

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.02 –

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

Специализация -

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ОБРАБОТКИ И ПЕРЕДАЧИ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ЗАЩИЩЕННЫЙ ОТ
НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ

Студентка _____ Пронина Наталья Юрьевна

Руководитель инженер 3-й категории

АО «НПП «Рубин» _____ Николаев И.О.

Нормоконтролёр _____ Иванов А.П.

Рецензент инженер 2-й категории

АО «НПП «Рубин» _____ Куприянов А.А.

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

Заведующий кафедрой _____ С.Л. Зефирова

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

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2018

Оглавление

Введение.....	4
1 Обзор существующих решений и выбор, с обоснованием комплектующих, для программно-аппаратного комплекса обработки и передачи конфиденциальной информации	6
2 Классификация технических каналов утечки конфиденциальной информации	13
2.1 Общие сведения технических каналов утечки информации.....	13
2.2 Технические каналы утечки речевой информации	14
2.3 Технические каналы утечки телекоммуникационной информации	17
2.4 Каналы утечки информации при ее передаче по каналам связи	21
2.5 Технические каналы утечки видовой информации.....	22
3 Перечень выявленных источников угроз безопасности информации.....	24
4 Сформированный список существующих методов защиты информации в помещениях.....	28
5 Выбор и сравнение систем, препятствующих записи акустического речевого сигнала и передаче его по беспроводным каналам связи специальными средствами несанкционированного съема информации.....	33
5.1 Методы и средства обнаружения и подавления диктофонов	33
5.2 Методы и средства обнаружения и подавления акустических закладок	34
6 Выбор и обоснование средств защиты, препятствующих перехвату конфиденциальной информации за счет побочных электромагнитных излучений и наводок	38
7 Выбор и обоснование средств защиты программно-аппаратного комплекса от утечки конфиденциальной информации по техническим каналам	50
7.1 Методы и средства защиты телефонных аппаратов и телефонных линий от утечки информации по каналам связи	50
7.2 Защита от утечки видовой информации.....	58

8	Выбор и сравнение средств защиты программно-аппаратного комплекса от внедрения аппаратных закладок	59
8.1	Виды аппаратных закладок.....	59
8.2	Выбор и сравнение средств защиты ПАК от внедрения аппаратных закладок	62
9	Обоснование и выбор систем, препятствующих несанкционированному доступу к конфиденциальной информации	64
9.1	Описание СЗИ от НСД Secret Net Studio.....	64
9.2	Описание СЗИ от НСД Страж NT (версия 4.0)	67
9.3	Выбор и обоснование СЗИ от НСД	71
9.4	Описание выбора АПКШ «Континент»	73
10	Разработка организационно-технических мероприятий по защите информации	75
11	Разработка структуры программно-аппаратного комплекса, защищенного от несанкционированного съема информации.....	78
12	Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	82
	Заключение	85
	Список используемых источников.....	87
	Приложение А Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ».....	90

Введение

В настоящее время информация играет важную роль, как в процессе экономического развития, так и в ходе конкурентной борьбы на внутреннем и внешнем рынках. Развитие предприятий, а так же благополучное функционирование в основном зависит от совершенствования их деятельности в области обеспечения информационной безопасности.

Прогресс в совершенствовании средств вычислительной техники, автоматизированных информационных систем, появление новых информационных технологий повышают производительность труда любой организации, но при этом ускоряют процесс несанкционированного доступа к конфиденциальной информации. Несанкционированное добывание информации осуществляется с помощью множественных технических устройств и средств разведки.

Для обеспечения информационной безопасности предприятия необходимо использовать самые надежные и современные методы и средства защиты информации. Данная необходимость обусловлена тем, что предприятия обрабатывают большой объем конфиденциальных данных, защита которых обязательна по требованиям законодательства. Комплексная система защиты информации обеспечит бесперебойное функционирование деятельности предприятия, предотвратит утечки конфиденциальной информации, а также предотвратит возможный ущерб репутации компании.

Разработка программно-аппаратного комплекса обработки и передачи конфиденциальной информации, защищенного от несанкционированного съема, является решением безопасной обработки и передачи конфиденциальной информации в организации.

Актуальность данной темы обусловлена быстрым развитием технических устройств и систем разведки, позволяющих несанкционированно снять информацию, которые представляют опасность

для организаций, использующих программно-аппаратные комплексы для обработки и передачи конфиденциальной информации.

Целью выпускной квалификационной работы является разработка структуры программно-аппаратного комплекса обработки и передачи конфиденциальной информации, защищенного от несанкционированного съема информации.

Задачами выпускной квалификационной работы являются:

- выбор комплектующих, для программно-аппаратного комплекса обработки и передачи конфиденциальной информации;
- анализ технических каналов утечки конфиденциальной информации;
- выявление источников угроз безопасности информации;
- выбор существующих методов защиты информации в помещениях;
- выбор средств защиты информации для программно-аппаратного комплекса, препятствующие несанкционированному снятию конфиденциальной информации;
- разработка организационно-технических мероприятий по защите информации;
- разработка структуры программно-аппаратного комплекса, защищенного от несанкционированного съема информации.

Разработанный программно-аппаратный комплекс обработки и передачи конфиденциальной информации, позволит обеспечить необходимую защиту от несанкционированного съема конфиденциальной информации в организации.

1 Обзор существующих решений и выбор, с обоснованием комплектующих, для программно-аппаратного комплекса обработки и передачи конфиденциальной информации

Программно-аппаратный комплекс — это набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач [1].

Программно-аппаратный комплекс состоит из двух основных частей [1].

Аппаратная часть — устройство сбора и обработки информации [1].

Программная часть — специализированное программное обеспечение, обрабатывающее и интерпретирующее данные, собранные аппаратной частью [1].

Программно-аппаратный комплекс (ПАК) должен обеспечивать обмен конфиденциальной информации между аналогичными комплексами по выделенным каналам связи.

Для реализации работоспособности программно-аппаратный комплекс должен иметь:

- процессор типа Intel Core i3 или аналогичный с тактовой частотой не менее 3 ГГц;
- оперативное запоминающее устройство не менее 4096 Мбайт;
- видеомонитор типа SVGA с диагональю не менее 17 дюймов;
- видеокарта объемом не менее 512 Мбайт;
- накопитель на жестких дисках объемом не менее 300 Гбайт;
- сетевая карта со скоростью передачи данных не менее 100 Мбит/с;
- USB-порт, в количестве не менее 4 штук;
- Ethernet интерфейс;
- плата медиаконвертера для подключения волоконно-оптической линии связи;
- операционная система – Microsoft Windows 7;

- клавиатура со встроенным тачпадом.

В состав комплекса необходимо включить:

- телефонный аппарат, работающий в стационарных сетях связи, с функцией контроля несанкционированного доступа;
- многофункциональное устройство с цветной лазерной технологией печати и разрешением сканирования не менее 600x600 dpi, без модуля Wi-Fi;

Для выбора мощного процессора, было рассмотрено два типа модели процессор Intel® Core™ i3-8350K и процессор Intel® Core™ i7-8700K. Важные характеристики каждого процессора, представлены в таблице 1.

Таблица 1 – Характеристика процессора Intel® Core™ i3-8350K и i7-8700K

Модель	Intel® Core™ i3-8350K	Intel® Core™ i7-8700K
Количество ядер	4	6
Базовая тактовая частота	4.00 ГГц	3.70 ГГц
Кэш-память	8 Мбайт	12 Мбайт
Технология Hyper-threading	Нет	Да
Технология Turbo boost	Нет	Да

Ядро процессора самый главный компонент, осуществляющий операции как обособленный процессор. Многоядерность является важным элементом для реализации одновременно нескольких задач оператора.

От тактовой частоты зависит как будет ядро обрабатывать информацию. Ядро работающее с более высокой тактовой частотой, будет обрабатывать информацию быстрее, чем с низкой тактовой частотой.

Кэш-память непосредственно встроена в процессор и по сути, то же самое, что и оперативная память RAM, но работает быстрее. Из-за этого существенно ускоряет работу сохранения во временном кэше данных, которые используются постоянно. Без временных хранилищ процессор работал бы медленнее, так как всегда ему приходилось бы обращаться к жесткому диску, что занимает намного больше времени.

Поддержка технологии Hyper-threading создает по два потока вычислений на каждое физическое ядро, которое дает возможность более эффективно использовать вычислительную мощность процессорного ядра. Процессор Intel® Core™ i7-8700K имеет 6 ядер, тогда с помощью данной технологии процессор способен обработать 12 потоков одновременно. Так как в процессоре Intel® Core™ i3-8350K нет данной технологии, то процессор способен обработать всего лишь 4 потока одновременно.

Внедренная Intel технология Turbo Boost допускает процессору динамически увеличивать частоту, если она необходима. Величина увеличения тактовой частоты зависит от количества активных ядер, текущего энергопотребления и температуры процессора. Процессор Intel® Core™ i7-8700K с базовой частотой 3.70 ГГц может благодаря этой технологии увеличить частоту передачи данных до 4.70 ГГц. Процессор Intel® Core™ i3-8350K не имея такой технологии производит передачу данных с базовой частотой 4.00 ГГц.

Соответственно процессор Intel® Core™ i7-8700K является более мощным и быстродействующим чем процессор Intel® Core™ i3-8350K, что имеет важное значение при объемной обработке и передачи конфиденциальной информации в программно-аппаратном комплексе.

Объем оперативной памяти определяет, с какой скоростью процессор сумеет обработать промежуточные данные при работе программ, хранящихся в оперативной памяти. Современное на сегодняшний день, является оперативное запоминающее устройство (ОЗУ) Kingston HyperX Fury DDR4-2666 и оперативное запоминающее устройство Crucial Ballistix Tactical DDR3.

ОЗУ Kingston модели HX426C15FBK2/8, имеет объем памяти 4Гбайт и 2 модуля в комплекте. Частота функционирования до 2666 МГц, пропускная способность памяти 21328 Мбит/сек. ОЗУ Crucial модели BLT2CP4G3D1608DT1TX0CEU, имеет объем памяти 4Гбайт и 2 модуля в комплекте. Частота функционирования до 1600 МГц, пропускная способность памяти 12800 Мбит/сек.

Соответственно было выбрано ОЗУ Kingston модели HX426C15FBK2/8, так как частота функционирования и пропускная способность выше, чем у модели Crucial, что влияет на быстроту обработки данных.

Видеомонитор типа SVGA с диагональю 17 дюймов имеет встроенное устройство управления и подключается к стандартному разъему компьютера и поддерживает стандартный аппаратный интерфейс, т. е. определенную последовательность управляющих сигналов, их полярность, уровень и форму.

Видеокарта модели PNY NVIDIA NVS 310 предназначена для быстрой и рентабельной интеграции. Данная видеокарта оснащена интерфейсом DisplayPort 1.2 и технологией NVIDIA Mosaic™. Так же в ней присутствует программное обеспечение для управления рабочим столом NVIDIA nView®. Поддерживает до двух 30-дюймовых дисплеев с разрешением 2560x1600. Выбранная модель имеет объем памяти 512 Мбайт.

Жесткий диск TOSHIBA P300 HDWD105UZSVA объемом 500 Гбайт имеет высокое качество и надежность. Обладает необходимым объемом и нужной скоростью передачи данных.

Сетевая карта (Ethernet-адаптер) — это периферийное устройство, которое дает возможность компьютеру взаимодействовать с иными устройствами сети. Модель сетевой карты TP-LINK TG-3468 имеет скорость передачи данных 10/100/1000 Мбит/сек.

Материнская плата модели ASRock H81M-ITX имеет размер платы mini-ITX, чипсет соответствует Intel H81. Плата содержит до 2 планок памяти DDR3, DIMM частотой от 1066 до 1600 МГц. В состав входит разъем SATA 6Gb/s: 2, на задней панели: 6xUSB, из них 2xUSB 3.0, оптический выход, Ethernet, D-Sub, HDMI, DVI, eSATA, PS/2 (клавиатура).

Ethernet интерфейс является проводным интерфейсом (технологией) передачи данных между устройствами для компьютерных сетей. Используется Gigabit Ethernet со скоростью 1000 Мбит/с стандарта 1000BASE-T.

Плата медиаконвертера модели PCB-2013W с преобразованием скорости передачи 10/100/1000 Мбит/с. Имеет один WDM порт и один разъем SC/UPC. Дальность оптического порта до 20 км по стандартному SMF волокну. Дальность электрического порта 8P8C до 100 м.

Операционная система (ОС) – Microsoft Windows 7 является самой популярной клиентской ОС от Microsoft, которая построена на сильных и слабых сторонах своих предшественников. Все службы усовершенствованы и новые опции безопасности делают данную систему более надежной. Кроме корректировки базовой системы и новых служб, Windows 7 предоставляет больше функций безопасности, улучшен аудит и мониторинг, а также существует возможность шифрования удаленных соединений и данных. Для обеспечения безопасности внутренних компонентов системы, Windows 7 содержит новые внутренние усовершенствованные системы защиты.

Nano IP-АТС АГАТ модели UX-5110 предназначен для управления звонками, проходящими через интернет-каналы, осуществляет передачу голосового трафика и данных по протоколам IP-телефонии. Nano IP-АТС использует сверхмощный цифровой процессор обработки сигнала. Данная модель имеет небольшой размер, что позволяет установить устройство в кейсе программно-аппаратного комплекса.

Характеристики nano IP-АТС АГАТ UX-5110:

- до 256 внутренних IP-абонентов;
- до 30 IP-транков;
- поддержка одновременно SIP и H323;
- факсы по T.38;
- встроенный модуль интеграции с информационными системами - CRM, ERP и т.п.;
- открытые интерфейсы - VoiceXML, TAPI, SNMP4;
- 2 порта Ethernet;
- все функции современной цифровой автоматизированной телефонной станции (АТС): голосовая и факсимильная почта с доставкой по

e-mail, DISA, IVR, ACD, очереди вызовов, конференцсвязь и еще десятки полезных функций.

Программно-аппаратный комплекс имеет встроенный блок питания с аккумуляторной батареей, ориентировочное время работы без подключения к сети примерно два часа.

Данные элементы программно-аппаратного комплекса интегрированы в кейс.

Телефонный аппарат серии Нефрит-2-Г-ЦБ, с кнопочным номеронабирателем и центральной батареей (ЦБ). Он предназначен для работы в специальных стационарных сетях связи. Питание аппарата происходит от коммутационного оборудования или от центральной батареи автоматической телефонной станции. Аппарат имеет магнитную и электростатическую экранировки, а также имеет функцию контроля несанкционированного доступа к телефонному аппарату.

Лазерное многофункциональное устройство модели HP LaserJet Pro M176n с цветной лазерной технологией печати и разрешением сканирования 1200x1200 dpi, без модуля Wi-Fi.

Структура программно-аппаратного комплекса обработки и передачи конфиденциальной информации, представлена на рисунке 1.

