВт)	160 МГц	1×10^{-6} / год (опционально 1×10^{-7} / год)	0,28 - 1,32 дБ	USB, LAN (Ethernet), GPIB	мобильный	WCDMA/HSPA/HSPA+ 3GPP LTE GSM/EGPRS/EDGE Evolution/VAMOS CDMA2000® 1xEV-DO CDMA2000® 1xRTT TD-SCDMA GSM-R TETRA cdmaOne DECT WLAN IEEE 802.11 a/b/g/j/p/n/ac
FSL	Rohde&Schwarz	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерение фазового шума; измерения параметров систем беспроводной связи различных стандартов.	от 9 кГц до 18 ГГц	- 162 дБ (мВт)	28 МГц	1×10^{-6} / год (опционально 1×10^{-7} / год)	0,5 - 1,2 дБ	USB, LAN (Ethernet), GPIB	мобильный	3GPP HSPA WiMAX™ CDMA2000®/1xEV-DO IEEE 802.11 a/b/g/n IEEE 802.15.1 Bluetooth® RFID MBMS DVB-C

Продолжение таблицы А.1

Тип	Изготовитель	Функциональные возможности	Диапазон частот	Отображаемый средний уровень шума (DANL)	Максимальная полоса анализа	Нестабильность частоты	Погрешность измерения уровня	Интерфейсы для работы с ПК	Мобильность	Анализ сигналов различных стандартов
FSH	Rohde&Schwarz	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; векторный анализ сигналов; анализ помех; ослабление в кабеле; демодуляция и измерение параметров модуляции; измерения параметров систем беспроводной связи различных стандартов.	от 9 кГц до 20 ГГц	- 141 дБ (мВт)	20 МГц	1×10^{-6}	1,0 дБ	USB, LAN (Ethernet)	носимый	GSM/GPRS/EDGE WCDMA/HSDPA/HSPA+ CDMA2000® 1xEV-DO LTE FDD/TDD TD-SCDMA/HSDPA
N9040B UXA	Keysight Technologies	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; импульсные измерения; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерение фазового шума; измерения параметров систем беспроводной связи различных стандартов; запись поступающих данных; измерение занятости каналов.	от 3 Гц до 50 ГГц	- 171 дБ (мВт)	1 ГГц	3×10^{-8} / год	0,19 - 1,28 дБ	USB, LAN (Ethernet), GPIB	стационарн.	1xEV-DO cdma2000®/cdmaOne GSM/EDGE/EVO iDEN/WiDEN/MotoTalk LTE FDD and TDD LTE-Advanced FDD / TDD Multi-standard radio (MSR) TD-SCDMA/HSPA W-CDMA/HSPA+ Bluetooth® Fixed WiMAX™ Mobile WiMAX™ WLAN 802.11a/b/g/n/ac ZigBee CMMB Digital cable TV DTMB (CTTB) DVB-T/H/T2 ISDB-T/TSB/ Tmm
N9962A UXA	Keysight Technologies	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; AM/FM - настройка на сигнал и режим прослушивания; Измерение напряженности поля.	от 9 кГц до 50 ГГц	- 159 дБ (мВт)	20 МГц	4×10^{-7} / год (опционально 1×10^{-8} / год)	0,5 дБ	USB, LAN (Ethernet)	носимый	
N9344C UXA	Keysight Technologies	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; измерение параметров импульсов; AM/FM - демодуляция сигнала; Измерение напряженности поля.	от 9 кГц до 20 ГГц	- 144 дБ (мВт)		1×10^{-6} / год	1,3 дБ	USB, LAN (Ethernet)	носимый	

Продолжение таблицы А.1

Тип	Изготовитель	Функциональные возможности	Диапазон частот	Отображаемый средний уровень шума (DANL)	Максимальная полоса анализа	Нестабильность частоты	Погрешность измерения уровня	Интерфейсы для работы с ПК	Мобиль-ность	Анализ сигналов различных стандартов
NI PXIE-5668R 26.5 GHZ VSA, 320 MHZ BW	National Instruments	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; импульсные измерения; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерение фазового шума; измерения параметров систем беспроводной связи различных стандартов; запись поступающих данных; работа в составе измерительных систем.	от 20 Гц до 26,5 ГГц	- 166 дБ (мВт)	765 МГц	от внешнего источника	0,1 дБ	PXI	зависит от исполнения шасси	EDGE, UMTS/HSPA+, WCDMA, LTE/LTE-Advanced, Bluetooth, 802.11a/b/g/n/p/ac, DVB-C/H/T, and ATSC.
RSA5126B	Tektronix	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; AM/FM - демодуляция сигнала; импульсные измерения; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерение фазового шума; измерения параметров систем беспроводной связи различных стандартов; запись поступающих данных.	от 1 Гц до 26,5 ГГц	- 156 дБ (мВт)	165 МГц	1×10^{-6} / год (опционально $7,5 \times 10^{-8}$ / год)	0,5 - 1,5 дБ	USB, LAN (Ethernet), GPIB	стационарн.	AMPS, NADC, NMT-450, PDC, GSM, CDMA, CDMA-2000, 1xEV-DO WCDMA, TD-SCDMA, LTE, WiMax 802.11a/b/j/g/p/n/ac, Bluetooth DECT, PHS AM, FM, ATSC, DVBT/H, NTSC GMRS/FRS, iDEN, FLEX, P25, PWT, SMR, WiMax
RSA507A	Tektronix	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; векторный анализ сигналов; демодуляция и измерение параметров модуляции; измерения параметров систем беспроводной связи различных стандартов; запись поступающих данных.	от 100 Гц до 7,5 ГГц	- 147 дБ (мВт)	40 МГц	1×10^{-6} / год	0,8 - 2,0 дБ	USB	носимый	AMPS, NADC, NMT-450, PDC, GSM, CDMA, CDMA-2000, 1xEV-DO WCDMA, TD-SCDMA, LTE, WiMax 802.11a/b/j/g/p/n/ac, Bluetooth DECT, PHS AM, FM, ATSC, DVBT/H, NTSC GMRS/FRS, iDEN, FLEX, P25, PWT, SMR, WiMax
MS2840A	Anritsu	Измерение уровня, частоты; измерение мощности сигнала в канале и в соседних каналах; демодуляция и измерение параметров модуляции; измерения параметров систем беспроводной связи различных стандартов; измерение BER; запись поступающих данных.	от 9 кГц до 44,5 ГГц	- 153 дБ (мВт)	125 МГц	1×10^{-7} / год (опционально 1×10^{-9} / год)	0,5 - 3,5 дБ	USB, LAN (Ethernet), GPIB	стационарн.	