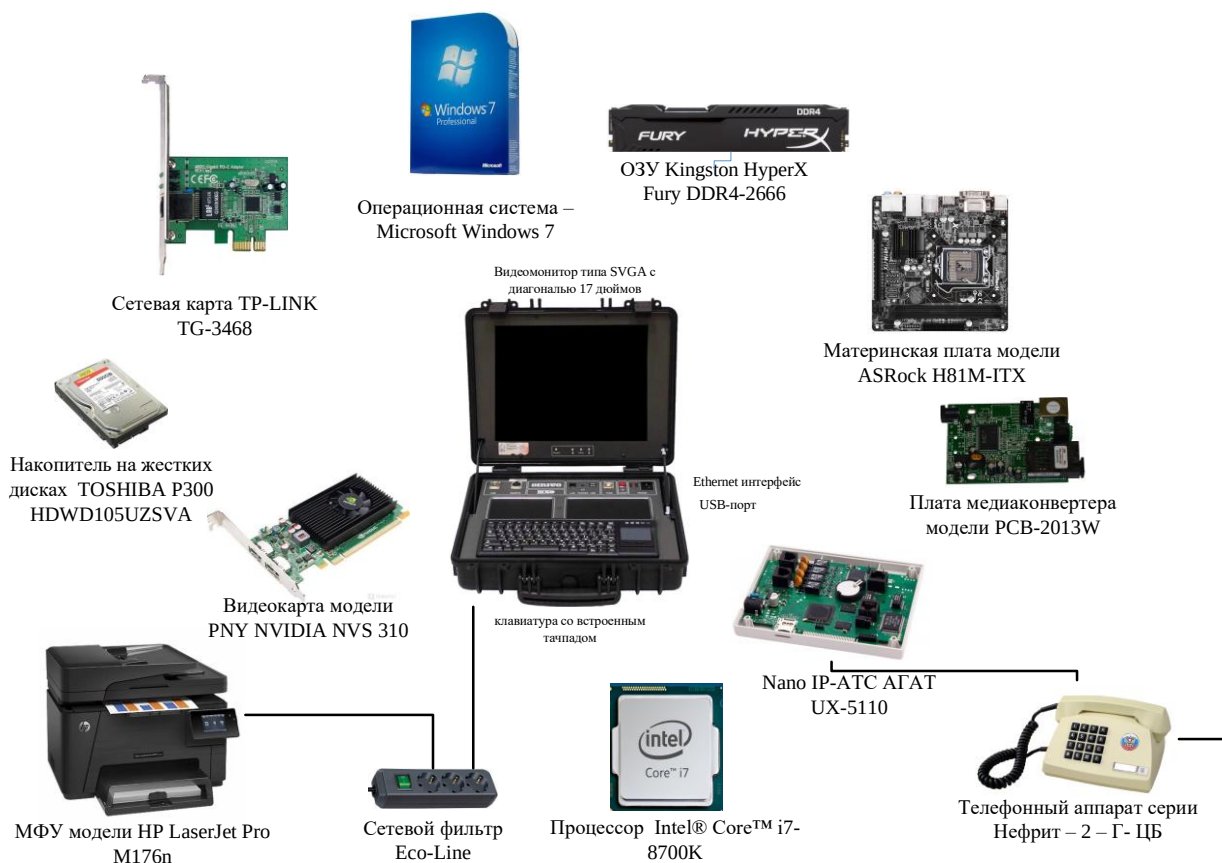


Рисунок 1 - Структура ПАК

2 Классификация технических каналов утечки конфиденциальной информации

2.1 Общие сведения технических каналов утечки информации

Утечка конфиденциальной информации - это несанкционированный процесс переноса конфиденциальной информации от источника к несанкционированному пользователю.

Физический путь переноса информации от её источника к несанкционированному пользователю называется каналом утечки информации. Канал, несанкционированный перенос информации в котором осуществляется с использованием технических средств, называется техническим каналом утечки информации [2].

Технический канал утечки конфиденциальной информации состоит из комплекса объекта технической разведки и физической среды распространения информативного сигнала, а также средств, которыми извлекается конфиденциальная информация.

Техническая защита конфиденциальной информации – защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования [3].

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата техническими средствами разведки (ТСР), технические каналы утечки программно-аппаратного комплекса можно разделить на:

- электромагнитные, электрические и параметрический - для телекоммуникационной информации;
- воздушные (прямые акустические), вибрационные (виброакустические), оптико-электронный, акустоэлектрический, и параметрические - для речевой информации;

- электромагнитные, электрические и индукционные – для информации при ее передаче по каналам связи;
- визуальный - для видовой информации [4].

2.2 Технические каналы утечки речевой информации

Речевая информация - это такая информация, в которой носителем представляют акустические сигналы. Акустический сигнал осуществляется за счет раздражения упругой среды, которые появляются при создании акустических колебаний. Акустическими колебания представляют собой колебания частиц устойчивой среды, которые исходят от источника колебаний в окружающее место в форме волн.

Вибрационные колебания появляются под влиянием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором присутствует источник речевой информации.

Следовательно, первоначальный вид речевого сигнала в защищаемом помещении представлен в виде акустических и вибрационных колебаний. Вторичными источниками являются преобразователи акустических и вибрационных колебаний (например, громкоговорители, телефоны, микрофоны и т.д.).

Перехват речевой информации ограниченного доступа, циркулирующей в защищаемых помещениях (ЗП), с учетом расположения в них различных технических средств, возможен по следующим техническим каналам.

Акустический канал утечки речевой информации, возникает за счет акустического излучения информативного речевого сигнала. Воздух служит средой распространения речевых сигналов. Перехват речевых сигналов осуществляется с помощью специально направленных микрофонов и высокочувствительных микрофонов. В состав направленных микрофонов

входят диктофоны или миниатюрные передатчики, которые соединяются с микрофоном.

Устройства, в состав которых входят микрофоны и передатчики, называются акустическими закладными устройствами.

Перехваченная речевая информация может передаваться по радиоканалу, сети электропитания, оптическому инфракрасному каналу, соединительным линиям вспомогательных технических средств и систем (ВТСС), посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот, телефонной линии с вызовом от внешнего телефонного абонента [2].

Специализированные приемные устройства, которые работают в необходимом диапазоне длин волн, производят прием информации, перехваченной закладными устройствами. Если осуществляется передача информации по телефонной линии, при вызове от внешнего абонента, то прием возможен с обычного телефонного аппарата.

Виброакустический канал утечки речевой конфиденциальной информации, возникает при помощи преобразования информативного акустического сигнала.

Средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.) [2].

Основным способом ведения акустической речевой разведки при использовании данного канала является перехват речевой информации с помощью микрофонов твердой среды (виброметров, акселерометров и т.п.). Также возможен перехват конфиденциальной информации по данному каналу с помощью закладных устройств. Устройства, которые для передачи перехваченной информации пользуются радиоканалом, называют радиостетоскопами. Передача перехваченной информации так же возможна по оптическому каналу и по ультразвуковому каналу (по инженерным коммуникациям).

Оптико-электронный канал утечки речевой конфиденциальной информации, осуществляет лазерное облучение тонких отражающих поверхностей (стекло, металлических поверхностей), которые реализуют вибрацию под воздействием акустического поля информативного речевого сигнала, и производит прием отраженного лазерного излучения.

Основным способом ведения акустической речевой разведки является перехват речевой информации с помощью оптико-электронной лазерной аппаратуры дистанционного прослушивания речи за счет диффузного отражения, а также за счет узконаправленного зеркального отражения.

Акустоэлектрический канал утечки речевой конфиденциальной информации, преобразует акустический информативный сигнал в электрический, с помощью «микрофонного эффекта» во ВТСС и распределяется по линиям и проводам, которые выходят за контролируемую зону.

Данный канал утечки речевой информации образуется при воздействии акустических речевых сигналов на элементы технических средств, в том числе и средств вычислительной техники (микрофоны, аналогово-цифровые преобразователи, усилительные устройства, устройства заземления, а также электроснабжение усилительных систем), расположенных в защищаемых помещениях.

Перехват акустоэлектрических колебаний производится при помощи подключения к соединительным линиям ВТСС специализированных высокочувствительных низкочастотных усилителей.

Параметрический канал утечки конфиденциальной информации осуществляется при помощи «высокочастотного облучения» защищаемого помещения, в котором размещены закладные устройства, элементы которых способны изменяться под воздействием речевого сигнала.

При использовании данного канала способ добывания информации в акустической речевой разведке за счет воздействия (зондирования) высокочастотным электромагнитным полем на технические средства,

попадающие в акустическое поле речевого сигнала, базируется на принудительной (навязываемой) модуляции отраженного от технического средства электромагнитного сигнала, приема и демодуляций этого сигнала. Аппаратура разведки, использующая метод высокочастотного облучения технических средств, в своем составе содержит предающее устройство высокочастотных электромагнитных сигналов (генератор зондирования), приемник модулированного сигнала, демодулятор речевого сигнала, устройство записи и воспроизведения речи.

2.3 Технические каналы утечки телекоммуникационной информации

Под телекоммуникационной информацией, понимается информация, обрабатываемая в технических средствах приема, обработки, хранения и передачи информации.

К техническим средствам приёма, обработки, хранения и передачи информации (ТСПИ) относят технические средства, непосредственно обрабатывающие конфиденциальную информацию. В их число входят электронно-вычислительные машины (ЭВМ), автоматические телефонные станции, информационно-коммуникационные системы, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д. [4].

Для обнаружения технических каналов утечки конфиденциальной информации в основном нужно рассматривать основные технические средства и системы (ОТСС), которые включают главное оборудование, оконечные устройства, коммутационные и распределительные устройства, соединительные линии, системы питания и заземления. Также необходимо, для обнаружения технических каналов, рассматривать вспомогательные технические средства и системы (ВТСС), которые устанавливаются в помещении, но не участвуют в обработке конфиденциальной информации. Данные ВТСС используются вместе с ТСПИ и находятся в зоне электромагнитного поля, создаваемого ТСПИ.

Перехват телекоммуникационной информации ограниченного доступа, циркулирующей в программно-аппаратном комплексе, возможен по следующим техническим каналам.

Электромагнитные каналы утечки информации, возникают за счёт различного вида побочных электромагнитных излучений и наводок (ПЭМИН) ТСПИ:

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;
- излучений на частотах самовозбуждения усилителей низкой частоты ТСПИ [4].

Носителем информации в программно-аппаратном комплексе служит электрический ток, в процессе которого параметры (амплитуда, частота, фаза) меняются по закону изменения информационного сигнала.

Элементы ПАК стоит осматривать как излучатели электромагнитного поля, несущего информацию, так как при протекании электрического тока по элементам ПАК вокруг них появляется электрическое и магнитное поле.

В состав программно-аппаратного комплекса могут входить задающие генераторы, генераторы тактовой частоты, генераторы стирания и т.п. Данные генераторы относятся к высокочастотным генераторам.

На элементах ВЧ – генераторов создаются электрические сигналы благодаря внешним воздействиям информационного сигнала. Электрические сигналы могут спровоцировать паразитную модуляцию собственных ВЧ – колебаний генераторов, которые излучаются в окружающее пространство.

Образования случайных паразитных обратных связей, которые переводят усилители в режим автогенерации сигналов, создают самовозбуждение усилителей низкой частоты ПАК (например, магнитофонов, усилителей систем и т.п.). Промодулированным информационным сигналом, в данном случае является сигнал на частотах

самовозбуждения. Самовозбуждение, прежде всего, обнаруживается при переводе усилителей низкой частоты в режим перегрузки.

Перехват ПЭМИН ПАК производится с помощью средств радиотехнической разведки, которые размещаются вне контролируемой зоны.

Электрические каналы утечки информации возникают за счёт:

- наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы КЗ;
- просачивания информационных сигналов в линии электропитания и цепи заземления ТСПИ;
- использования закладных устройств [4].

Наводки электромагнитных излучений ПАК происходят при наличии гальванической связи соединительных линий ПАК, посторонних проводников, линий ВТСС и при излучении элементами ПАК информационных сигналов. Величина наводимых сигналов в основном зависит от силы излучаемых сигналов, расстояния до проводников и длины совместного пробега соединительных линий ПАК. Побочные электромагнитные излучения могут принимать случайные антенны, которые представляют собой цепь ВТСС или посторонний проводник. Случайные антенны бывают двух видов.

Сосредоточенная случайная антенна выступает в роли технического средства. Распределенная случайная антенна представляет собой кабели, провода и другие коммуникации.

Из-за присутствия магнитных связей между выходным трансформатором усилителя и трансформатором блока питания, осуществляется проникновение информационных сигналов в линии электропитания. Так же проникновение информационного сигнала в линию электропитания, возможно за счет неравномерной нагрузки на выпрямитель, что приводит к перемене потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов может происходить в системе заземления, в которую провода сети электропитания, экраны соединительных кабелей, металлические трубы систем водоснабжения и т.д. Данные проводники вместе с заземляющим устройством создают разветвлённую систему заземления.

Кроме этого, перехват информационных сигналов может происходить с помощью подключения к соединительным линиям ВТСС, посторонним проводникам, к их системам электропитания и заземления.

Съём защищаемой информации, возможен с помощью закладных устройств (ЗУ), которые скрытно внедряются в ПАК. Закладные устройства образуют излучения, которые модулируются информационным сигналом. Данные устройства являются мини-передатчиками. Перехваченная защищаемая информация, с помощью закладных устройств, может передаваться по каналу связи или записываться на специальное запоминающее устройство и передаваться только по команде. Передача информации осуществляется на приёмный пункт, для передачи используются линии электропитания ПАК, радиоканал, оптический (инфракрасный) канал.

Параметрические каналы реализуются при помощи «высокочастотного облучения» ПАК.

Когда происходит взаимодействие облучающего электромагнитного поля с элементами ПАК, то возникает переизлучение электромагнитного поля. Иногда вторичное излучение обладает модуляцией, которая обусловлена воздействием информационного сигнала.

Чтобы осуществить перехват защищаемой информации по параметрическому каналу нужно иметь специализированные высокочастотные генераторы с антеннами и специальные приёмные устройства.

2.4 Каналы утечки информации при ее передаче по каналам связи

Для передачи по каналам связи используются ультракороткие волны, телефонная радиосвязь, кабельные и волоконно-оптические линии связи. При передаче информации по каналам связи, каналы утечки делятся на электромагнитные, электрические и индукционные.

Электромагнитные каналы в основном применяются для прослушивания телефонных разговоров, при котором происходит излучение передатчиков средств связи. Данное электромагнитное излучение перехватывается портативными средствами радиоразведки.

Электрический канал перехвата информации, в основном так же применяется для перехвата телефонных разговоров. Для перехвата информации передаваемой по кабельным линиям связи, используют контактное подключение аппаратуры перехвата к кабельным линиям связи. Контактное подключение осуществляется для снятия информации с низкочастотных и коаксиальных кабелей связи. Существуют устройства, которые используют передачу по радиоканалу, они подключаются к телефонным линиям связи и называются телефонными закладками.

При индукционном канале утечки информации используются индукционные датчики, которые не требуют контактного подключения к линиям связи, они осуществляют съем с высокочастотных кабелей. В данном канале возникает электромагнитное поле вокруг кабеля связи, так как по нему проходят электрические сигналы. Так же съем информации в данном канале возможен с помощью высокочувствительных низкочастотных усилителей. Существуют так же специальные средства бесконтактного съема, которые могут передавать перехваченную информацию по радиоканалу.

2.5 Технические каналы утечки видовой информации

Помимо речевой и телекоммуникационной информации, существенное значение отражает видовая информация. Данная информация перехватывается в виде изображений объектов или документов, с применением технических средств.

В зависимости от характера информации можно выделить следующие способы ее получения:

- наблюдение за объектами;
- съемка объектов;
- съемка (снятие копий) документов [2].

Наблюдение за объектами, осуществляется с помощью разных технических средств, это зависит от освещения и условий наблюдения за объектами. Если наблюдение проводится днем, то используют оптические приборы. Если наблюдение проводится ночью, то используют приборы ночного видения. Расстояние до объекта тоже является важным в наблюдении, так если производится наблюдение с большого расстояния, то используют средства с длиннофокусными оптическими системами, а если производится наблюдение с близкого расстояния, то используют скрытно установленные телевизионные камеры. Телевизионные камеры способны передавать перехваченное изображение по кабелю и по радиоканалу на мониторы.

Съемка объектов осуществляется с помощью телевизионных и фотографических средств, выбор средства обусловлена освещением и условием съемки. Съемка объектов выполняется для детального исследования объектов и подтверждения итогов наблюдения. Если осуществляется съемка в дневное время суток, да еще и с большого расстояния, то применяют фотоаппараты или телевизионные камеры с длиннофокусными объективами. Если осуществляется съемка в дневное время суток с близкого расстояния, то используют портативные

камуфлированные фотоаппараты, а так же телекамеры, которые могут осуществлять видеозапись и передавать изображение по радиоканалу. Осуществление съемки объектов в ночное время суток проводится с близкого расстояния, и используют портативные фотоаппараты, а так же телевизионные камеры, оснащенные приборами ночного видения.

Съемка документов производится с помощью портативных фотоаппаратов.

3 Перечень выявленных источников угроз безопасности информации

В качестве источников угроз безопасности информации могут выступать субъекты (личность) и средства негласного съема информации.

Источники угроз стремятся к следующим целям:

- ознакомление с защищаемыми сведениями;
- модификация защищаемых сведений;
- уничтожение защищаемых сведений.

Источники угроз безопасности информации могут находиться внутри защищаемой организации (внутренние источники) и вне защищаемой организации (внешние источники).

Источники угроз безопасности информации для программно-аппаратного комплекса можно разделить на две основные группы:

- вызванные действиями субъекта (антропогенные источники угроз);
- вызванные техническими средствами (техногенные источники угроз) [5].

Антропогенными источниками угроз безопасности информации являются субъекты, которые в результате своих действий могут быть совершить умышленные или случайные преступления. Данные источники представляют наибольший интерес с точки зрения организации защиты, поскольку действия субъекта всегда можно оценить, предсказать и принять соответствующие меры.

Субъект, который имеет санкционированный или несанкционированный доступ к работе со штатными средствами защищаемого объекта, рассматривается в виде антропогенного источника угроз. Субъекты (источники), действия которых приводят к нарушению безопасности информации, могут внешние и внутренние.

Внешние источники могут быть случайными или преднамеренными, а так же иметь разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур [5].

Внутренние источники, выступают в роли профессиональных специалистов в сфере разработки, использования программных и технических средств. Так же некоторые внутренние источники имеют представление о структуре и функций программно-аппаратных средств защиты информации.

К внутренним источникам относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация) [5].

К особой группе внутренних антропогенных источников относятся лица с нарушенной психикой, а так же завербованные и умышленно внедренные агенты.

Техногенные источники угроз информационной безопасности менее прогнозируемые, так как являются техническими средствами. Данные источники требуют особого внимания, поскольку зависят от свойств техники. В современных условиях происходит значительное количество техногенных катастроф, вызванные физическим и моральным устареванием технического парка и отсутствием материальных средств на его обновление, следовательно, техногенные источники угроз безопасности информации особенно актуальны. Техногенные источники угроз, могут быть внутренними и внешними.

К внутренним источникам таких угроз относятся:

- использование не сертифицированного и не лицензионного программного обеспечения для хранения, передачи и обработки информации;

- не качественные программные средства обработки информации;

- использование не качественных технических средств;

- вспомогательные средства (охраны, сигнализации, телефонии)

[5].

К внешним источникам техногенных угроз информационной безопасности относятся:

- каналы связи;

- недоброкачественные внешние поставки программных и аппаратных средств;

- сети инженерных коммуникации (водоснабжения, канализации)

[5].

Основными угрозами информационной безопасности, реализованные с помощью технических устройств негласного получения конфиденциальной информации, обрабатываемой в программно-аппаратном комплексе, являются:

- наличие электрических сигналов распределяющих по линиям и проводным цепям, которые создаются за счет преобразования информативных сигналов из акустических в электрические при помощи микрофонного эффекта;

- наличие опасных сигналов при высокочастотном облучении и высокочастотном навязывании;

- утечка конфиденциальной информации при помощи побочных электромагнитных излучений и наводок;

- перехват конфиденциальной информации с помощью закладных устройств, установленных в технических средствах иностранного производства;

- перехват конфиденциальной информации за счет перехвата информативного сигнала устройствами негласного получения информации и передаче его по беспроводным каналам связи;
- утечка речевой конфиденциальной информации по виброакустическому каналу;
- перехват конфиденциальной информации по каналам связи;
- перехват конфиденциальной информации визуально-оптическим способом;
- копирование конфиденциальной информации в результате несанкционированного доступа в ПАК.

4 Сформированный список существующих методов защиты информации в помещениях

Методы защиты информации в помещениях обеспечивают защиту от:

- несанкционированного физического проникновения к помещению;
- визуального наблюдения;
- подслушивания;
- перехвата электромагнитных излучений.

Защита от несанкционированного физического проникновения к помещению реализуется с помощью препятствий.

На входе предприятия (организации) должен быть организован контрольно-пропускной пункт. Проход сотрудников на территорию предприятия осуществляется по пропускам. Пропуск представляет собой основной документ, который обеспечивает право на проход.

Во всех коридорах, ведущих к помещению, должны быть установлены видеонаблюдения.

Для помещений осуществляется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей конфиденциальную информацию, а также исключается или существенно затрудняется возможность несанкционированного проникновения и пребывания в этих помещениях посторонних лиц.

В защищаемом помещении обязаны размещать списки, в которых указываются работники, допущенные в данное помещение. Защищаемое помещение, после завершения работ, должны осматриваться специальными ответственными лицами. После этого защищаемое помещение закрывается на замок и опечатывается. Ключи защищаемого помещения передают охраннику. Данные ключи могут получить только лица имеющие допуск к данному помещению. Списки работников подписываются начальником подразделения и утверждаются начальником службы безопасности.

Защита от визуального наблюдения осуществляется с помощью:

- создания наилучшего размещения ПАК, для недопущения неправомерного наблюдения;
- использования средств преграждения, а именно темные стекла, шторы, жалюзи и т.п.;
- выбора помещений, в которых окна направлены на безопасное направление;
- использования специальных средств гашения экрана ПАК.

Защита от подслушивания реализуется с помощью пассивных и активных методов и средств.

Пассивные методы защиты от прослушивания осуществляют:

- снижение речевых сигналов на контролируемой зоне до требуемого уровня, для исключения перехвата речевых сигналов средствами разведки;
- снижение информационных электрических сигналов в соединительных линиях ВТСС, которые обладают микрофонным эффектом, до требуемого уровня, для исключения перехвата электрических сигналов средствами разведки;
- снижение или исключение проникновения сигналов высокочастотного навязывания во ВТСС, которые обладают микрофонным эффектом;
- выявление излучений акустических закладок и диктофонов, которые осуществляют запись;
- выявление неправомерных подключений к телефонным линиям связи.

Активные методы защиты от прослушивания реализуют:

- формирование маскирующих акустических и вибрационных помех, для снижения отношения сигнал/шум на границе контролируемой зоны до требуемого значения, исключающих перехват информационного акустического сигнала средствами разведки;

- формирование маскирующих электромагнитных помех в соединительных линиях, линиях электропитания ВТСС, которые обладают микрофонным эффектом, для снижения отношения сигнал/шум до требуемого значения, исключающих перехват информационного сигнала средствами разведки;
- электромагнитное и ультразвуковое подавление диктофонов, которые осуществляют запись;
- формирование прицельных радиопомех акустическим и телефонным радиозакладкам для снижения отношения сигнал/шум до требуемого значения, исключающих перехват информационного сигнала средствами разведки;
- нейтрализация средств неправомерного подключения к телефонным линиям;
- уничтожение средств неправомерного подключения к телефонным линиям.

Ослабление акустических (речевых) сигналов создается с помощью звукоизоляции помещений. Звукоизоляция помещений проводится для исключения утечки акустической (речевой) информации по прямому акустическому и вибрационному каналам. Она направлена на нейтрализацию источников акустических сигналов. Главное условие к звукоизоляции помещений является снижение соотношения сигнал/шум в вероятных местах утечки конфиденциальной информации посредством уменьшения информативного сигнала.

Самыми слабыми звукоизолирующими элементами в помещении являются двери и окна.

В защищаемом помещении необходимо устанавливать двойные двери с тамбуром, в которых должна обладать вибрационная развязка. Для усиления звукоизоляции, двери обиваются уплотнительными прокладками, и проводится облицовка внутренних поверхностей тамбура.

Для звукоизоляции окон, необходимо использовать тройное остекление окон на двух рамах, которые закрепляются на отдельные коробки. Между коробками целесообразно укладывать звукопоглощающий материал.

Акустические экраны используют для усиления звукоизоляции помещения, они устанавливаются в наиболее опасных местах распространения звука.

Для усиления звукоизоляции стен, используют материалы, резко отличающиеся друг от друга, и важным элементом является применение однослойных и многослойных ограждений.

Для звукоизоляции технологических коммуникаций, оснащенных проемами, обеспечивается с использованием специальных коробов, прокладок, вязкоупругих заполнителей и т.п. Для осуществления звукоизоляции в вентиляционных каналах применяются акустические фильтры и глушители.

Если пассивные средства защиты от прослушивания в помещении не осуществляют соответствующую защиту по звукоизоляции, то необходимо применять активные меры защиты.

Активные меры защиты осуществляют акустические и виброакустические маскировки информационных сигналов. Маскировку речевых сигналов обеспечивают с помощью наложения помех. Акустическая маскировка снижает отношение сигнал/шум на границе контролируемой зоны за счет увеличения уровня шума (помехи).

Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброакустическому и оптико-электронному каналам утечки информации [6].

Для создания акустических помех используются специальные генераторы шумового сигнала, к которым подключаются звуковые колонки и (или) вибрационные излучатели.

В помещениях, в местах где наибольшая возможность

несанкционированного снятия информации, устанавливают звуковые колонки систем зашумления. Вибрационные излучатели же устанавливаются на рамах, стеклах, трубопроводах, стенах, потолках и т.п., и приводят к существенному повышению в них уровня вибрационных шумов, что ухудшает прием и восстановление перехваченной речевой информации.

Защита информации с помощью перехвата электромагнитных излучений осуществляется за счет:

- экранирования зданий, отдельных помещений и средств, линий связи, при помощи поглощающих и отражающих материалов;
- маскировка сигналов, осуществляется применением генераторов активных помех, подавляющих фильтров в цепях. Генераторы защищают, с помощью наложения помех в ограждающие конструкции, речевую информацию, которая находится в помещении. Защита речевой информации осуществляется от прослушивания с помощью микрофонов, лазерных систем съёма информации и т.д;
- снижение излучений, при применении эквивалентных антенн, естественных и промышленных помех, за счет звукового или шумового фона;
- применение локальных систем, которые не имеют выход за контролируемую зону.

5 Выбор и сравнение систем, препятствующих записи акустического речевого сигнала и передаче его по беспроводным каналам связи специальными средствами несанкционированного съема информации

5.1 Методы и средства обнаружения и подавления диктофонов

Для обнаружения работающих в режиме записи диктофонов применяются так называемые детекторы диктофонов [6].

Детекторы диктофонов обнаруживают магнитное поле, которое создает диктофон в режиме записи. Магнитное поле наводит электродвижущую силу, которая исходит из шума, с помощью блока обработки сигналов. Если превышает пороговое значение сигнала, то срабатывает звуковая сигнализация. Недостатком данных приборов является постоянная корректировка порога обнаружения.

Существуют переносные варианты детекторов диктофонов. В данном случае датчик сигнализации и блок анализа детектора располагается в кармане оператора, а поисковая антенна же находится в рукаве. Если превышает пороговое значение, то означает что диктофон находится в режиме записи. При обнаружении излучения датчик сигнализации оповещает оператора о предполагаемой записи разговора, с помощью вибрации.

Существуют стационарные детекторы диктофонов, которые обустроены несколькими датчиками.

Стационарный детектор так же состоит из блока анализа, антенны и индикатора. Антенна, блок анализа и индикатор обнаружения, в данном случае размещается в столе программно-аппаратного комплекса. При обнаружении излучения диктофона срабатывает индикация.

Работающие диктофоны создают слабый показатель магнитного поля, поэтому диапазон их обнаружения детекторами незначительна.

Помимо средств обнаружения диктофонов применяют средства подавления диктофонов.

Для этих целей используются устройства электромагнитного

подавления типа «Рубеж», «Шумотрон» и устройства ультразвукового подавления типа «Завеса» [6].

Средства подавления диктофонов осуществляют электромагнитное подавление, с помощью сильнейших шумовых сигналов. Для подавления прежде всего применяют импульсные сигналы. Помеховые сигналы, которые излучаются антеннами, влияют на элементы электронной схемы диктофона, посредством этого производят в них наводки шумовых сигналов. Следовательно, одновременно производится запись разговора и шумового сигнала, что вызывает существенное искажение записи разговора.

Средства подавления диктофонов основанные на ультразвуковом подавлении, осуществляют сильные беззвучные ультразвуковые колебания. Данные средства воздействуют на микрофоны диктофонов, это и есть их преимущество. Существенные искажения записываемых сигналов, реализуются благодаря перегрузке усилителя низкой частоты диктофона, при помощи ультразвукового воздействия.

Сравнивая средства электромагнитного подавления и ультразвукового подавления, можно отметить что, ультразвуковое подавление является наиболее подходящим, так как оказывают подавление в большом секторе.

Например, комплекс «Завеса» при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 м³ [6].

К сожалению, у средства ультразвукового подавления есть недостаток. Если на микрофон диктофона положить фильтр из специального материала, то действенность ультразвукового подавления значительно снижается.

5.2 Методы и средства обнаружения и подавления акустических закладок

Для обнаружения радиозакладок в защищаемых помещениях проводят визуальный осмотр помещения. Обнаружение осуществляется по демаскирующим признакам их внешнего вида.

При поиске радизакладок и их подавления используются индикаторы поля, интерсепторы, радиочастотомеры, сканерные приемники, программно-аппаратные комплексы контроля и другие технические средства [7].

Самый наилучший способ выявления радиозакладок в защищаемых помещениях служит круглосуточный радиоконтроль, для этого применяют специальные программно-аппаратные комплексы контроля. Данные программно-аппаратные комплексы состоят из широкополосной антенны и звуковой колонки, которые подключаются к блокам коммутатора, с помощью данных элементов контролируется защищаемое помещение.

До обнаружения передачи информации радиозакладкой, можно осуществить постановку прицельных помех на частоте передачи закладки, например с помощью постановки помех АРК-СП.

Пространственное электромагнитное зашумление, так же может применяться для подавления радиозакладок. Для этого необходимо воспользоваться генератором шума с повышенной мощностью, так как многие радиозакладки имеют высокую мощность.

Для подавления диктофонов и акустических закладок в помещении, был выбран блокиратор «Завеса-Аудио», представленный на рисунке 2.



Рисунок 2 - Блокиратор «Завеса-Аудио»

Данный блокиратор излучает мощные беззвучные ультразвуковые колебания, которые приводят к значительным искажениям записываемых (передаваемых) сигналов.

Технические характеристики:

- время непрерывной работы – от 3 до 4 часа (мин/макс);
- дальность блокирования микрофонов – от 2 до 7 метров;

- время заряда аккумуляторной батареи – 5 часов (не более);
- эффективный угол излучения помехи - 80 градусов;
- количество излучателей – 4 шт.;
- габаритные размеры – 110-73-25 мм (Д-Ш-В);
- диапазон рабочей температуры – от плюс 5 до минус 40 °С;
- относительная влажность – не более 85% [8].

Данный блокиратор «Завеса-Аудио» результативно подавляет все типы микрофонов, независимо от типа устройства. Производит блокировку проводных микрофонов, радиомикрофонов, диктофонов цифровых и пленочных, диктофонов в мобильных телефонах и смартфонах. Блокирует микрофоны в мобильных телефонах не зависимо от типа и стандарта телефона (GSM, 3G, 4G, CDMA и т.д.).

Для блокировки устройств передачи информации по беспроводной связи необходимо применять устройство ЛГШ-719. Блокиратор беспроводной связи ЛГШ-719, осуществляет блокирование устройств, которые работают в определенных стандартах, способных неправомерно снять информацию.

Блокирование осуществляется в следующих стандартах:

- IMT-MC-450;
- GSM900;
- DSC/GSM1800, (DECT1800);
- IMT-2000/UMTS (3G);
- 4G (LTE, WiMAX);
- 4G – 800;
- Bluetooth;
- Wi-Fi [9].

Данный блокиратор производит шумовую помеху в нужном диапазоне частот. Блокирование беспроводных стандартов связи осуществляется в защищаемом помещении. У данного блокиратора имеется регулировка, которая определяет мощность помехового сигнала в

определенном диапазоне. Блокиратор ЛГШ-719 представлен на рисунке 3.



Рисунок 3 – Блокиратор ЛГШ-719

Данный блокиратор обеспечит защиту от неправомерно съема конфиденциальной информации через стандарты сотовой связи, а так же произведет блокировку устройств неправомерного прослушивания, которые построены на базе сотового телефона и цифровых каналов передачи данных Bluetooth и Wi-Fi.

6 Выбор и обоснование средств защиты, препятствующих перехвату конфиденциальной информации за счет побочных электромагнитных излучений и наводок

Защита конфиденциальной информации, которая обрабатывается ПАК, от утечки за счет ПЭМИН, реализуется с помощью пассивных и активных методов и средств.

Пассивные методы защиты информации осуществляют:

- снижение побочных электромагнитных излучений ПАК на границе контролируемой зоны до требуемого значения, для исключения перехвата электромагнитных излучений средствами разведки;
- снижение наводок побочных электромагнитных излучений ПАК в посторонних проводниках и соединительных линиях ВТСС, которые выходят за контролируемую зону, до требуемого значения, для исключения перехвата электромагнитных излучений средствами разведки;
- снижение или исключение просачивания информационных сигналов ПАК в цепи электропитания, которые выходят за контролируемую зону, до требуемого значения, для исключения перехвата информационных сигналов средствами разведки.

Активные методы защиты информации реализуют:

- формирование маскирующих пространственных электромагнитных помех, для снижения отношения сигнал/шум на границе контролируемой зоны до требуемого значения, исключающих перехват информационного сигнала ПАК средствами разведки;
- формирование маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС для снижения отношения сигнал/шум на границе контролируемой зоны до требуемого значения, исключающих перехват средствами разведки информационного сигнала ПАК.

Ослабление побочных электромагнитных излучений и наводок ПАК

производится за счет экранирования и заземления ПАК, а так же его соединительных линий.

Исключение и уменьшение просачивания информационных сигналов программно-аппаратного комплекса в цепи электропитания, осуществляется с помощью фильтрации информационных сигналов.

Маскирующие электромагнитные помехи реализуются с применением систем пространственного и линейного зашумления. Они представляют собой генераторы шумового сигнала.

Экранирование технических средств. Работоспособность программно-аппаратного комплекса связано с протеканием электрических токов различных частот и образованием разности потенциалов, все эти величины порождают магнитные и электрические поля, которые называются побочными электромагнитными излучениями.

Узлы и элементы программно-аппаратного комплекса, формируют на небольшом расстоянии электромагнитные поля, либо с преобладанием магнитной составляющей, либо с преобладанием электрической составляющей. Преобладание зависит от протекающего тока и перепада напряжения, если ток маленький, а перепады напряжения большие, то преобладает электрическая составляющая, а если противоположные значения, то магнитная.

Электрическое и магнитное поля переменны, и формируются не только вокруг программно-аппаратного комплекса, но и вокруг соединительных линий (провода, кабели) ПАК.

Электромагнитные излучения и наводки ПАК, создают благоприятные условия для снятия конфиденциальной информации, так как из-за электромагнитного излучения появляются электромагнитные и параметрические каналы утечки информации, и возникают наводки информационных сигналов в посторонних токоведущих линиях и конструкциях.

Для действенного уменьшения уровня ПЭМИН необходимо

использовать экранирование их источников.

Различают следующие способы экранирования:

- электростатическое;
- магнитостатическое;
- электромагнитное [6].

При электростатическом экранировании внедряется соединенный с основным проводом токопроводящий экран, который уменьшает паразитную емкость между электрическими цепями.

При электростатическом экранировании, заземление экрана является важным действием, так как электростатическое поле выносится на металлический экран, а электрические заряды сводятся на землю. Металлический экран поможет целиком ликвидировать воздействие электростатического поля.

Эффективность экранирования зависит от емкости связи и рецептора наводки, при снижении емкости связи эффективность экранирования возрастает. Следовательно, главной функцией экранирования является уменьшение емкости связи между экранируемыми составляющими конструкции.

Для повышения эффекта экранирования, нужно качественно соединить отдельные части экрана между собой, не должно быть соединительных проводов между корпусом и частями экрана.

Магнитостатическое экранирование осуществляет, через соседнее магнитное поле, подавление паразитных индуктивных связей между двумя электрическими цепями.

Материал экрана должен обладать большой магнитной проницаемостью и изготавливаться из магнитомягких материалов. Толщина стенок экрана должна быть как можно толще, это приводит к усилению эффективности. Заземление экрана не обязательно. При использовании многослойных экранов эффективность увеличивается.

Экранирование высокочастотного магнитного поля реализовано на

основе магнитной индукции, которая образует в экране вихревые токи. Магнитное поле в этом случае внутри экрана слабое, а вне экрана сильное. Внутренние слои экрана экранируются вихревыми токами, которые двигаются в поверхностных слоях, и по мере проникновения в глубь металла магнитное поле ослабевает.

Эффективность магнитного экранирования основывается от электрических особенностей материала и от частоты, чем частота меньше, тем действие экрана слабее. Заземление экрана не обязательно, так как не влияет на эффективность магнитного экранирования.

Электромагнитное экранирование используется на больших частотах и подавляет электромагнитное поле. Высокочастотное электромагнитное поле ухудшается созданным полем обратного направления. Экранирующее действие вихревых токов устанавливается обратным полем и поверхностным эффектом в материале экрана.

Помимо элементов программно-аппаратного комплекса, экранировать необходимо соединительные линии и монтажные провода.

Для хорошей эффективности экранирования, нужно применять витую пару, в которой должна использоваться защищенная экранирующая оболочка.

При малых частотах применяют коаксиальные кабели с двойной оплеткой, при больших частотах внешняя поверхность толщины экрана важна для экранирования, и если толщина превосходит глубину проникновения поля, то двойное экранирование не нужно.

Экранированные провода и кабели в большей степени используют для соединения отдельных блоков и узлов друг с другом.

Высокую защиту от ПЭМИН при экранировании, гарантируют информационные линии связи типа экранированного трифиляра, триаксильного кабеля, экранированного плоского кабеля.

Заземление технических средств. Главным условием для эффективности экранирования, так и для защиты ПАК, является правильное заземление ПАК и соединительных линий.

Заземление построено на защитных действиях, оно уменьшает значение разности потенциалов между заземленными предметами до безопасного значения, и отводит токи утечки при контакте проводников.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы [6].

Одноточечная последовательная схема заземления самая простая. Но недостатком этой схемы является то, что по участку заземляющей цепи протекают обратные токи разных цепей. Поэтому в посторонних цепях может появляться опасный сигнал.

Одноточечная параллельная схема заземления требует много заземляющих проводников и поэтому иногда появляется трудность с обеспечением малого сопротивления заземления участков цепи. В системе заземления возможно возникновение уравнивающих токов и появления разности потенциалов, это обусловлено тем, что в системе используется приличное число заземляющих проводников, в которых появляются нежелательные связи, образуя несколько путей заземления для каждого устройства.

Многоточечная схема заземления самая наиболее надежная. С помощью данной схемы производится заземление каждого отдельного устройства и участка корпуса. При выполнении многоточечной системы заземления нужно обходиться специальными мерами для устранения замкнутых контуров.

Система заземления обязана содержать общий заземлитель, заземляющий кабель, шины и провода, а сопротивление его элементов должна быть как можно меньше. Элемент заземления, с помощью индивидуального ответвления, обязан быть присоединен к заземлителю, не

используя последовательное подключение. Необходимо остерегаться применения общих проводников в системах экранирующих заземлений, а также необходимо исключать замкнутые контуры, которые могут появиться из-за нежелательных связей между устройствами и цепями. Контактные соединения не должны производить гальванические пары и оксидные пленки на контактирующих поверхностях. Не разрешается для заземления применять нулевые фазы электросетей, металлические трубы систем отопления, водоснабжения и т.п.

Фильтрация информационных сигналов. Для предотвращения опасных сигналов, которые циркулируют в программно-аппаратном комплексе, применяют фильтрацию. Программно-аппаратный комплекс излучает электромагнитные поля и наводки, но с помощью фильтрации происходит устранение нежелательных колебаний за пределы ПАК.

Фильтрации опасных сигналов в цепях питания ПАК осуществляется с помощью разделительных трансформаторов и помехоподавляющих фильтров.

Разделительные трансформаторы. Разделительные трансформаторы осуществляют развязку первичной и вторичной цепей, в первой цепи образуются наводки, а во второй цепи не проникают данные наводки. Если во второй цепи наводки проникают, то значит, что в цепях присутствуют нежелательные резистивные и емкостные связи между обмотками.

Для снижения связи обмоток, между первичной и вторичной обмотками прокладывают заземленную прокладку или фольгу, которая называется внутренним экраном. При использовании данного экрана, наводка в первичной обмотке замыкается на землю, но выделяет электростатическое поле вокруг себя, что может являться поводом для проникновения наводок во вторую цепь.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

- разделения по цепям питания источников и рецепторов наводки,

если они подключаются к одним и тем же шинам переменного тока;

- устранения асимметричных наводок;
- ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки [6].

В разделительных трансформаторах наделяется высокое сопротивление между обмотками с помощью средства развязки и экранирования. Они осуществляют малое сопротивление для наводок из первичной обмотки на землю. Емкость между обмотками мала, а сопротивление высокое, поэтому данные разделительные трансформаторы имеют высокую степень подавления наводок.

Помехоподавляющие фильтры. Для того чтобы уменьшить или исключить электромагнитные помехи распространяющиеся по проводникам, цепям, линиям необходимо применение помехоподавляющих фильтров, которые нейтрализуют внешние и внутренние источники помех. На данный момент существует большое количество различных типов фильтров (фильтры нижних частот, фильтры верхних частот, заграждающие фильтры и полосовые), которые делают возможным ослабление опасных сигналов на различных местах частотного диапазона. Фильтры подавляют сигналы с частотами, которые лежат за пределами рабочей полосы.

Подавление проникновения информационных сигналов в цепи электропитания осуществляется при помощи фильтров нижних частот.

Фильтр нижних частот игнорирует сигналы с частотами ниже граничной частоты и препятствует частотам выше граничной частоты.

Защитные фильтры обязаны гарантировать функционирование, даже при механических нагрузках и перепадах температур. Напряжение и ток должны совпадать с напряжением и током фильтруемой цепи, а снижение опасных сигналов должна быть не менее требуемой, при этом ослабление полезного сигнала должно быть несущественным.

Фильтры цепей питания должны иметь минимальное затухание (не

больше 0,2 дБ) в цепи постоянного тока и максимальное затухание (не меньше 60 дБ) в полосе подавления. Сетевые фильтры обязаны работать результативно при больших проходящих токах, повышенных напряжениях и значительно высоких уровнях мощности.

Конструктивно фильтры подразделяются на:

- фильтры на элементах с сосредоточенными параметрами (LC-фильтры) - обычно предназначены для работы на частотах до 300 МГц;
- фильтры с распределенными параметрами (полосковые, коаксиальные или волноводные) - применяются на частотах свыше 1 ГГц;
- комбинированные - применяются на частотах от 300 МГц до 1 ГГц. В настоящее время промышленностью выпускаются несколько серий защитных фильтров [6].

Пример сетевого помехоподавляющего фильтра Фаза-1-10. За счет подавления наводок опасных (информативных) сигналов, данный фильтр предотвращает утечку информации с программно-аппаратного комплекса обработки и передачи конфиденциальной информации по линиям питающей сети, выходящими за пределы защищаемого помещения или за границы контролируемой зоны. Фильтр Фаза-1-10, представлен на рисунке 4.



Рисунок 4 – Помехоподавляющий фильтр Фаза-1-10

Технические характеристики:

- эффективность подавления наводок в сети в диапазоне частот от 10 кГц до 1 МГц – от 40 до 150 дБ;
- эффективность подавления наводок в сети в диапазоне частот от 1 МГц до 1000 МГц – не менее 55 дБ;
- напряжение сети с частотой от 50 до 60 Гц – от 100 до 240 В;

- нагрузочная способность – до 2000 ВА;
- количество подключаемых потребителей – 3;
- ток утечки – от 6 до 10 мА;
- масса – 1,4 кг [10].

Пространственное и линейное зашумление. Применение пассивных методов защиты, сформированных на использовании фильтрации и экранирования программно-аппаратного комплекса, не всегда является достаточным. Пассивные методы ослабевают уровень ПЭМИН, что приводит к снижению опасного сигнала, но иногда опасный сигнал на границе контролируемой зоны выше позволенного значения. В этом случае применяют активные методы защиты, основанные на формировании помехового шума, которое провоцирует снижение отношения сигнал/шум.

Перехват побочных электромагнитных излучений по электромагнитному каналу осуществляется с помощью пространственного зашумления. Устранение съема наводок информационных сигналов с линий ВТСС реализуется за счет линейного зашумления.

Система пространственного зашумления, используется для образования маскирующих электромагнитных помех в диапазоне частот, где может возникать перехват ПЭМИН ПАК. Образованные помехи должны осуществлять наименьшее допустимое значение отношения сигнал/шум на границе контролируемой зоны (КЗ), уровень помехи не должен превышать требуемых норм.

Если отношение опасного сигнал/шум не превосходит требуемого допустимого значения, вычисляемого по специальным методикам для каждой частоты ПЭМИН ПАК, то задача пространственного зашумления является выполненной.

При использовании пространственного зашумления применяются помехи типа «белого шума» или «синфазные помехи».

Метод «синфазной помехи» осуществляется за счет импульсов случайной амплитуды, которая соответствует импульсам полезного сигнала.

Поэтому помеховой сигнал аналогичен спектру ПЭМИН ПАК, а точнее система имитирует помеху соответствующего скрываемого сигнала.

На сегодняшний день, в большинстве случаев применяют пространственное зашумление с помехой типа «белый шум». Данный тип помехи излучает широкополосный шумовой сигнал, который значительно превышает уровень побочных электромагнитных излучений.

Шумовой сигнал осуществляется с помощью специализированного генератора шума, который выполнен в виде отдельного блока с питанием от сети, или в виде отдельной платы, которая встраивается в системный слот компьютера и питание осуществляется от общей шины компьютера.

Пространственное зашумление защищает ПАК в основном от утечки электромагнитного канала, но так как шумовой сигнал при излучении наводится и в соединительные линии ВТСС и в посторонние проводники, которые выходят за пределы КЗ, то защита производится и от электрического канала утечки информации.

Линейное зашумление реализуется для скрывания наведенных опасных сигналов в соединительных линиях ВТСС и посторонних проводниках, которые выходят за пределы контролируемой зоны.

В системе линейного зашумления используется генератор шума, который образует шумовое маскирующее напряжение с определенными характеристиками и подключается в зашумляемую линию.

Ниже представлены примеры генераторов шума и их описание.

Генератор шума ГШ-К-180 выполнен в виде платы, которая встраивается в системный слот компьютера. Реализует защиту ПЭМИН программно-аппаратного комплекса, размещенного в помещении площадью приблизительно от 40 до 50 м². Данный генератор шума создает и излучает в окружающее пространство электромагнитное поле шума, а так же наводит маскирующий сигнал в отходящие цепи и инженерные коммуникации. Генератор шума ГШ-К-1800, представлен на рисунке 5.



Рисунок 5 – Генератор шума ГШ-К-1800

Технические характеристики:

- диапазон рабочих частот – от 0,1 до 1800 МГц;
- коэффициент качества шума – не менее 0,8;
- регулировка уровня – дискретная;
- индикация – свет, звук;
- антенна – рамочная;
- электропитание – плюс 12 В, плюс 5 В;
- потребляемая мощность – менее 5 Вт [10].

Генератор шума «Бриз» обеспечивает защиту объектов информатизации. Генератор является широкополосным, который образует помеху в диапазоне до 2000 МГц. Осуществляет маскировку ПЭМИН, производит блокирование радиоканалов мощностью до 10 мВт и подавляет приемники различных систем дистанционного управления.

Генератор шума «Бриз», представлен на рисунке 6.



Рисунок 6 - Генератор шума «Бриз»

Технические характеристики:

- диапазон рабочих частот – от 0,2 до 2000 МГц;
- интегральное значение выходной мощности- не менее 7 Вт;
- питание – сеть 220 В, 50 Гц;
- потребляемая мощность – не более 15 ВА;

- размеры корпуса изделия – 50-95-145 мм (Д-Ш-В);
- масса – не более 1 кг [10].

Для защиты программно-аппаратного комплекса, обработки и передачи конфиденциальной информации, необходимо применять пассивные и активные методы защиты от утечки по ПЭМИН. Для исключения просачивания информационных сигналов в цепи электропитания использовать помехоподавляющий фильтр Фаза-1-10. Данный фильтр за счет подавления наводок опасных (информативных) сигналов, предотвращает утечку информации с программно-аппаратного комплекса обработки и передачи конфиденциальной информации по линиям питающей сети, выходящими за пределы защищаемого помещения или за границы контролируемой зоны. Так как ПАК является переносным, заземление ПАК и его соединительных линий нецелесообразно. Экранирование в основном осуществляется при правильном заземлении, и для того чтобы это средство работало, необходимо уметь корректно экранировать ПАК и его соединительных линий, что является трудоемким процессом. Поэтому экранирование ПАК и соединительных линий не лучший вариант. Для защиты от ПЭМИН необходимо так же использовать пространственное зашумление, представляющее из себя генератор шумового сигнала. В данном случае, для защиты программно-аппаратного комплекса, удобнее применять встроенный в системный слот компьютера генератор шума ГШ-К-180. Защита обеспечивается путём создания и излучения в окружающее пространство электромагнитного поля шума и наведения маскирующего сигнала в отходящие цепи и инженерные коммуникации.

Данные средства защиты от ПЭМИН, смогут обеспечить защиту конфиденциальной информации, обрабатываемой в программно-аппаратном комплексе.

7 Выбор и обоснование средств защиты программно-аппаратного комплекса от утечки конфиденциальной информации по техническим каналам

7.1 Методы и средства защиты телефонных аппаратов и телефонных линий от утечки информации по каналам связи

Для защиты телефонных аппаратов и телефонных линий от утечки по каналам связи нужно принимать во внимание некоторые моменты:

- с помощью телефонных аппаратов возможно прослушивание и перехват разговоров, которые ведутся в защищаемом помещении;
- телефонные линии, которые распределены в защищаемом помещении, могут применяться в виде источников питания закладных устройств и для передачи перехваченной речевой информации;
- к телефонной линии возможно подключение индуктивных датчиков, осуществляющих перехват телефонных разговоров;
- телефонная линия может использоваться для неправомерного ведения телефонных разговоров.

Исходя из вышеизложенного, методы и средства защиты телефонных линий необходимо сконцентрировать на предотвращение:

- применения телефонных линий, для несанкционированного снятия информации (разговоров), которые ведутся в защищаемом помещении;
- прослушивания телефонных разговоров, которые осуществляются по текущим телефонным линиям;
- неправомерного пользования телефонных линий, для осуществления телефонных разговоров.

В телефонном аппарате присутствуют элементы (звонковая цепь, телефонный и микрофонный капсули), которые обладают «микрофонным эффектом», то есть они могут преобразовать акустический сигнал в электрический. За счет этого, на них образуются опасные информационные сигналы.

Подключение специализированных высокочувствительных низкочастотных усилителей к телефонной линии, даже если телефонный аппарат не производит звонки, может осуществить перехват информативных сигналов, которые возникают в звонковой цепи.

Даже при отключении микрофона от телефонной линии, сигнал навязывания поступает в микрофонную цепь, где моделируется информационным сигналом. В данном случае используется метод съема «высокочастотного навязывания».

Поэтому необходимо производить защиту всех элементов телефонного аппарата.

От утечки речевой информации, применяют пассивные и активные методы и средства. Они способны обеспечить защиту телефонного аппарата от утечки конфиденциальной информации по акустoeлектрическому каналу.

К наиболее широко применяемым пассивным методам защиты относятся:

- ограничение опасных сигналов;
- фильтрация опасных сигналов [11].

Ограничение опасных сигналов формируется на основе особенностей полупроводниковых элементов (диодов). Они обладают высоким сопротивлением, что предотвращает проникновение опасных сигналов в телефонную линию. Данные диоды, а точнее диодные ограничители, подключаются к линии звонка.

Фильтрация опасных сигналов осуществляет защиту телефонных аппаратов от «высокочастотного навязывания». Фильтр вносится в звонковую и микрофонную цепь телефонного аппарата. В основном для более устойчивой защиты телефонного аппарата применяют одновременно фильтр и ограничитель.

Активным методом защиты в данном случае является линейное зашумление телефонных линий. Зашумление защищает речевую информацию от утечки по электроакустическому каналу. В данном случае,

шумовой сигнал поступает в линию телефонного аппарата, когда не осуществляется разговор по телефонному аппарату. Шумовой сигнал прерывается только тогда, когда трубка телефонного аппарата снята.

В защищаемых помещениях, кроме защиты телефонных аппаратов, нужно защищать телефонные линии, так как в помещении могут быть установлены акустические закладки, которые могут питаться от телефонных линий, и могут производить передачу информации по телефонным линиям.

Для защиты телефонных линий применяют пассивные и активные методы и средства защиты. Пассивные методы защиты осуществляют блокирование акустических закладок, активные же методы в основном используют линейное зашумление линий и уничтожение закладных устройств.

Защита телефонных разговоров от перехвата информации по большей части реализуется активными методами. К основным из них относятся:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод «обнуления»);
- подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной

маскирующей помехи);

- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);

- подача в телефонную линию высоковольтных импульсов (метод «выжигания») [11].

При методе синфазной маскирующей низкочастотной (НЧ) помехи осуществляется подача маскирующих сигналов речевого диапазона в провода телефонных линий. Данные помехи не вызывают мешающего влияния на телефонный разговор, так как сигналы компенсируют друг друга. Но когда съем конфиденциальной информации производят с одного провода, то происходит влияние помехового сигнала на телефонный разговор. Если уровень помехи превышает полезный сигнал, то съем информации становится неосуществим. Для маскирующего помехового сигнала, применяют дискретные сигналы.

Метод синфазного маскирующего низкочастотного сигнала применяется для глушения телефонных радиозакладок и диктофонов, которые либо подключены контактно к линиям, либо подключены при помощи индукционных датчиков.

Метод высокочастотной маскирующей помехи, осуществляет в линию телефонного аппарата подачу широкополосного маскирующего сигнала типа «белого шума» или дискретного сигнала. Данная помеха осуществляется во время разговора по телефонному аппарату и глушит многие прослушивающие устройства. Частоты маскирующих сигналов выбираются так, чтобы уровень микрофона закладки или диктофона смог подавить речевой сигнал, но не повредить качество телефонного разговора. Эффективность помехового сигнала выше, если используется маленькая частота помехового сигнала, но при этом происходит высокое мешающее воздействие на разговор. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на

полезный сигнал. В основном применяются частоты в диапазоне от 6 до 20 кГц.

Метод ультразвуковой маскирующей помехи осуществляет в линию телефонного аппарата ультразвуковые помехи, принцип работы такой же что и у метода высокочастотной помехи. Только частоты ультразвукового сигнала используют в основном от 20 до 100 кГц.

Метод повышения напряжения, применяется ослабления функционирования радиозакладок. Он производится при помощи поднятия напряжения в телефонной линии до 24 В во время разговора. Такое напряжение производит ухудшение разборчивости речи, в связи с размытием спектра в радиозакладке. Некоторые телефонные закладки при подаче на них такого напряжения, отключаются.

Метод «обнуления» реализует введение в линию постоянного напряжения, которое не отличается от напряжения поднятой трубки, но с обратной полярностью. Данный метод производит ухудшение функционала прослушивающего устройства, которое подключается к линии и использует его питание.

Метод низкочастотной маскирующей помехи основан на наложении маскирующего сигнала речевого диапазона частот. Данный метод производит подавление проводных закладок, которые передают информацию, применяя телефонную линию. Так же нейтрализует запись диктофонов, с помощью сматывания пленки в режиме записи шума.

Компенсационный метод основывается на односторонней маскировке речевых сообщений, но к сожалению этот метод не применяется для двухсторонних телефонных разговоров. При передаче сообщения подается маскирующая помеха в телефонную линию, при помощи специализированного генератора. Эта же помеха подается на вход адаптивного фильтра, речевой сигнал подается на другой вход фильтра. Данный фильтр выделяет речевой сигнал и подавляет шумовой сигнал, после этого полезный сигнал поступает на телефонный аппарат.

Метод «выжигания» осуществляется с помощью подачи высоковольтных импульсов в линию телефона, при этом при такой подаче телефонный аппарат отключается от линии. Данный метод реализует электрическое «выжиганию» входных каскадов и блоков питания закладных устройств. При использовании текущего метода, в линию подается две подачи импульсов. В первом случае для подавления параллельно подключенных устройств, во втором случае для подавления последовательных подключенных устройств.

Защита телефонных линий может осуществляться как одним методом, так и несколькими (комплексная защита).

Кроме активной защиты, могут применяться устройства, которые контролируют параметры телефонных линий и обнаруживают несанкционированное подключение.

Использование метода контроля телефонных линий, проводится на основе специальных проверок. При применении данного метода обнаруживается факт подключения устройств перехвата, так как любое подключение производит изменение электрических параметров линий.

К примеру, некоторые контроллеры телефонных линий, способны за считанные минуты выявить закладные устройства, подключенные к линиям телефонного аппарата.

В настоящее время, разработаны контроллеры, которые не только обнаруживают факт несанкционированного подключения, но производят подавление подключаемых устройств. В данном контроллере в большинстве случаев используется метод высокочастотной маскирующей помехи. При выявлении несанкционированного подключения, в контроллере включается автоматическое подавление.

Для исключения неправомерного пользования телефонных линий, к которым производят подключение параллельных телефонных аппаратов, используют специализированные блокираторы. Данный блокиратор при помощи сравнения напряжения, осуществляет анализ телефонной линии.

Когда трубка несанкционированного подключенного телефонного аппарата снята, то в линии напряжение снижается. Если понижение напряжения зафиксировано, то срабатывает сигнализация и производится блокирование набора номера несанкционированного телефонного аппарата.

Данные устройства сигнализируют не только факт подключения к телефонным линиям, но и предупреждает о коротком замыкании или об обрыве телефонной линии.

В программно-аппаратном комплексе используется телефонный аппарат серии Нефрит-2-Г-ЦБ, с кнопочным номеронабирателем и центральной батареей. Он предназначен для работы в специальных стационарных сетях связи. Питание аппарата происходит от коммутационного оборудования или от центральной батареи автоматической телефонной станции. Аппарат имеет магнитную и электростатическую экранировки, а также имеет функцию контроля несанкционированного доступа к телефонному аппарату. Телефонный аппарат полностью защищен от несанкционированного снятия (перехвата) конфиденциальной информации. В нем используется контроллер, который обнаруживает факт несанкционированного подключения и производит автоматическое подавление подключаемых устройств (используется метод высокочастотной маскирующей помехи). Единственным нюансом, считается то, что во время разговора по телефонному аппарату, возможен перехват речевой информации, циркулирующей в защищаемом помещении. Поэтому для защиты от утечки конфиденциальной информации по акустическим каналам, во время разговора необходимо использовать генератор Соната-АВ.

Система защиты речевой информации от утечки по техническим каналам Соната-АВ, модель 4Б, представлена на рисунке 7.



Рисунок 7 - Система защиты речевой информации Соната-АВ, модель 4Б

Система активной защиты речевой информации «Соната-АВ» модель 4Б, осуществляет защиту от утечки речевой информации по акустическим, виброакустическим и акустоэлектрическим каналам, в защищаемых помещениях.

Состав изделия «Соната-АВ» модель 4Б:

- блок электропитания и управления: «Соната-ИП4.1», «Соната-ИП4.2»;
- генератор-акустоизлучатель: «СА-4Б», «СА-4Б1»;
- генератор-вибровозбудитель: «СВ-4Б», «СВ-4Б1»;
- размыкатель телефонной линии: «Соната-ВК4.1»;
- размыкатель слаботочной линии: «Соната-ВК4.2»;
- размыкатель линии Ethernet: «Соната-ВК4.3»;
- пульт управления: «Соната-ДУ4.1»;
- устройства сопряжения: «Соната-СК4.1», «Соната-СК4.2» [10].

Генераторы-акустоизлучатели «СА-4Б», «СА-4Б1» и генераторы-вибровозбудители «СВ-4Б», «СВ-4Б1» представляют собой электроакустические преобразователи со встроенными генераторами электрического шумового напряжения [10].

Данные генераторы реализуют систему защиты конфиденциальной информации от перехвата по акустическим и виброакустическим каналам.

7.2 Защита от утечки видовой информации

Защита от утечки видовой информации — это мероприятия, которые исключают или существенно затрудняют выход конфиденциальной информации за пределы КЗ, с помощью распространения световой энергии.

Для защиты конфиденциальной информации от утечки видовой информации рекомендуется:

- размещать элементы ПАК так, чтобы не допустить отражение света в стороны возможного местоположения злоумышленника;
- понизить отражательные свойства элементов ПАК;
- понизить освещенность элементов ПАК;
- пользоваться средствами преграждения или существенного ослабления отраженного света: шторы, темные стекла, экраны и т.п.;
- использовать средства маскирования для защиты и введения в заблуждение злоумышленника;
- применять средства пассивной и активной защиты источника от неуправляемого распространения отражательного или излученного света;
- реализовывать маскировку элементов ПАК, меняя отражательные свойства и контраст фона;
- использовать маскирующие средства сокрытия элементов, в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

8 Выбор и сравнение средств защиты программно-аппаратного комплекса от внедрения аппаратных закладок

8.1 Виды аппаратных закладок

Электронные устройства перехвата (закладные устройства) скрытно внедряемые в ПАК, осуществляют съём информации, обрабатываемой в ПАК. Закладные устройства образуют излучения, которые модулируются информационным сигналом. Данные устройства являются мини-передатчиками. Перехваченная защищаемая информации, с помощью закладных устройств, может передаваться по каналу связи или записываться на специальное запоминающее устройство и передаваться только по команде. Передача информации осуществляется на приёмный пункт, для передачи используются линии электропитания ПАК, радиоканал, оптический (инфракрасный) канал.

Закладные устройства, внедряемые в ПАК, по виду перехватываемой информации можно разделить на:

- аппаратные закладки для перехвата изображений, выводимых на экран монитора;
- аппаратные закладки для перехвата информации, вводимой с клавиатуры;
- аппаратные закладки для перехвата информации, выводимой на периферийные устройства (например, принтер);
- аппаратные закладки для перехвата информации, записываемой на жёсткий диск ПАК;
- аппаратные закладки для перехвата по телефонному каналу связи [12].

Аппаратные закладки для перехвата изображений, выводимых на экран монитора, скрытно устанавливаются в корпусе монитора или в системный блок ПАК. Данные закладки контактно подключаются к кабелю монитора

или к кабелю блока ПАК. В их состав входит блок перехвата, компрессия, передающий блок, блок управления и блок питания.

С помощью закладки для перехвата изображений, осуществляется перехват информации, которая представляет собой видеоизображение. Видеоизображение передается на приёмный пункт в цифровом виде по радиоканалу, линии электросети, выделенной линии. На приемном пункте перехваченное изображение восстанавливается, на экране компьютера перехваченное изображение отображается в реальном масштабе времени. Дополнительная информация записывается на жёсткий диск для дальнейшей обработки.

Например, аппаратная закладка RAGEMASTER позволяет перехватить сигнал от VGA монитора [13].

Данная закладка внедряется в VGA-кабель, которая соединяет видеокарту и монитор. Осуществляется захват соответствующего сигнала с цветового красного канала. Закладка включается от излучателя при облучении радиосигналом. Внешний вид данной закладки представлен на рисунке 8.



Рисунок 8 – Аппаратная закладка RAGEMASTER

Аппаратные закладки для перехвата информации, вводимой с клавиатуры компьютера в основном осуществляют перехват паролей пользователей и текстовых документов. Данные закладки считаются самыми распространёнными закладными устройствами. Они подключаются к интерфейсу клавиатуры, после их установки в корпусе клавиатуры или внутри системного блока. Перехватываемая защищаемая информация либо сразу передается по радиоканалу, либо записывается на flash-память.

Например, закладка SUFRLYSPAWN излучает радиосигнал, который несет информацию о каждой нажатой клавише. Данный радиосигнал может быть принят приемной станцией, которая находится вне здания [13].

Аппаратные закладки для перехвата информации, выводимой на принтер, совершают перехват текстовых документов. Данные закладки скрытно внедряются в корпус принтера. Перехватываемая информация передается на приёмный пункт по радиоканалу, линии электросети.

Аппаратные закладки для перехвата информации, записываемой на жёсткий диск компьютера, скрытно внедряются в системный блок компьютера и контактно подключаются через специальный блок перехвата к интерфейсу, соединяющему жёсткий диск с материнской платой. Данные закладки перехватывают сигналы, которые поступают в блок специальной обработки, где производится обработка сигнала по специальной программе. Происходит запись файлов в оперативную память или flash память. Записанная в памяти информация, передаётся на приёмный пункт в цифровом виде по сети или радиоканалу. Для дальнейшей обработки информация записывается на жёсткий диск в виде отдельных файлов.

Аппаратные закладки для перехвата по телефонному каналу связи, внедряются параллельно или через индукционный датчик в телефонную трубку или в разрыв телефонного провода. Перехваченная защищаемая информация передается либо по радиоканалу, либо записывается на цифровые диктофоны. В настоящее время некоторые телефонные закладки включаются автоматически при снятии телефонной трубки и сразу же осуществляют передачу разговора по радиоканалу на приемный пункт перехвата. Данные закладки применяются в виде микрофона телефонного аппарата, которые не имеют своего источника питания.

Например, телефонная радиозакладка, выполненная в виде конденсатора модели РК-130. Пример закладки представлен на рисунке 9.



Рисунок 9 – Телефонная закладка РК-130

8.2 Выбор и сравнение средств защиты ПАК от внедрения аппаратных закладок

Средствами защиты программно-аппаратного комплекса от внедрения аппаратных закладок является выявление закладных устройств и их уничтожение.

Выявление портативных электронных устройств перехвата информации (закладных устройств) осуществляется проведением специальных обследований, а также специальных проверок объекта ПАК [14].

Специальное обследование осуществляется с помощью визуального осмотра ПАК, без использования каких либо технических средств. Поиск закладных устройств осуществляется по демаскирующим признакам их внешнего вида.

Специальная техническая проверка ПАК проводится с использованием специальных технических средств. Осуществляется специальная проверка ПАК и вспомогательных технических средств, с применением рентгеновских комплексов. Так же производится организация радиоконтроля и побочных электромагнитных излучений ПАК.

Перед осмотром ПАК включается, с использованием индикатора поля выявляется наличие в них источников радиоизлучения, после этого они обесточиваются и разбираются.

Визуальный осмотр блоков и плат ПАК осуществляется с помощью лупы.

Подозрительные и странные неразборные блоки, платы и элементы схем ПАК проверяются с помощью рентгеновских комплексов.

Если присутствуют снимки типовых блоков и печатных плат аналогичных ПАК, то производится их сравнение с наблюдаемыми.

Главными демаскирующими признаками аппаратных закладок, внедренных в ПАК, являются:

- признаки внешнего вида - присутствие блоков или устройств непонятного назначения, подключенных к информационным кабелям или платам блоков ПАК; наличие дополнительных плат или появление в блоках дополнительных радиоэлементов; присутствие на платах следы свежей пайки; странные различия элементов от заводских;
- присутствие в контролируемом ПАК, сравнительно большой мощности радиоизлучения;
- корреляционные изменения спектра радиосигнала с преобразованием режимов работы ПАК;
- отличие рентгеновских снимков (изображений) блоков или печатных плат от типовых, наличие дополнительных непонятных элементов (микросхем, диодов, резисторов.), а так же их расположения не соответствует типовому расположению, наличие дополнительных проводников, соединений и т.д.

Для исключения закладных устройств в ПАК необходимо заказывать технические средства у проверенных поставщиков. А так же при возникновении неполадок в технических средствах отправлять их в ремонтные работы к проверенным работодателям. Обязательным действием после ремонта является проверка технических средств на закладные устройства.

Данные обследования и проверки помогут выявить закладные устройства в программно-аппаратном комплексе, что обеспечит защиту от несанкционированного съема конфиденциальной информации.

9 Обоснование и выбор систем, препятствующих несанкционированному доступу к конфиденциальной информации

9.1 Описание СЗИ от НСД Secret Net Studio

Средства защиты информации от несанкционированного доступа (СЗИ от НСД) - программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации [15].

Secret Net Studio является сертифицированным средством защиты информации от несанкционированного доступа для операционных систем (ОС) семейства Microsoft Windows [16].

Основные функции СЗИ от НСД Secret Net Studio:

- контроль входа пользователей в систему (идентификация и аутентификация пользователей);
- дискреционное разграничение доступа к файловым ресурсам, устройствам, принтерам;
- мандатное (полномочное) разграничение доступа к файловым ресурсам, устройствам, принтерам, сетевым интерфейсам, включая:
 - контроль потоков конфиденциальной информации в системе;
 - контроль вывода информации на съемные носители;
- контроль состояния устройств компьютера с возможностями:
 - блокирования компьютера при изменении состояния заданных устройств;
 - блокирования подключения запрещенного устройства (устройства из запрещенной группы);
- теневое копирование информации, выводимой на внешние носители и на печать;
- автоматическая маркировка документов, выводимых на печать;
- контроль целостности файловых объектов и реестра;

- создание замкнутой программной среды для пользователей;
- очистка оперативной и внешней памяти при ее перераспределении;
- изоляция процессов (выполняемых программ) в оперативной памяти;
- защита содержимого локальных жестких дисков при несанкционированной загрузке операционной системы;
- антивирусная защита компьютеров;
- обнаружение вторжений;
- межсетевое экранирование сетевого трафика;
- авторизация сетевых соединений;
- функциональный контроль ключевых защитных подсистем;
- регистрация событий безопасности;
- централизованное и локальное управление параметрами работы механизмов защиты;
- централизованное и локальное управление параметрами работы пользователей;
- мониторинг и оперативное управление защищаемыми компьютерами;
- централизованный сбор, хранение и архивирование журналов [16].

Вход в систему предусматривает ввод имени и пароля пользователя или использование персональных идентификаторов (eToken, Rutoken, JaCarta, ESMART или iButton). Так же предусмотрены режимы усиленной аутентификации. Для пользователей устанавливаются ограничения на количество неудачных попыток входа в систему. Если пользователь определенное количество раз предъявляет неверную ключевую информацию или пароль, то система блокирует компьютер. Так же система блокируется при изъятии идентификатора.

Для предотвращения несанкционированного вывода конфиденциальных документов на локальные и сетевые принтеры используется механизм контроля печати.

Механизм защиты информации на локальных дисках компьютера (механизм защиты дисков) предназначен для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера. Загрузка считается санкционированной, если она выполнена средствами операционной системы (ОС) с установленным клиентским программным обеспечением (ПО) Secret Net. Все другие способы загрузки ОС считаются несанкционированными (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере). Механизм обеспечивает защиту информации при попытках доступа, осуществляемых с помощью штатных средств операционной системы. Действие механизма защиты дисков основано на модификации загрузочных секторов (boot-секторов) логических разделов на жестких дисках компьютера.

Разграничение доступа пользователей к файлам, каталогам, и файлам на локальных дисках осуществляется с помощью дискреционного управления.

Разграничение доступа пользователей к устройствам, выполняется на основании списков устройств, которые формируются механизмом контроля подключения и изменения устройств.

Механизм замкнутой программной среды позволяет определить для любого пользователя компьютера индивидуальный перечень программного обеспечения, разрешенного для использования.

Система Secret Net Studio предоставляет возможность шифрования содержимого объектов файловой системы (файлов и папок). Для операций зашифрования и расшифрования используются специальные хранилища — криптографические контейнеры или криптоконтейнеры. Физически криптоконтейнер представляет собой файл, который можно подключить к системе в качестве дополнительного диска. Криптоконтейнер является

образом диска, но все действия с ним выполняются через драйвер механизма шифрования. Драйвер обеспечивает работу с пользовательскими данными в контейнере в режиме «прозрачного шифрования». То есть пользователь, после подключения криптоконтейнера в качестве диска, выполняет операции с файлами на этом диске так же, как и на любом другом носителе.

Система Secret Net Studio обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации. Используется подсистема межсетевого экранирования.

При действующем механизме авторизации сетевых соединений осуществляется добавление специальной служебной информации к сетевым пакетам, с помощью которой обеспечивается аутентичность и целостность передаваемых данных и защита от атак типа Man in the Middle.

Secret Net Studio реализует обнаружение и блокирование внешних и внутренних вторжений, направленных на защищаемый компьютер.

Secret Net Studio позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. При проверке компьютера осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др. Это позволяет обнаружить и заблокировать внешние и внутренние сетевые атаки, направленные на защищаемый компьютер.

В состав клиентского ПО системы Secret Net Studio включен VPN клиент, предназначенный для организации доступа удаленных пользователей к ресурсам. VPN клиент обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи.

9.2 Описание СЗИ от НСД Страж NT (версия 4.0)

Страж NT (версия 4.0) представляет собой программный комплекс средств защиты информации с использованием аппаратных идентификаторов. СЗИ от НСД Страж NT (версия 4.0) предназначена для

комплексной защиты информационных ресурсов от несанкционированного доступа [17].

СЗИ от НСД Страж NT (версия 4.0) может применяться при разработке систем защиты информации для одно- и многопользовательских автоматизированных систем под управлением операционных систем Windows 7 и выше [17].

В СЗИ «Страж NT» реализованы следующие ключевые функции:

- идентификация и аутентификация пользователей до загрузки операционной системы при предъявлении персонального идентификатора и пароля;
- идентификация и аутентификация при смене пользователей без перезагрузки операционной системы;
- терминальная идентификация пользователей при подключении к терминальному серверу;
- блокировка компьютера при изъятии персонального идентификатора пользователя;
- ограничение неуспешных попыток входа в систему;
- сокрытие логической структуры жесткого диска в целях доверенной загрузки операционной системы;
- управление учетными записями пользователей и персональными идентификаторами;
- реализация дискреционного принципа контроля доступа к защищаемым ресурсам, таким как носители информации, папки, файлы, принтеры, устройства;
- реализация мандатного принципа контроля доступа к защищаемым ресурсам, таким как носители информации, папки, файлы, принтеры;
- контроль потоков информации, в том числе и именованных каналов;

- настройка замкнутой программной среды для пользователей, в том числе и в автоматических режимах;
- контроль запуска DOS-приложений в 32 - разрядных ОС;
- учет и контроль носителей информации;
- преобразование информации на флэш-накопителях;
- контроль подключаемых устройств;
- регистрация всех действий пользователей и администраторов системы защиты;
- маркировка и регистрация документов, выдаваемых на печать;
- работа с журналами событий, их фильтрация и поиск;
- архивирование журналов (в том числе и по расписанию);
- контроль целостности защищаемых файлов и модулей системы защиты;
- очистка файлов при их удалении;
- очистка файлов подкачки страниц при завершении работы;
- восстановление работоспособности системы защиты в случае сбоя;
- ведение резервных копий модулей системы защиты;
- тестирование механизмов системы защиты;
- формирование отчетов по настройкам системы защиты;
- управление сценариями настроек системы защиты;
- архивирование (в том числе и по расписанию) и восстановление настроек защищаемых ресурсов;
- экспорт настроек СЗИ на удаленные компьютеры;
- развертывание системы защиты на удаленных компьютерах;
- настройку подсистем и механизмов системы защиты на удаленных компьютерах [17].

В качестве персональных идентификаторов в СЗИ «Страж NT» могут применяться стандартная 3,5” дискета, устройства iButton, USB – ключи eToken Pro, eToken Pro Java, Guardant ID, Rutoken S, eSmart, смарт-карты,

USB-флэш-накопители. Неправильные идентификаторы отвергаются системой. При предъявлении правильного идентификатора, на экран выводится запрос на ввод пароля, после трех неуспешных попыток, компьютер блокируется.

Дискреционный принцип контроля доступа пользователей к защищаемым объектам осуществляется на основе списков управления доступом. К защищаемым объектам в системе защиты относятся носители информации, папки, файлы, устройства, принтеры и т.д.

Система защиты информации позволяет на каждый защищаемый ресурс устанавливать атрибуты защиты, к которым относятся список контроля доступа и идентификатор безопасности владельца ресурса.

Мандатный принцип контроля доступа реализован посредством назначения защищаемым ресурсам, каждому пользователю системы и прикладным программам меток конфиденциальности и сравнения их при запросах на доступ.

Загрузка посторонней операционной системы типа MS-DOS с дискеты или CD-ROM диска при установке данного СЗИ становится невозможной. При попытке прочитать содержимое диска при его подключении к другому компьютеру логическая структура диска будет не доступна.

Подсистема контроля устройств компьютера позволяет устанавливать разрешения на различные типы устройств. При попытке подключить устройство, запрещенное данному пользователю, подсистема контроля устройств отключит данное устройство.

Для защиты ввода вывода на отчуждаемый носитель в СЗИ «Страж NT» предусмотрены подсистемы учета носителей и преобразования информации на отчуждаемых носителях.

9.3 Выбор и обоснование СЗИ от НСД

Для определения выбора надежного СЗИ от НСД, необходимо рассматривать главные механизмы защиты, обеспечивающие защиту конфиденциальной информации.

СЗИ от НСД Страж NT (версия 4.0) является надежным и удобным в использовании механизмом защиты информации. Достоинством данного СЗИ является четыре типа идентификации пользователей, через которые проходит пользователь при входе в систему. При аутентификации пользователь может пользоваться устройствами идентификации разных типов и паролем с именем. При несоответствии идентификатора компьютер блокируется. Так же плюсом является реализованный в СЗИ дискреционный принцип доступа и мандатный принцип контроля доступа. Используется подсистема запуска программ, которая предназначена для обеспечения целостности и замкнутости программной среды и реализована путем разрешения для исполняемых файлов режима запуска. В данной СЗИ предусмотрена возможность тестирования системы защиты, что является важным для поддержания системы защиты.

СЗИ от НСД Secret Net Studio является удобным и самым устойчивым СЗИ от несанкционированного доступа. В нем используются механизмы защиты, обеспечивающие защиту от многих воздействий, а именно:

- защиту от несанкционированного доступа к информационным ресурсам компьютеров;
- контроль устройств, подключаемых к компьютерам;
- обнаружение вторжений в информационную систему;
- антивирусную защиту;
- межсетевое экранирование сетевого трафика;
- авторизацию сетевых соединений.

Аутентификация пользователя при входе в систему может осуществляться с помощью разных аппаратных идентификаторов и паролем

с именем. При не соответствии идентификатора компьютер блокируется. В данной системе реализовано дискреционное управление доступа к ресурсам файловой системы, устройствам, принтерам и мандатное разграничение доступа. Присутствует механизм защиты информации на локальных дисках компьютера (механизм защиты дисков) предназначенный для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера. Используется механизм замкнутой программной среды, которая позволяет определить для любого пользователя компьютера индивидуальный перечень программного обеспечения, разрешенного для использования. В данном СЗИ так же осуществляется контроль печати, обеспечивая разграничение доступа пользователей к принтерам. Так же предоставляется возможность шифрования содержимого объектов файловой системы. Система обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации. Secret Net Studio реализует обнаружение и блокирование внешних и внутренних вторжений, направленных на защищаемый компьютер. Система позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. В состав системы включен VPN клиент, предназначенный для организации доступа удаленных пользователей к ресурсам. VPN клиент обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи.

Сравнивая СЗИ Страж (4.0) и СЗИ от НСД Secret Net Studio можно с уверенностью определиться с выбором системы защиты от НСД. Secret Net Studio, является более укомплектованной и надежной, в данной системе используются механизмы защиты, обеспечивающие защиту от многих воздействий на систему ПАК.

9.4 Описание выбора АПКШ «Континент»

АПКШ «Континент» 3.7 предназначен для построения виртуальных частных сетей (VPN) на основе общих сетей передачи данных, использующих протоколы семейства TCP/IP.

Комплекс обеспечивает криптографическую защиту информации, передаваемой по открытым каналам связи, между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры [16].

Комплекс реализует следующие основные функции:

- криптографическая защита данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN;
- межсетевое экранирование;
- скрывание внутренней структуры локальных вычислительных сетей;
- автоматическая регистрация событий, связанных с функционированием комплекса, в том числе событий НСД;
- централизованное управление компонентами комплекса [16].

Актуальная на сегодняшний день ключевая схема, выполняет шифрование каждого пакета на уникальном ключе, создает гарантированную защиту от вероятности дешифрации перехваченных данных.

АПКШ «Континент» 3.7 осуществляет фильтрацию принимаемых и передаваемых пакетов, для защиты от проникновения со стороны сетей общего пользования.

Алгоритм шифрования комплекса ГОСТ 28147-89 режим гаммирования с обратной связью, длина ключа 256 бит. Защита передаваемых данных от искажения осуществляется по ГОСТ 28147-89 режим выработки имитовставки. Фильтрация IP-пакетов производится в соответствии с задаваемыми правилами фильтрации.

Для обеспечения криптографической защиты конфиденциальной информации передаваемой по сети, была выбрана модель АПКШ «Континент» IPC-100.

Данная модель имеет небольшой размер и поддерживает сетевые интерфейсы:

- 6x 1000BASE-T Ethernet 10/100/1000 RJ45;
- 2x 1000BASE-X оптический Gigabit Ethernet SFP.

Скорость передачи данных криптошлюза до 300 Мбит/с, межсетевого экрана до 400 Мбит/с, криптокоммутатора до 300 Мбит/с, детектора атак до 260 Мбит/с.

АПКШ «Континент» модели IPC-100, представлена на рисунке 10.



Рисунок 10 - АПКШ «Континент» IPC-100.

Данный АПКШ «Континент» IPC-100 обеспечит соответствующую защиту конфиденциальных данных, передаваемых по каналам связи.

10 Разработка организационно-технических мероприятий по защите информации

Важным требованием по защите информации, является проведение организационных и технических мероприятий.

Организационно-технические мероприятия - совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации [18].

Организационные мероприятия - это мероприятия по защите информации, которые производят регламент производственной деятельности, исключающей или существенно затрудняющей несанкционированное снятие конфиденциальной информацией.

К основным организационным мероприятиям по защите информации относятся:

- определение должностного лица, ответственного за обеспечение безопасности конфиденциальной информации;
- разработка документов, регламентирующих обработку конфиденциальных данных;
- определение и установление границ контролируемых зон;
- проведение аттестации защищаемого помещения по требованиям безопасности информации и оформление аттестата соответствия;
- приобретение сертифицированных средств защиты информации, организация контроля их эффективности;
- проведение обучения, повышения осведомленности работников, осуществляющих обработку конфиденциальной информации;
- организация обучения лиц, использующих средства защиты информации, правилам работы с ними;
- контроль и учет применяемых средств защиты информации, а также эксплуатационной и технической документации к ним, носителей конфиденциальных данных;

- установление правил доступа к конфиденциальной информации;
- организация процедуры регистрации и учета всех действий, совершаемых с конфиденциальной информацией в ПАК;
- организация учета лиц, допущенных к работе с конфиденциальной информацией при работе в ПАК;
- организация процедуры периодического внутреннего контроля и (или) аудита соответствия обработки информации требованиям законодательных и нормативных актов;
- формирование архивного хранения конфиденциальных документов;
- выявление технических устройств и программ, представляющих возможность несанкционированно снять конфиденциальную информацию.

Технические мероприятия - это мероприятия по защите информации, осуществляющие выполнение технических решений, включающее использование специальных технических средств.

К техническим мероприятиям по защите информации с использованием пассивных средств относятся:

- контроль и ограничение доступа к программно-аппаратному комплексу во время проведения работ, связанных с обработкой и передачей информацией, осуществляется с помощью установки технических средств и систем ограничения и контроля доступа;
- звукоизоляция ЗП;
- размещение в цепях электропитания ПАК, а также в линиях осветительной и розеточной сетей ЗП помехоподавляющих фильтров.

К техническим мероприятиям по защите информации с использованием активных средств относятся:

- пространственное и линейное электромагнитное зашумление с использованием генератора шума;

- формирование акустических и вибрационных помех с использованием генератора акустического шума;
- подавление диктофонов и акустических закладок в режиме записи с использованием блокиратора;
- подавление беспроводной связи;
- использование средств защиты информации от несанкционированного доступа;
- использование криптографической защиты.

Перечисленные организационные и технические мероприятия по защите информации, считаются довольно действенными и не несут серьезных проблем с персоналом. Применение данных мероприятий обеспечат защиту конфиденциальной информации обрабатываемой в программно-аппаратном комплексе.

11 Разработка структуры программно-аппаратного комплекса, защищенного от несанкционированного съема информации

Для разработки структуры программно-аппаратного комплекса, защищенного от несанкционированного съема, в п.1 был определен выбор основных комплектующих для ПАК, и разработана структура ПАК обработки и передачи конфиденциальной информации. Программно-аппаратный комплекс обработки и передачи конфиденциальной информации соответствует предъявленным техническим требованиям, и в его состав входят:

- телефонный аппарат Нефрит 2-Г-ЦБ, работающий в стационарных сетях связи, с функцией контроля несанкционированного доступа;
- многофункциональное устройство HP LaserJet Pro M176n с цветной лазерной технологией печати и разрешением сканирования 1200x1200 dpi, без модуля Wi-Fi;
- папо IP-АТС АГАТ модели UX-5110, осуществляет управление звонков, проходящих через интернет-каналы, передачу голосового трафика и данных по протоколам IP-телефонии.

Для защиты программно-аппаратного комплекса обработки и передачи конфиденциальной информации от несанкционированного съема информации, определены средства защиты представленные ниже.

Блокиратор «Завеса-Аудио», осуществляет подавления диктофонов и акустических закладок в помещении. Его необходимо включить в состав, так как в ПАК входит телефонный аппарат, при разговоре оператора речевая конфиденциальная информация может записываться на устройства. Работа блокиратора основана на излучении мощных неслышимых человеческим ухом ультразвуковых колебаний, приводящих к существенным искажениям записываемых (передаваемых) сигналов. Блокиратор «Завеса-Аудио» эффективно подавляет проводные микрофоны, радиомикрофоны,

диктофоны (включая профессиональные) цифровые и пленочные, диктофоны в мобильных телефонах и смартфонах.

Блокиратор беспроводной связи ЛГШ-719, производит блокировку работ устройств несанкционированного получения информации, работающих в стандартах сотовой связи.

Встраиваемый в системный слот компьютера генератор шума ГШ-К-180. Реализует защиту ПЭМИН программно-аппаратного комплекса, размещенного в помещении площадью приблизительно от 40 до 50 м². Данный генератор шума создает и излучает в окружающее пространство электромагнитное поле шума, а так же наводит маскирующий сигнал в отходящие цепи и инженерные коммуникации

Помехоподавляющий фильтр Фаза-1-10. За счет подавления наводок опасных (информативных) сигналов, данный фильтр предотвращает утечку информации с программно-аппаратного комплекса обработки и передачи конфиденциальной информации по линиям питающей сети, выходящими за пределы защищаемого помещения или за границы контролируемой зоны.

Система защиты речевой информации от утечки по техническим каналам Соната-АВ, модель 4Б. Необходима для исключения перехвата речевой конфиденциальной информации во время разговора по телефонному аппарату. Соната-АВ модель 4Б, защищает речевую информацию в выделенных помещениях, от утечки по акустическим, виброакустическим и акустоэлектрическим каналам.

СЗИ от НСД Secret Net Studio является удобным и самым устойчивым СЗИ от несанкционированного доступа. В нем используются механизмы защиты, обеспечивающие защиту от многих воздействий, а именно:

- защиту от несанкционированного доступа к информационным ресурсам компьютеров;
- контроль устройств, подключаемых к компьютерам;
- обнаружение вторжений в информационную систему;
- антивирусную защиту;

- межсетевое экранирование сетевого трафика;
- авторизацию сетевых соединений.

Аутентификация пользователя при входе с систему может осуществляться с помощью разных аппаратных идентификаторов и паролем с именем. При не соответствии идентификатора компьютер блокируется. В данной системе реализовано дискреционное управление доступа к ресурсам файловой системы, устройствам, принтерам и мандатное разграничение доступа. Присутствует механизм защиты информации на локальных дисках компьютера (механизм защиты дисков) предназначенный для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера. Используется механизм замкнутой программной среды, которая позволяет определить для любого пользователя компьютера индивидуальный перечень программного обеспечения, разрешенного для использования. В данном СЗИ так же осуществляется контроль печати, обеспечивая разграничение доступа пользователей к принтерам. Так же предоставляется возможность шифрования содержимого объектов файловой системы. Система обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации. Secret Net Studio реализует обнаружение и блокирование внешних и внутренних вторжений, направленных на защищаемый компьютер. Система позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. В состав системы включен VPN клиент, предназначенный для организации доступа удаленных пользователей к ресурсам. VPN клиент обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи.

АПКШ «Континент» IPC-100 обеспечит криптографическую защиту конфиденциальной информации, передаваемой по открытым каналам связи. Актуальная на сегодняшний день ключевая схема, выполняет шифрование каждого пакета на уникальном ключе, создает гарантированную защиту от вероятности дешифрации перехваченных данных.

Средствами защиты программно-аппаратного комплекса от внедрения аппаратных закладок является выявление портативных электронных устройств перехвата информации при помощи проведения специальных обследований, а также специальных проверок объекта ПАК.

Организационные и технические мероприятия по защите информации, обеспечивают дополнительную защиту конфиденциальной информации обрабатываемой в программно-аппаратном комплексе.

Все представленные средства защиты от несанкционированного съема информации, необходимо включить в ПАК обработки и передачи конфиденциальной информации.

Средства защиты, применяя к программно-аппаратному комплексу, предотвратят несанкционированный съем конфиденциальной информации. Структура программно-аппаратного комплекса обработки и передачи конфиденциальной информации, защищенного от несанкционированного съема, представлена на рисунке 11.

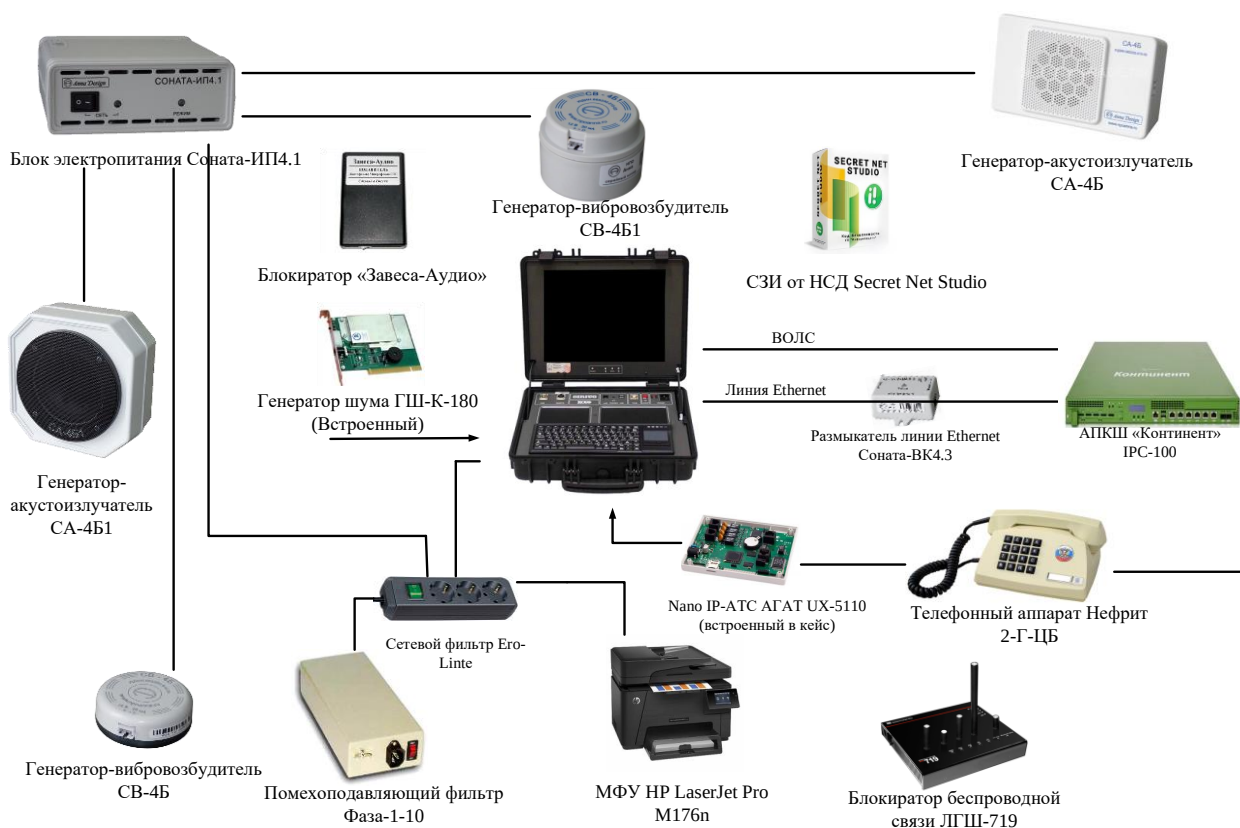


Рисунок 11 - Структура программно-аппаратного комплекса, защищенного от несанкционированного съема

12 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Специалист по защите информации подвергается воздействию опасностей и в своей трудовой деятельности. Трудовая деятельность реализуется в пространстве, которая называется производственная среда. Работа за компьютером – это интеллектуальный труд. Поэтому основная часть нагрузки перепадает на нервную систему, а именно на сердечно-сосудистую систему.

Опасные и вредные производственные факторы, обладающие свойствами психофизиологического воздействия на сердечно-сосудистую систему, подразделяют на два вида. А именно на:

- физические перегрузки, связанные с тяжестью трудового процесса;
- нервно-психические перегрузки, связанные с напряженностью трудового процесса [19].

Физические перегрузки - характеристика трудового процесса, отражающая преимущественную нагрузку на функциональные системы организма, особенно на сердечно-сосудистую систему.

Перегрузка характеризуется физической динамической нагрузкой, формой рабочей позы, степенью наклона корпуса.

Нервно-психические перегрузки - характеристика трудового процесса, отражающая нагрузку преимущественно на центральную нервную систему, эмоциональную сферу работника.

К факторам, характеризующим нервно-психические перегрузки, относятся: умственное перенапряжение, интеллектуальные, сенсорные, эмоциональные нагрузки, степень монотонности нагрузок, режим работы [20].

Действие всех выше факторов приводит к заболеваниям сердечно-

сосудистой системы. Особо негативным фактором, является излучение компьютера.

Электромагнитные поля негативно влияют на центральную нервную систему, вызывая головные боли, головокружения, тошноту, депрессию, бессонницу, отсутствие аппетита, возникновение синдрома стресса. Низкочастотное электромагнитное поле может явиться причиной болезней сердечно-сосудистой системы. Нарушения здоровья и заболевания пользователей компьютера являются, как правило, результатом воздействия не какого-либо отдельного фактора, а всего комплекса [20].

Для того чтобы снизить воздействие психофизиологических факторов, влияющих на сердечно-сосудистую систему организма, необходимо систематическое занятие физкультурой. Если здоровый человек ведет «сидячий» образ жизни и не занимается физкультурой, то при небольших физических нагрузках появляется сердцебиение и учащается дыхание. Иначе, если человек тренированный, то легко справляется с физическими нагрузками.

Сила и работоспособность сердечной мышцы, главного двигателя кровообращения, находится в прямой зависимости от силы и развития всей мускулатуры. Поэтому физическая тренировка, развивая мускулатуру тела, в то же время укрепляет сердечную мышцу. У людей с неразвитой мускулатурой мышца сердца слабая, что выявляется при любой физической работе [21].

Необходимо уделять время ежедневной утренней гимнастики, которая улучшит сердечно-сосудистую систему. Физические упражнения рекомендовано выполнять на свежем воздухе, если нет такой возможности, то в хорошо проветренном помещении. Хорошей идеей, для восстановления сердечно-сосудистой системы, считается вечерняя прогулка после работы. Прогулка на свежем воздухе улучшает самочувствие и повышает работоспособность. Таким образом, ежедневная прогулка на свежем воздухе от 1 до 1,5 часа считается важным элементом здорового образа жизни

человека. Прогулка на свежем воздухе снимает напряжение трудового дня, успокаивает возбужденные нервные центры, восстанавливает сердечно-сосудистую систему.

Заключение

В ходе дипломного проектирования были рассмотрены технические каналы утечки информации, проанализированы источники угроз программно-аппаратного комплекса, выявлены существующие методы защиты информации в помещении. Определены средства защиты программно-аппаратного комплекса обработки и передачи конфиденциальной информации, от несанкционированного съема. А так же разработаны организационно-технические мероприятия, которые создадут дополнительную защиту программно-аппаратного комплекса, от несанкционированного съема конфиденциальной информации.

Средствами защиты для программно-аппаратного комплекса являются:

- блокиратор подавления диктофонов и акустических закладок «Завеса-Аудио»;
- блокиратор беспроводной связи ЛГШ-719;
- генератор шума ГШ-К-180, обеспечивающий защиту от ПЭМИН;
- помехоподавляющий фильтр Фаза-1-10;
- система защиты речевой информации от утечки по техническим каналам Соната-АВ, модель 4Б;
- СЗИ от НСД Secret Net Studio;
- АПКШ «Континент» IPC-100;
- выявление закладных устройств;
- организационно-технические мероприятия.

Данные представленные средства защиты от несанкционированного съема информации, обеспечат защиту программно-аппаратного комплекса обработки и передачи конфиденциальной информации.

Результатом дипломного проектирования является разработанная структура программно-аппаратного комплекса, защищенного от несанкционированного съема информации.

По результатам дипломного проектирования была написана статья на тему: «Предотвращение утечки конфиденциальной информации, циркулирующей в программно-аппаратном комплексе обработки и передачи конфиденциальной информации», которая опубликована в сборнике материалов международной научно-практической конференции «Особенности современного этапа развития естественных и технических наук», состоявшаяся 28 декабря 2017 г. в г. Белгороде и проводимая Агентством перспективных научных исследований [22, с. 164]. Сборник также размещен в электронной библиотеке и включен в Российский индекс научного цитирования (РИНЦ).

Цель дипломного проектирования достигнута. Дипломный проект соответствует требованиям технического задания. Таким образом, дипломный проект выполнен в полном объеме.

Список используемых источников

1. Свободная энциклопедия [Электронный ресурс]: программно-аппаратный комплекс. Режим доступа: https://ru.wikipedia.org/wiki/Программно-аппаратный_комплекс (дата обращения: 18.10.2017).
2. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.
3. Р 50.1.056-2005 Техническая защита информации. [Электронный ресурс]: основные термины и определения. Режим доступа: http://www.infosait.ru/norma_doc/47/47735/index.htm (дата обращения: 20.10.2017).
4. Артамонов В.А., Артамонова Е.В. Каналы утечки информации (Аналитический обзор) [Электронный ресурс]: каналы утечки информации. Режим доступа: <http://knigi.konflib.ru/8tehnicheskie/149092-1-udk-6813-artamonov-artamonova-kanali-utechki-informacii-analiticheskiy-obzor-pod-tehnicheskim-kanalom-utechki-i.php> (дата обращения: 27.10.2017).
5. Источники угроз защищаемой информации [Электронный ресурс]: угрозы информационной безопасности. Научная статья. Режим доступа: <https://www.scienceforum.ru/2015/1215/11851> (дата обращения: 29.10.2017).
6. Хорев А.А. Способы и средства защиты информации. Часть 1. Методы и средства защиты информации от утечки по техническим каналам. Учебное пособие. МО РФ.2000. - 234 с.
7. Каторин Ю. Ф., Куренков Е.В. Большая энциклопедия промышленного шпионажа «Издательство Полигон», 2000. - 896 с.
8. ZavesaAudio [Электронный ресурс]: блокираторы диктофонов и микрофонов «Завеса-Аудио». Режим доступа:

<http://zavesaaudio.ru/Catalog/audio-zavesa/blokirator-zavesa-audio/> (дата обращения: 8.11.2017).

9. Лаборатория ППШ. [Электронный ресурс]: противодействие промышленному шпионажу. Режим доступа: <http://www.pps.ru/?part=catalog&product=241> (дата обращения: 27.11.2017).

10. ООО «Центр безопасности информации» [Электронный ресурс]: средства защиты информации от утечки по техническим каналам. Режим доступа: <http://www.cbi-info.ru/groups/page-72.htm> (дата обращения: 27.11.2017).

11. Хорев А.А. Методы и средства защиты телефонных аппаратов и телефонных линий. Научно-технический журнал «Специальная техника» 1998-2017 - 11с.

12. Хорев А.А. Классификация электронных устройств перехвата информации [Электронный ресурс]: Научно-технический журнал «Спецтехника и связь». Режим доступ: <http://www.bnti.ru/showart.asp?aid=907&lvl=04.01>. (дата обращения: 28.11.2017).

13. Клянчин А.И. Каталог закладок АНБ (Spiegel). Часть 2. Рабочее место оператора. Журнал: вопросы кибербезопасности. Выпуск № 3. 2014 - 8с.

14. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 3. Методы поиска электронных устройств перехвата информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.

15. Руководящий документ [Электронный ресурс]: защита от несанкционированного доступа к информации. Термины и определения, Гостехкомиссия России от 30 марта 1992. Режим доступа: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-30-marta-1992-g3> (дата обращения: 11.12.2017).

16. «Код безопасности» [Электронный ресурс]: продукция средств защиты информации от несанкционированного доступа. Режим доступа: <https://www.securitycode.ru/products/> (дата обращения: 11.12.2017).

17. Рубинтех технологии информационной безопасности [Электронный ресурс]: продукция «Страж NT». Режим доступа: http://www.guardnt.ru/gnt_40.html (дата обращения: 19.12.2017).

18. Аверченков. В.И., Рытов. М.Ю. Методы и средства инженерно-технической защиты информации. Глава 6. Методы и средства противодействия способам НСД к информации. Учебное пособие 2-е издание, стереотипное Москва - Издательство «ФЛИНТА» - 2011.

19. ГОСТ 12.0.003-2015 [Электронный ресурс]: система стандартов по безопасности труда. Опасные и вредные производственные факторы. Классификация. М.: Стандартиформ, 2016. Режим доступа: <http://www.internet-law.ru/gosts/gost/62075/> (дата обращения: 21.12.2017).

20. Гора Е.П. Экология человека. Глава 4. Социальная адаптация. Учебное пособие для вузов. М.: Дрофа, 2007. - 540 с.

21. Лекции по физической культуре [Электронный ресурс]: физические тренировки. Режим доступа: <http://mirznanii.com/a/222795/lektsii-po-fizkulture-ogu> (дата обращения: 21.12.2017).

22. Особенности современного этапа развития естественных и технических наук: сборник научных трудов по материалам Международной научно-практической конференции 28 декабря 2017 г.: в 2 ч./ Под общ. ред. Е. П. Ткачевой. – Белгород: ООО Агентство перспективных научных исследований (АПНИ), 2018. – Часть II. – 220 с.

Приложение А
(обязательное)

Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ»