

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

ЗАКРЫТЫЙ ИНФОРМАЦИОННЫЙ КОНТУР, ОБЕСПЕЧИВАЮЩИЙ
СБОР, ХРАНЕНИЕ, ОБРАБОТКУ, ОБМЕН И ПРЕДОСТАВЛЕНИЕ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Студент



Тихомиров Павел Александрович

Руководитель инженер 3-й категории

АО «НПП «Рубин»



Яшин Е.В.

Нормоконтролёр



Иванов А.П.

Рецензент инженер 3-й категории

АО «НПП «Рубин»



Зорькин А.С.

Работа допущена к защите (протокол заседания кафедры от 23.01.18 № 9)

Заведующий кафедрой



С.Л. Зефирова

Работа защищена с отметкой хорошо (протокол заседания ГЭК
от 24.01.18 № 11)

Секретарь ГЭК



А.Г. Фатеев

Пенза 2018

*Работа проверена 11.01.2018
13.01.2018 БС Султанов*

Оглавление

Введение.....	5
1 Анализ существующей нормативно-правовой базы в области защиты конфиденциальной информации	8
1.1 Понятие и виды конфиденциальной информации	8
1.2 Понятие и виды защиты конфиденциальной информации	11
2 Исследование технических каналов утечки и источников угроз безопасности конфиденциальной информации	14
2.1 Технические каналы утечки информации	14
2.2 Источники угроз безопасности информации	25
3 Понятие информационного контура организации.....	29
4 Разработка схемы информационного контура	31
5 Классификация закрытого информационного контура по требованиям защиты информации	33
5.1 Классификация информационных систем.....	33
5.2 Определения уровня значимости информации, обрабатываемой в закрытом информационном контуре	33
5.3 Определение масштаба закрытого информационного контура как информационной системы	35
5.4 Определение класса защищенности закрытого информационного контура	35
6 Определение актуальных угроз безопасности информации, обрабатываемой в закрытом информационном контуре.....	36
6.1 Используемая нормативно-методическая документация	36
6.2 Определение угроз безопасности информации и их источников	36
6.3 Определение возможных способов реализации угроз безопасности информации	41
6.4 Определение актуальных угроз безопасности информации в информационной системе	44

7	Определение требований к системе защиты информации, обрабатываемой в закрытом информационном контуре.....	50
7.1	Порядок определения требований к системе защиты информации информационной системы	50
7.2	Выбор мер защиты для закрытого информационного контура	53
7.3	Определение необходимых средств защиты информации	59
8	Сравнительный анализ и выбор системы защиты информации закрытого информационного контура.....	65
8.1	Выбор системы защиты информации от несанкционированного доступа	65
8.2	Выбор АПМДЗ	73
8.3	Выбор средств защиты от несанкционированного доступа.	78
9	Разработка комплекса организационно-технических мер защиты информации в закрытом информационном контуре.....	79
9.1	Организационные меры защиты информации.....	79
9.2	Технические меры защиты информации	81
10	Выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации закрытого информационного контура.....	83
10.1	Выбор средства анализа защищенности.....	83
10.2	Выбор средства резервного копирования	86
10.3	Выбор генератора электромагнитного шума	88
10.4	Структура закрытого информационного контура	92
11	Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	95
11.1	Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации.....	95
11.2	Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов	98

Заключение	100
Список используемых источников.....	101
Приложение А Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ»	105

Введение

Вопрос защиты информации от несанкционированного доступа возник очень давно, с тех пор, как у человека появились основания скрывать какую-либо информацию от других людей. С развитием общества, государства, науки и техники информации становится все больше, а ее ценность растет. Информация, владение которой может принести обладателю какие-то преимущества, выгоду, является наиболее ценной. И такая информация существует везде: ей владеют государства, организации, частные лица. Поэтому оборот и защита конфиденциальной информации регулируются на уровне федеральных законов и других нормативно-правовых документов.

Стремительное развитие и внедрение средств вычислительной техники в производство значительно увеличивает производительность труда, позволяет обрабатывать большие объемы информации за меньшее время. Но с увеличением количества информации, обрабатываемой в электронном виде, все более актуальной становится проблема обеспечения ее безопасности.

Обработка больших объемов конфиденциальной информации требует особых условий. Одним из вариантов обеспечения таких условий является использование изолированных АРМ. Однако это существенно замедляет производственный процесс, поскольку обмен конфиденциальной информацией между операторами возможно осуществлять только «вручную» с использованием съемных носителей. Так же могут существенно возрасти финансовые затраты, ведь для доступа к открытым источникам информации, например к какой-либо базе данных, операторам понадобятся дополнительные АРМ.

Исключить эти недостатки можно путём создания защищенной локальной сети, распределенной между несколькими помещениями, объединяющей в себе сервер и автоматизированные рабочие места, на которых обрабатывается конфиденциальная и открытая информация, не имеющей выхода во внешнюю сеть. В рамках работы такая сеть была названа закрытым информационным контуром.

Закрытый информационный контур позволит оптимизировать производственный процесс благодаря обеспечению оперативного обмена конфиденциальной информацией без использования съемных носителей и обеспечения доступа к базе данных со всех АРМ, а также уменьшить финансовые затраты благодаря сокращению числа АРМ.

Целью выпускной квалификационной работы является разработка структуры закрытого информационного контура, обеспечивающего сбор, хранение, обработку, обмен и предоставление конфиденциальной информации, с применением программно-аппаратных средств защиты информации и организационно-технических мер, для отдела промышленного предприятия.

Задачами выпускной квалификационной работы являются:

- анализ существующей нормативно-правовой базы в области защиты конфиденциальной информации;
- исследование технических каналов утечки и источников угроз безопасности конфиденциальной информации;
- определение понятия информационного контура организации;
- разработка схемы информационного контура отдела предприятия;
- классификация закрытого информационного контура по требованиям защиты информации;
- определение актуальных угроз безопасности информации, обрабатываемой в закрытом информационном контуре;
- определение требований к системе защиты информации, обрабатываемой в закрытом информационном контуре;
- сравнительный анализ и выбор системы защиты информации закрытого информационного контура;
- разработка комплекса организационно-технических мер защиты информации в закрытом информационном контуре;
- выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации закрытого информационного контура;

– исследование вредных психофизиологических факторов, влияющих на психоэмоциональное состояние специалиста по защите информации, а также методов и средств физической культуры, снижающих их воздействие.

1 Анализ существующей нормативно-правовой базы в области защиты конфиденциальной информации

1.1 Понятие и виды конфиденциальной информации

Согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1] (далее - Закон об информации), циркулирующую в обществе информацию можно разделить на общедоступную и информацию ограниченного доступа, т.е. информацию, доступ к которой ограничивается федеральными законами.

В зависимости от порядка предоставления информация подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по договоренности лиц, принимающих участие в соответствующих отношениях;
- информацию, которая подлежит предоставлению или распространению согласно федеральным законам;
- информацию, распространение которой на территории Российской Федерации ограничено или запрещено [1].

Также законом об информации определено понятие конфиденциальности информации. Согласно ему, конфиденциальность информации - это обязательное для исполнения требование к лицу не передавать полученную им информацию посторонним лицам без согласия ее обладателя [1].

Виды конфиденциальной информации определены Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» [2]. К ней относятся:

- сведения о частной жизни гражданина, прямо или косвенно позволяющие определить его личность (персональные данные);
- сведения, являющиеся тайной следствия и судопроизводства, сведения о применении в отношении определённых лиц мер государственной защиты, а также сведения об этих мерах;

- служебные сведения, доступ к которым ограничивается государственными органами в соответствии с Гражданским кодексом Российской Федерации и (или) федеральными законами (служебная тайна);
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен согласно Конституции Российской Федерации и федеральным законам (тайна переписки, почтовых отправлений, телефонных переговоров, нотариальная, врачебная, адвокатская тайна);
- сведения, обусловленные коммерческой деятельностью, доступ к которым ограничивается в соответствии с Гражданским кодексом Российской Федерации и (или) федеральными законами (коммерческая тайна);
- сведения о сущности изобретений, их моделей или опытных образцах до публикации в официальных источниках информации о них;
- сведения, содержащиеся в личных делах осужденных, а также сведения о исполнении судебных заключений и других актов [2].

Из представленных видов конфиденциальной информации в закрытом информационном контуре будут присутствовать следующие:

- служебные сведения ограниченного доступа (служебная тайна);
- сведения, связанные с коммерческой деятельностью (коммерческая тайна).

Постановлением Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти...» [3] (далее - Положение) определяется порядок обработки служебной информации в федеральных органах исполнительной власти, на подведомственных им предприятиях, в учреждениях и организациях. Согласно Положению, к служебной информации ограниченного распространения можно относить несекретную информацию, затрагивающую деятельности организаций, ограничения на распространение которой накладываются в связи с служебной необходимостью. Положением установлено, что на документах, содержащих служебную тайну, ставится по-

метка «Для служебного пользования». Кроме того, Положение определяет порядок изготовления, учета и оборота документов ограниченного распространения.

Определение коммерческой тайны представлено в Федеральном законе от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне» [4]. В нем коммерческая тайна определена как режим конфиденциальности информации, позволяющий ее обладателю при прочих обстоятельствах повысить доходы, избежать расходов, сохранить или улучшить положение на рынке или получить другую коммерческую выгоду в виду неизвестности такой информации другим лицам.

Закон «О коммерческой тайне» определяет следующие виды информации, которая не может относиться к коммерческой тайне:

- информация, которая содержится в учредительных документах юридических лиц, документах, подтверждающих факт внесения юридических лиц и индивидуальных предпринимателей в государственные реестры;
- информация, содержащаяся в документах, дающих право на занятие предпринимательской деятельности;
- информация, о составе имущества государственных или муниципальных унитарного предприятий, государственных учреждений и об использовании ими средств бюджетов;
- информация о уровне загрязнения окружающей среды, состоянии противопожарной безопасности, безопасности продуктов питания, санитарно-эпидемиологической обстановке, радиационной обстановке и других факторах, оказывающих неблагоприятное влияние на обеспечение безопасного функционирования промышленных объектов или безопасности населения в целом;
- информация о численности и составе работников, об условиях и принципах оплаты труда, о профессиональной заболеваемости и травматизма на производстве, о наличии вакантных рабочих мест.

Закон «О коммерческой тайне» устанавливает организационные меры, обеспечивающие безопасность документов, содержащих сведения, составляющие коммерческую тайну, от неправомерного доступа. В том числе законом

установлено, что на документах, содержащих такие сведения, должен проставляться гриф «Коммерческая тайна» [4].

1.2 Понятие и виды защиты конфиденциальной информации

Согласно Закону об информации, защита информации - это принятие комплекса организационно-технических мер, нацеленных на:

- обеспечение защиты информации от неправомерного доступа, модификации, уничтожения, блокирования и иных неправомерных действий;
- обеспечение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации [1].

Терминология, связанная с защитой информации, представлена в ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Согласно этому ГОСТу защита информации - деятельность, направленная на исключение возможности утечки защищаемой информации, предотвращение неправомерных и непреднамеренных воздействий на защищаемую информацию, то есть информацию, являющуюся предметом собственности и подлежащую защите согласно требованиям нормативно-правовых документов или требованиям, устанавливаемым обладателем информации.

ГОСТ Р 50922-2006 выделяет следующие виды защиты информации:

- правовая защита информации - обеспечение безопасности информации правовыми методами, включающими в себя разработку нормативно-правовых документов, регулирующих полномочия доступ к информации, ввод в действие этих документов и контроль за их исполнением;
- техническая защита информации - обеспечение безопасности информации некриптографическими методами в соответствии с действующими нормативно-правовыми документами с применением специальных технических, программных и программно-технических средств;
- криптографическая защита информации - обеспечение безопасности информации благодаря ее криптографическому преобразованию;

– физическая защита информации - обеспечение безопасности информации благодаря применению организационных мероприятий и технических средств, создающих препятствия для получения физического доступа к объекту защиты посторонних лиц [5].

Организационные мероприятия, направленные на обеспечение физической защиты информации, предполагают установление режимных, временных, территориальных, пространственных ограничений на доступ к объекту защиты [5].

Защита информации осуществляется от:

– утечки - неконтролируемое распространение информации вследствие ее разглашения, получения к ней неправомерного доступа или перехвата техническими разведками;

– несанкционированного воздействия - целенаправленное воздействие на защищаемую информацию, в результате которого происходит искажение, уничтожение или блокирование доступа к информации, а также утрате или сбою ее носителя;

– непреднамеренного воздействия - воздействие на защищаемую информацию, связанное с ошибками пользователей, сбоями в работе программных и технических средств системы, природных явлений и иных не антропогенных происшествий, в результате которого происходит искажение, уничтожение или блокирование доступа к информации, а также утрате или сбою ее носителя;

– разглашения - неправомерного доведения защищаемой информации до лиц, не имеющих доступа к этой информации;

– несанкционированного доступа - получения защищаемой информации злоумышленником с нарушением установленных обладателем информации правил доступа к защищаемой информации;

– разведки - перехвата защищаемой информации технической, агентурной разведкой [5].

Для конфиденциальной информации порядок защиты информации устанавливается владельцем информационных ресурсов или уполномоченным им лицом на основании Закона об информации.

Контроль за соблюдением требований к системе защиты информации, а также реализацию защитных мер в информационной системе, обрабатывающей информацию ограниченного доступа в негосударственных организациях, возложены на государственные органы. Владелец информации также имеет право осуществлять аналогичный контроль. Законом устанавливаются только перечни сведений, которые не могут быть отнесены к конкретному виду конфиденциальной информации [6].

2 Исследование технических каналов утечки и источников угроз безопасности конфиденциальной информации

2.1 Технические каналы утечки информации

2.1.1 Общая классификация технических каналов утечки информации.

Техническим каналом утечки информации (ТКУИ) называют совокупность объекта разведки, технических средств разведки (ТСР), с помощью которых злоумышленник добывает информацию на объекте разведки, и физической среды, в которой распространяется информативный сигнал. Иными словами, под ТКУИ подразумевают способ получения с помощью технических средств информации об объекте. Под разведывательной информацией обычно понимают сведения об объекте разведки независимо от их формы представления.

Носителями информации являются сигналы. Сигналы различны по своей физической природе. Различают электрические, электромагнитные, акустические, оптические сигналы. Информация содержится в их изменяющихся параметрах.

В зависимости от своей природы сигналы распространяются в различных физических средах. Средой распространения могут быть газовые, жидкостные и твердые среды, например: воздух, вода, конструкции зданий, линии связи и другие токопроводящие элементы.

Технические средства разведки применяются для приема и измерения параметров сигналов и последующего выделения из них информации.

Классификация технических каналов утечки информации в графическом виде приведена на рисунке 1.



Рисунок 1 - Классификация технических каналов утечки информации

2.1.2 Технические каналы утечки информации при обработке ОТСС.

Основными техническими средствами и системами (ОТСС) называют технические средства, на которых производится обработка конфиденциальной информации. К ним относятся электронно-вычислительные машины, режимные телефонные станции, системы связи, системы звукоусиления [7].

При идентификации технических каналов утечки информации ОТСС необходимо рассматривать как совокупность основного (стационарного) оборудования, оконечных устройств, линий связи (проводов и кабелей, прокладываемых между отдельными ОТСС и их элементами), коммутационных устройств, сети электропитания и заземления.

Технические средства, на которых обрабатывается конфиденциальная информация, в совокупности с помещением, в котором они находятся, составляют объект ОТСС. Под объектами ОТСС понимают также выделенные помещения, предназначенные для ведения конфиденциальных переговоров.

Наряду с ОТСС в помещениях устанавливаются технические средства, которые непосредственно не участвуют в обработке конфиденциальной информации, но используются совместно с ОТСС и находятся в зоне электромагнитного поля, создаваемого ими. Они называются вспомогательными техническими средствами и системами (ВТСС). Среди них можно выделить технические средства открытой телефонной связи, системы противопожарной и охранной сигнализации, электрификации, радиофикации, электробытовые приборы [7].

Основной риск утечки информации по техническим каналам несут ВТСС, линии которых выходят за пределы контролируемой зоны (КЗ). Контролируемой зоной называют территорию, в которой исключено пребывание посторонних лиц и транспортных средств [7].

Кроме линий, непосредственно соединяющих ОТСС и ВТСС, за пределы КЗ могут выходить посторонние провода и кабели, проходящие через помещения, в которых расположены ОТСС и ВТСС, а также металлические трубы отопления и водопровода и другие металлоконструкции. Они называются посторонними проводниками.

В зависимости от физической среды распространения сигнала, его природы и способов перехвата, ТКУИ подразделяются на электромагнитные, электрические и параметрические.

К электромагнитным каналам относятся каналы утечки, возникающие за счет побочных электромагнитных излучений (ПЭМИ) ОТСС, а именно:

- излучений элементов ОТСС;
- излучений промодулированных информативным сигналом сигналов высокочастотных генераторов ОТСС;
- излучений на частотах самовозбуждения усилителей низкой частоты ОТСС [8].

В ОТСС носителем информации является электрический ток, в изменяющихся параметрах которого содержится информация. При прохождении тока по элементам ОТСС в пространстве возникает электромагнитное поле, промодулированное по закону информационного сигнала.

Электромагнитные излучения высокочастотных генераторов ОТСС и ВТСС. В состав ОТСС и ВТСС могут входить различные высокочастотные генераторы, например: генераторы тактовых частот, генераторы измерительных приборов. В процессе работы электрическая составляющая информационного сигнала может наводиться на провода и другие элементы, а магнитная составляющая - на катушки индуктивности, дроссели цепей электропитания. В результате собственные колебания генератора могут быть промодулированы информационным сигналом, и эти промодулированные колебания будут излучаться в окружающее пространство.

Самовозбуждение усилителей низких частот ОТСС возможно благодаря случайным преобразованиям отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные. В этом случае усилитель переходит в режим автогенерации сигналов. Частота самовозбуждения находится в пределах рабочих частот нелинейных элементов УНЧ. Сигнал на частотах самовозбуждения как правило модулируется информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в режим перегрузки.

Перехватить эти излучения, промодулированные информационным сигналом, возможно с помощью радиотехнических средств разведки, находящимися за пределами КЗ. Зона, в которой возможен такой перехват с последующей расшифровкой сигнала, то есть зона, в которой отношение «информационный сигнал/помеха» превышает некоторое допустимое значение, называется зоной 2 с радиусом R2 [7]. Местоположение зоны 2 относительно других зон безопасности схематично изображено на рисунке 2.

Причинами возникновения электрических каналов утечки информации могут быть:

- наводки ПЭМИ ОТСС на посторонние проводники, имеющие выход за пределы контролируемой зоны;
- утечка информативных сигналов в линии электропитания ОТСС;
- утечка информативных сигналов в линии заземления ОТСС [8].

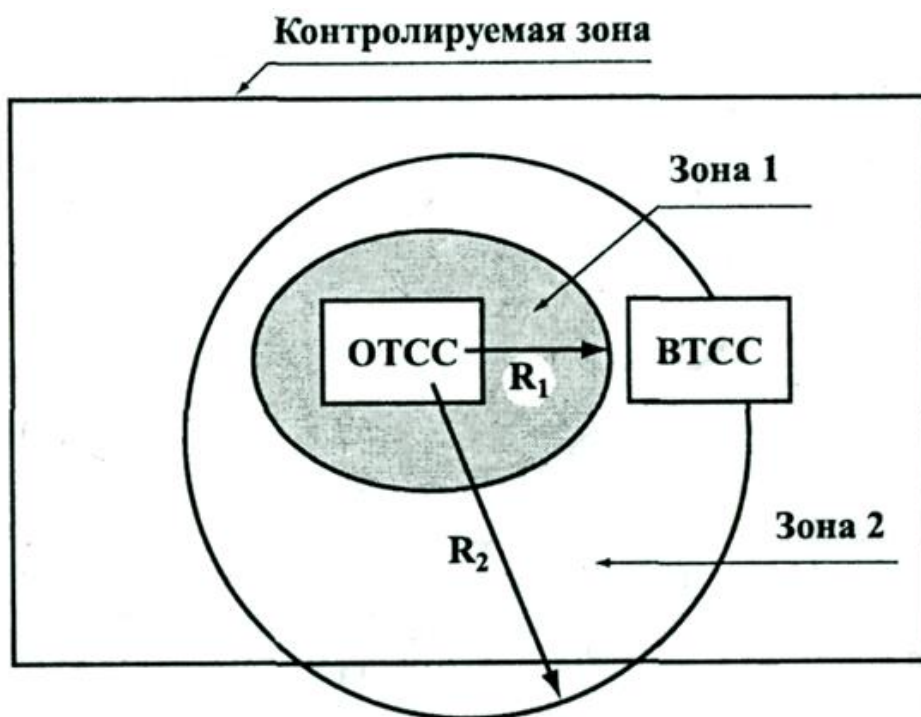


Рисунок 2 - Зоны безопасности информации

Наводки ПЭМИ ОТСС возникают при излучении элементами ОТСС, а также их проводниками информативных сигналов вблизи посторонних проводников. Уровень наводимых сигналов зависит от мощности излучаемого информативного сигнала, расстояния до постороннего проводника, а также от протяженности совместного пробега посторонних проводников и линий ОТСС.

Окружающее пространство ОТСС, в пределах которого на случайные антенны наводится информативный сигнал с уровнем, выше некоторого допустимого, называется (опасной) зоной 1 [7]. Местоположение зоны 1 относительно других зон безопасности схематично отображено на рисунке 2.

Случайной антенной называется цепь ВТСС или посторонний проводник, на который могут навестись побочные электромагнитные излучения.

Случайные антенны подразделяются на сосредоточенные и распределенные. К сосредоточенным случайным антеннам относятся устройства, такие как телефон, громкоговоритель. К распределенным случайным антеннам относят протяженные элементы, такие как провода, металлические коммуникации, металлоконструкции [7].

Утечка информативных сигналов в цепи электропитания возможна как за счет ПЭМИ, так и за счет внутренних паразитных связей выпрямительного устройства блока питания. Кроме того, усиление информационных сигналов происходит напрямую от источника электропитания, что может создавать на внутреннем сопротивлении источника питания падение напряжения, которое при недостойном затухании в фильтре может быть зафиксировано в линии электропитания. Также значение потребляемого тока в усилителях зависит от амплитуды информационного сигнала, что в свою очередь создает неравномерную нагрузку на источник питания и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Утечка информативных сигналов в цепи заземления происходит за счет наводок на многочисленные цепи заземления, а также имеющие гальваническую связь с землей металлоконструкции.

Перехватить наведенный на посторонние проводники информативный сигнал возможно с помощью непосредственного подключения к этим проводникам, а также системам электропитания и заземления. Для этих целей используются специальные технические средства разведки и специальная высокочувствительная измерительная аппаратура.

Перехват обрабатываемой в ОТСС информации возможен также с помощью «высокочастотного облучения». При облучении ОТСС происходит переизлучение электромагнитного поля элементами ОТСС, которое чаще всего оказывается промодулировано информативным сигналом. Для выделения информации из переизлученного сигнала может использоваться временная или частотная развязка. В связи с изменением параметров сигналов при переизлучении, данный канал называется параметрическим. Перехватить информацию по этому каналу возможно с помощью специальных узконаправленных высокочастотных генераторов и специальных радиоприемных устройств.

Нередки случаи съема информации с использованием электронных устройств негласного получения информации, (аппаратных закладок). Они устанавливаются непосредственно внутрь ОТСС и представляют собой передатчики,

излучающие сигнал, который модулируется информационным сигналом. Перехваченная информация либо в реальном времени передается нарушителю, либо накапливается и передается по команде. Чаще всего закладки устанавливаются в технические средства иностранного производства.

2.1.3 Технические каналы утечки акустической (речевой) информации.

Акустической информацией называют информацию, носителем которой является акустический сигнал. Информация, источником сигнала которой является человеческая речь, называется речевой. Акустический сигнал представляет собой механические колебания, которые распространяются от источника в виде волн различной длины.

Источники акустических сигналов подразделяются на первичные и вторичные. Первичными являются механические колебательные системы, например голосовые связки человека. Вторичными являются преобразователи различных типов, например электроакустические, представляющие собой устройства преобразования акустического сигнала в электрический и обратно, такие как микрофоны, громкоговорители [8].

Акустические сигналы могут простыми (тональными) и сложными. Простые представляют собой синусоидальное колебание, а сложные - спектр таких колебаний.

Речевой сигнал представляя собой сложный акустический сигнал в диапазоне частот от 200 Гц до 6 кГц.

Каналы утечки акустической информации в зависимости от среды распространения и способа перехвата подразделяются на воздушные, вибрационные, электроакустические, параметрические и оптико-электронный.

В воздушных каналах утечки акустической информации средой распространения сигнала является воздух. Перехват сигнала осуществляется с помощью специальных высокочувствительных микрофонов. Они соединяются с миниатюрными записывающими устройствами и (или) передатчиками. Такие устройства называют акустическими закладками. Перехваченная такими микрофонами информация может передаваться по различным каналам: радиоканалу,

оптическому каналу (в инфракрасном диапазоне), по цепям электропитания, по металлоконструкциям (как с помощью электрических колебаний, так и с помощью механических ультразвуковых колебаний).

Прием перехваченной информации осуществляется на специальные устройства, работающие в соответствующем диапазоне, или на обычный телефон, в случае установки закладки в телефонном аппарате.

Использование закладных устройств требует проникновения на объект. В случае, когда это невозможно, но есть прямая видимость на источник акустического сигнала, применяют направленные микрофоны.

В вибрационных каналах утечки средой распространения сигнала являются конструкции зданий, коммуникации и другие твердые тела. Для перехвата информации по такому каналу используются специальные контактные микрофоны, называемые стетоскопами. Чаще всего они применяются в совокупности с электронным усилителем и называются электронными стетоскопами.

По вибрационному каналу также возможно осуществить перехват с помощью закладок. Для передачи перехваченной информации чаще всего используется радиоканал, такие устройства называются радиостетоскопами. Но также возможна передача по оптическому каналу (в инфракрасном диапазоне) и с помощью ультразвуковых колебаний по металлоконструкциям.

Электроакустические каналы утечки информации возникают за счет электроакустических преобразований сигналов и включают в себя перехват сигналов от ВТСС, обладающих микрофонным эффектом, а также с помощью высокочастотного навязывания.

Некоторые элементы ВТСС (трансформаторы, реле, электромагниты, звонки) способны изменять свои параметры под воздействием акустических сигналов. Изменение параметров приводит к возникновению в этих элементах электродвижущей силы, изменяющейся по закону информационного акустического сигнала или модуляции протекающих электрических сигналов акустическим.

Кроме того, ВТСС могут содержать непосредственно электроакустические преобразователи (сирены сигнализации, громкоговорители). Преобразование акустического сигнала в электрический называют «микрофонным эффектом».

Перехват информации в данном канале осуществляет с помощью непосредственного подключения специальных высокочувствительных низкочастотных усилителей к линиям ВТСС, обладающих микрофонным эффектом.

Перехват с помощью высокочастотного навязывания может быть осуществлен с помощью облучения ОТСС и ВТСС высокочастотным сигналом и принятия переизлученного сигнала, промодулированного информационным сигналом. Для приема сигнала используются специальные высокочувствительные приемники. Для исключения взаимного влияния зондирующего и переотраженного сигнала можно использовать импульсные сигналы. Наиболее часто этим способом перехватываются переговоры, ведущиеся по телефону, имеющему выход за пределы КЗ. Для исключения влияния высокочастотного сигнала на АТС в линию ставятся специальные высокочастотные фильтры.

Оптико-электронный канал утечки акустической информации образуется при облучении лазерным лучом тонких отражающих поверхностей, которые колеблются под воздействием акустического сигнала (окон, зеркал). Отраженный луч модулируется по амплитуде и фазе информационным сигналом и принимается специальным приемником оптического излучения. При демодуляции луча выделяется акустический сигнал. Лазер и приемник могут быть установлены в разных местах.

Для перехвата информации в этом канале использую сложные лазерные акустические локационные системы, работающими в инфракрасном диапазоне. Часто их называют лазерными микрофонами.

Параметрический канал возникает в результате воздействия акустических колебаний на элементы ОТСС и ВТСС и соответствующего ему незначительного изменения их взаимного расположения, что может привести к изменению параметров излучаемого ими высокочастотного сигнала. Это обусловлено тем, что

изменение взаимного расположения некоторых элементов, например витков катушки индуктивности, приводит к изменению индуктивности, а следовательно и частоты излучения генератора, т.е. к частотной модуляции информационным сигналом. Или под воздействием акустического сигнала может меняться расстояние между пластинами конденсаторов, и, следовательно, меняться емкость по закону информационного сигнала. Промодулированные информационным сигналом высокочастотные колебания могут быть перехвачены с помощью средств радиоразведки.

Кроме того, параметрический канал может быть реализован методом высокочастотного облучения помещений, в которых установлены полуактивные закладки, параметры элементов которых могут изменяться под воздействием акустического сигнала. Для перехвата информации по этому каналу необходимы специальный передатчик с направленным излучением и приемник.

2.1.4. Технические каналы утечки информации при ее передаче по каналам связи.

После обработки ОТСС информация может передаваться по каналам связи. В настоящее время наиболее распространены коротковолновые, ультракоротковолновые, радиорелейные, тропосферные, космические каналы связи, а также кабельные и оптоволоконные линии связи. В зависимости от канала связи и способа перехвата информации выделяют электрический, электромагнитный и индукционный каналы утечки.

Высокочастотные электромагнитные излучения передатчиков средств радиосвязи, несущие информационный сигнал, могут без труда приниматься портативными средствами радиоразведки и при необходимости раскодироваться.

Данный канал используется для перехвата разговоров, ведущихся по средствам радиосвязи, сотовым телефонам и другим беспроводным средствам связи.

Электрический канал утечки информации, передаваемой по проводным линиям связи, предполагает непосредственное контактное подключение к линии связи аппаратуры разведки.

Наиболее простой способ - непосредственное параллельное подключение к линии связи, однако такой способ может быть легко обнаружен, поскольку приводит к изменению характеристик линии связи.

Поэтому чаще средства разведки подключаются к линии связи через согласующие устройства или специальные устройства компенсации падения напряжения. в этом случае обнаружение подключения к линии связи аппаратуры разведки становится существенно затруднено [9].

Такой способ применяют для обычных низкочастотных и коаксиальных кабелей. Для кабелей, в которых поддерживается давление воздуха данный способ не подойдет, поскольку несанкционированное подключение будет сразу обнаружено.

Часто электрический канал применяют для перехвата телефонных разговоров. Перехватываемая информация может записываться или передаваться в реальном времени в пункт приема. устройства, подключаемые к телефонным линиям для перехвата разговоров, называют телефонными закладками.

Поскольку факт непосредственного подключения к линии связи может быть обнаружен, более привлекательным выглядит индуктивный канал утечки, не требующий контактного подключения. В данном канале используется электромагнитное поле, возникающее вокруг проводника при протекании через него тока. Информационный сигнал, протекающий в линии связи, снимается с помощью специального индукционного датчика. Обычно данный метод перехвата информации применяется для съема с симметричных высокочастотных кабелей.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и экранированных стальной лентой или проволокой. Кроме того, к ним могут подключаться средства записи или передачи снятого сигнала.

Кроме информации, обрабатываемой ОТСС, и акустической информации, важную роль играет видовая информация, которая перехватывается разведками в виде изображений объектов, документов.

Способы снятия видовой информации в зависимости от ее характера и назначения можно разделить на два вида:

- наблюдение за объектом;
- съемка объекта.

Наблюдение за объектом ведется в течение определённого (часто длительного) времени. В зависимости от условий могут использоваться различные технические средства разведки. Для наблюдения в светлое время суток применяются оптические приборы, в темное время суток - приборы ночного видения. Кроме того, могут применяться телевизионные системы и тепловизоры. Наблюдение с телевизионных систем может в реальном времени передаваться в пункты приема по проводным или радиоканалам, а также записываться на носитель.

Съемка объектов проводится для документирования результатов разведки и подробного изучения объектов. Для съемки могут использоваться телевизионные и фотографические системы. Фотоаппараты используются, если требуется получить внешний вид отдельного объекта - здания, прибора или человека, а видеокамеры применяют, когда необходима запись какого-либо динамического процесса, например действий отдельных лиц или технологического процесса.

Для съемки с большого расстояния могут средства съемки могут применяться совместно с оптическими приборами. При съемке с близкого расстояния возможна маскировка средств съемки. Кроме того, возможно комплектование фотоаппаратов и телекамер средствами записи или передачи информации в реальном времени по проводному или радиоканалу. Также возможно использование средств съемки совместно с приборами ночного видения или телевизорами для съемки в темное время суток.

2.2 Источники угроз безопасности информации

Все источники угроз безопасности информации можно разделить на три основные группы:

- антропогенные источники угроз (связанные с действиями человека);

- техногенные источники угрозы (связанные с техническими средствами);
- стихийные источниками.

Антропогенные источники представляют собой субъекты, имеющие правомерный или неправомерный доступ к информации или средствам ее обработки. Антропогенные источники можно разделить по отношению к информационной системе на внешние и внутренние, по характеру - на случайные и преднамеренные.

Внешние случайные (непреднамеренные) антропогенные источники могут реализовывать угрозы через ошибки при проектировании информационной системы, ошибки при разработке программного обеспечения, сбои в работе технических средств и т.п. Как пример таких источников можно персонал поставщиков различных услуг, надзорных организаций, аварийных служб. Угрозы, исходящие от таких источников, не несут за собой злого умысла, они происходят по незнанию, халатности, из любопытства.

Внешние преднамеренные источники напротив, имеют злой или корыстный умысел. Их целью является умышленное нанесение ущерба, вывод из строя систем, искажение или кража информации за счет неправомерного проникновения на объект информатизации [10].

Внутренними источниками угроз являются как правило высококвалифицированные сотрудники, хорошо знающие принципы работы программных и аппаратных средств обработки и защиты информации, знакомые со спецификой решаемых системой задач, имеющие непосредственный доступ к информационной системе. К ним можно отнести основной персонал информационной системы, представителей службы защиты информации, персонал ответственный за обеспечение, а также обслуживающий персонал.

Среди угроз, исходящих от внутренних источников, особое место занимают угрозы, связанные с ошибочными действиями или нарушением эксплуатационной и распорядительной документации.

Кроме того, особую группу внутренних антропогенных источников составляют лица с психическими отклонениями, которые могут относиться к

любой категории сотрудников. Меры противодействия угрозам, исходящим от таких источников, могут отличаться от угроз, исходящих от других внутренних источников.

Наибольшую опасность несут преднамеренные угрозы, исходящие и от внешних, и от внутренних антропогенных источников. Такие угрозы можно разделить на 3 основных класса:

- угрозы, связанные с преднамеренными действиями лиц, имеющих непосредственный доступ к информационной системе, реализующих угрозы непосредственно внутри предприятия;
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступ к информационной системе и совершающими свои действия удаленно из внешних сетей;
- угрозы, связанные с действиями лиц, не имеющими доступ к информационной системе, реализуемые через технические каналы утечки информации.

Техногенные источники угроз непосредственно зависят от свойств технических средств. Они, так же как и антропогенные, могут быть внешними и внутренними.

К внешним источникам относятся элементы инфраструктуры информационных систем, такие как средства связи (телефонные линии, сети передачи данных), инженерные коммуникации (водоснабжение, отопление).

К внутренним источникам относятся технические и программные средства информационной системы, вспомогательные средства (сигнализация), другие присутствующие на объекте информатизации технические средства, а также вредоносное программное обеспечение и закладные устройства.

Стихийные источники угроз характеризуются непредсказуемостью и разнообразием. Как правило, они являются внешними по отношению к информационной системе [11]. В первую очередь под ними подразумеваются различные стихийные бедствия, такие как пожары, землетрясения, ураганы и т.д. Появление таких источников тяжело спрогнозировать, исходящим от них угрозам тяжело

противодействовать, а ущерб в случае реализации угрозы может быть довольно велик.

Как правило, защита от угроз, исходящих от техногенных и стихийных источников, в основном осуществляется путем разработки оператором инструкций и правил поведения в случае реализации таких угроз для их нейтрализации и минимизации ущерба.

3 Понятие информационного контура организации

Для многих реальных задач защиты информации в локальных вычислительных сетях существует необходимость контурирования объектов автоматизации по принципу разделения грифа и, как следствие, создания контуров безопасности, в которых обрабатываются документы с разными метками конфиденциальности. Контуров безопасности может быть столько, сколько типов различной по степени конфиденциальности информации циркулирует в системе. Рассмотрим случай, когда таких контуров два: открытый и закрытый (защищенный).

Открытая информация может свободно циркулировать между обоими контурами преимущественно в одну сторону – из открытого контура в закрытый.

Конфиденциальная информация закрытого контура может циркулировать только внутри этого контура. Взаимодействие с открытым контуром возможно только при «понижении грифа». Обмен информацией между объектами осуществляется посредством создания выделенной защищенной информационно-телекоммуникационной системы (ИТКС) по специализированным каналам связи, а также и при помощи сертифицированных криптографических средств.

Схема циркуляции информации между контурами приведена на рисунке 3.

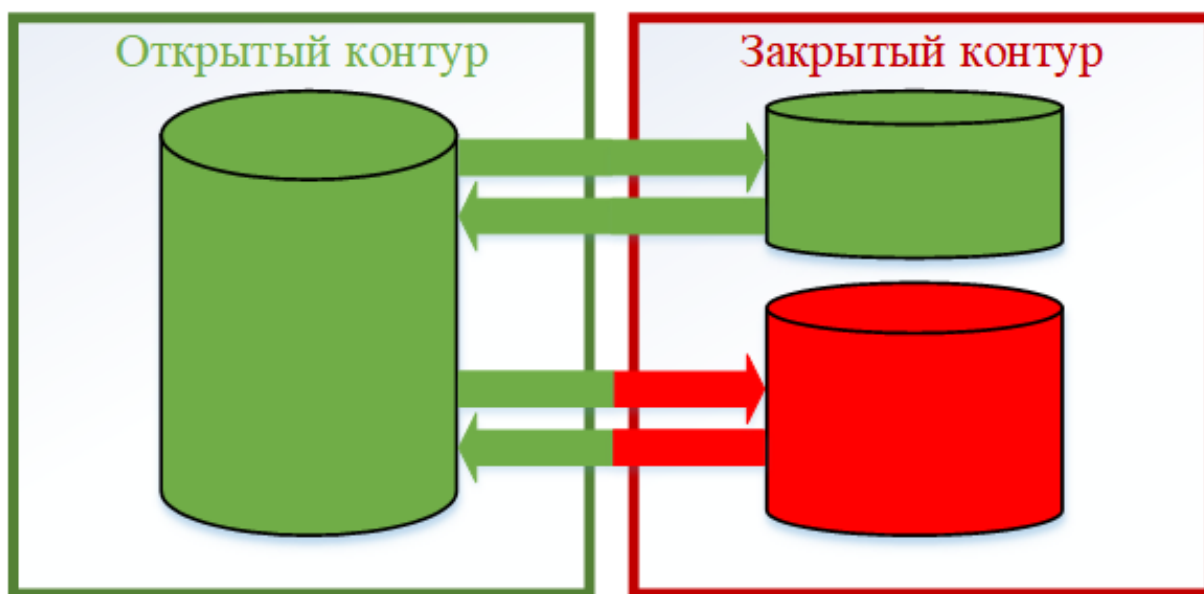


Рисунок 3 - Схема циркуляции информации между контурами

Зеленым цветом показан открытый контур безопасности объекта автоматизации, красным - закрытый контур. Стрелками показаны потоки информации (зеленый - открытая информация, красным - конфиденциальная информация). Одноцветные стрелки означают свободный обмен информацией. Изменение цвета стрелки означает изменение грифа конфиденциальности информации.

Таким образом обеспечивается следующий порядок циркуляции информации между контурами:

- открытая информация свободно (без изменения грифа) циркулирует между контурами, для ее обмена не требуется ни понижения, ни повышения грифа. Повышение грифа конфиденциальности вследствие, например, контекстной подборки, автоматически превращает информацию в конфиденциальную, которая должна обрабатываться в закрытом контуре;
- конфиденциальная информация свободно циркулирует только внутри закрытого контура. Попасть в открытый контур такая информация может только с понижением грифа.

4 Разработка схемы информационного контура

Под информационным контуром подразумевается информационная система, существующая в рассматриваемом отделе в настоящее время. В данной информационной системе обработка конфиденциальной информации осуществляется на изолированных АРМ, не подключенных ни к каким сетям. АРМ, не предназначенные для обработки конфиденциальной информации, подключены к внутренней сети организации, а также к сети Интернет.

Структура данной информационной системы приведена на рисунке 4.



Рисунок 4 - Структура незащищенного информационного контура

В такой системе обмен информацией между АРМ крайне затруднен. Передача на АРМ, предназначенное для обработки конфиденциальной информации, исходной открытой информации, а также обмен конфиденциальной информацией между этими АРМ возможен только с использованием зарегистрированных отчуждаемых носителей (USB-флеш-накопителей). АРМ, предназначенные для обработки открытой информации, необходимы только для того, чтобы сотрудники могли иметь доступ к источникам исходной открытой информации (базе

данных), но при этом на них необходимы дополнительные материальные затраты.

Исключить эти недостатки можно путём создания защищенной локальной сети, распределенной между несколькими помещениями, объединяющей в себе сервер и автоматизированные рабочие места, на которых обрабатывается конфиденциальная и открытая информация, не имеющей выхода во внешнюю сеть. Такой сетью и является закрытый информационный контур.

5 Классификация закрытого информационного контура по требованиям защиты информации

5.1 Классификация информационных систем

В соответствии с Приложением №1 «Определение класса защищенности информационной системы» к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным Приказом №17 ФСТЭК от 11.02.2017 [12] (далее - Требования), класс информационной системы определяется в зависимости от значимости информации, обрабатываемой в ней, а также от ее масштаба. Устанавливаются три класса защищенности информационной системы, которые определяются в зависимости от уровня значимости информации, обрабатываемой в информационной системе, и масштаба информационной системы. Самый низкий класс - третий, самый высокий - первый.

5.2 Определения уровня значимости информации, обрабатываемой в закрытом информационном контуре

Уровень значимости информации зависит от степени возможного ущерба, который будет причинен обладателю информации в результате нарушения одного или нескольких свойств безопасности информации (конфиденциальности, целостности или доступности).

Степень возможного ущерба может быть:

- высокой, если в результате нарушения как минимум одного из свойств безопасности информации возможны существенные негативные последствия и информационная система не сможет выполнять возложенные на нее функции;
- средней, если в результате нарушения как минимум одного из свойств безопасности информации возможны умеренные негативные последствия и

информационная система не сможет выполнять хотя бы одну из возложенных на нее функции;

– низкой, если в результате нарушения как минимум одного из свойств безопасности информации возможны незначительные негативные последствия или информационная система будет выполнять возложенные на нее функции с недостаточной эффективностью.

Информация имеет высокий уровень значимости, если при нарушении как минимум одного из свойств безопасности информации будет нанесен высокий ущерб. Информация имеет средний уровень значимости, если при нарушении как минимум одного из свойств безопасности информации будет нанесен средний ущерб, а в случае нарушения других свойств не будет нанесен высокий ущерб. Информация имеет низкий уровень значимости, если при нарушении любого из свойств безопасности информации будет нанесен низкий ущерб.

Если в системе обрабатывается два или более видов конфиденциальной информации, уровень значимости определяется отдельно для каждого типа информации, а общий уровень значимости информации в информационной системе определяется по наивысшему показателю возможного ущерба, определенному для каждого вида информации.

Степени ущерба для каждого из свойств безопасности информации ограниченного доступа, обрабатываемой в закрытом информационном контуре, приведены в таблице 1.

Таблица 1 - Степень ущерба для конфиденциальной информации, обрабатываемой в закрытом информационном контуре

Вид информации ограниченного доступа	Свойство безопасности информации	Степень ущерба
Служебная тайна	Конфиденциальность	Средняя
	Целостность	Низкая
	Доступность	Средняя
Коммерческая тайна	Конфиденциальность	Высокая
	Целостность	Средняя
	Доступность	Высокая

В соответствии с таблицей 1 для обрабатываемой в закрытом информационном контуре информации ограниченного доступа определен высокий уровень значимости.

5.3 Определение масштаба закрытого информационного контура как информационной системы

Согласно Требованиям о защите информации, не составляющей государственную тайну, информационная система может иметь:

- федеральный масштаб, если она функционирует на территории РФ и имеет сегменты в различных субъектах РФ;
- региональный масштаб, если она функционирует на территории одного субъекта РФ и имеет сегменты в нескольких муниципальных образованиях;
- объектовый масштаб, если она функционирует на территории одного муниципального образования или организации.

Поскольку закрытый информационный контур функционирует в пределах одной организации, он имеет объектовый масштаб.

5.4 Определение класса защищенности закрытого информационного контура

Согласно Требованиям, класс защищенности информационной системы определяется в соответствии с таблицей 2.

Таблица 2 - Определение класса защищенности информационной системы

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
Высокий	K1	K1	K1
Средний	K1	K2	K2
Низкий	K2	K3	K3

В соответствии с таблицей 2 для закрытого информационного контура определен первый класс защищенности.

6 Определение актуальных угроз безопасности информации, обрабатываемой в закрытом информационном контуре

6.1 Используемая нормативно-методическая документация

Определение актуальных угроз безопасности информации в закрытом информационном контуре проводится на основе следующих нормативно методических документов:

- методика определения угроз безопасности информации в информационных системах. ФСТЭК России, 2015 год (проект) (далее - Методика) [13];
- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год (далее - Базовая модель) [14].

6.2 Определение угроз безопасности информации и их источников

Угрозы информационной безопасности системы определяются с целью выяснения, возможно ли при каких-либо обстоятельствах нарушение одного из свойств безопасности информации и какие последствия такое нарушение принесет обладателю информации [13].

При определении угроз безопасности информации учитываются состав элементов информационной системы, наличие и структура взаимосвязей между ними, а также с внешними информационными системами.

Угрозы безопасности конфиденциальной информации, обрабатываемой в закрытом информационном контуре, были определены в соответствии с базовой моделью угроз персональных данных ФСТЭК. Согласно базовой модели угроз в распределенных информационных системах, не подключенных к внешним сетям и сетям международного обмена, возможна реализация следующих угроз информационной безопасности:

- угрозы утечки информации по техническим каналам;
- угрозы несанкционированного доступа.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН);
- угрозы утечки видовой информации;
- угрозы утечки акустической (речевой) информации.

Угрозы утечки акустической информации из рассмотрения исключены, поскольку в помещениях закрытого информационного контура не будут проводиться конфиденциальные переговоры.

Угрозы несанкционированного доступа связаны с действиями нарушителей, имеющих доступ к информационной системе, в том числе и ее пользователей, и включают в себя:

- угрозы, реализуемые во время загрузки операционной системы, направленные на кражу аутентификационной информации, модификацию BIOS;
- угрозы, реализуемые после загрузки операционной системы и направленные на получение несанкционированного доступа с помощью стандартных функций операционной системы или какой-либо прикладной программы;
- угрозы внедрения вредоносных программ;
- угрозы анализа сетевого трафика и перехвата передаваемой по сети информации;
- угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений;
- угрозы внедрения ложного объекта сети;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ [14].

Угрозы внедрения по сети вредоносных программ и угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений из рассмотрения исключены, поскольку закрытый информационный контур не подключен к внешним сетям.

Важным этапом в процессе определения угроз безопасности информации в информационной системе является определение лиц или событий (явлений), в результате действий которых может произойти нарушение одного из свойств безопасности информации, то есть источников угроз.

В соответствии с параграфом 2.2 источники угроз безопасности информации могут быть следующих типов:

- антропогенные;
- техногенные;
- стихийные.

Используемая методика нацелена именно на угрозы, исходящие от антропогенных источников, и не содержит методов оценки других источников угроз, поэтому рассматриваться будут только антропогенные источники угроз. Они также часто называются нарушителями.

По наличию непосредственного доступа к элементам системы или обрабатываемой информации нарушителей можно разделить на два типа:

- внешние нарушители - лица, не имеющие физического доступа к компонентам системы;
- внутренние нарушители - лица, имеющие постоянный или временный непосредственный доступ к компонентам информационной системы.

Возможности нарушителей по реализации угроз характеризуются их потенциалом. Разделяют 3 вида потенциала: базовый (низкий), базовый повышенный (средний) и высокий.

Возможные потенциалы нарушителей и соответствующие им возможности приведены в таблице 3.

Таблица 3 - Потенциалы нарушителей

Потенциал нарушителей	Возможности по реализации угроз безопасности информации	Вероятность проявления активности нарушителя в рассматриваемой организации
Базовый (низкий)	Получают информацию о возможных уязвимостях компонентов информационной системы и информацию о методах и средствах реализации угроз из общедоступных источников. Могут самостоятельно создавать методы и средства реализации угроз на основе полученной и общедоступных источников информации.	Высокая, так как в данную группу входят большинство пользователей ИС, обслуживающего персонала и потенциальные внешние нарушители
Базовый повышенный (средний)	Обладают всеми возможностями нарушителей с базовым потенциалом. Осведомлены о защитных мерах, применяемых в информационных системах данного типа. Получают информацию об уязвимостях информационной системы на основе ее анализа с использованием общедоступного программного обеспечения. Осведомлены о структурно-функциональных характеристиках и особенностях функционирования информационной системы	Средняя, так как в данную группу входят часть пользователей ИС, и потенциальных внешних нарушителей. Вхождение в данную группу обслуживающего персонала маловероятно
Высокий	Обладают всеми возможностями нарушителей с базовым и средним потенциалами. Могут осуществить несанкционированный доступ к информационной системе из сети, к которой имеется доступ. Имеют доступ к аппаратному и программному обеспечению информационной системы для преднамеренного внесения в них закладок и уязвимостей. Осведомлены об используемых в информационной системе защитных мерах, программных и аппаратных средствах защиты информации. Могут получить возможность об уязвимостях информационной системы с использованием специальных технических и программных средств. Могут самостоятельно создавать средства и методы реализации угроз безопасности информации в информационной системе с применением специальных технических средств.	Низкая, так как обрабатываемая информация имеет низкую ценность для иностранных государств

Виды нарушителей, имеющих возможность реализации угроз в закрытом информационном контуре, а также их типы, потенциалы и возможные цели приведены в таблице 4.

Таблица 4 - Виды нарушителей

Вид нарушителя	Тип нарушителя	Потенциал нарушителя	Возможные цели реализации угроз безопасности информации
Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Высокий	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.
Внешние субъекты (физические лица)	Внешний	Базовый	Причинение имущественного ущерба. Любопытство или желание самореализоваться. Идентификация уязвимостей для их дальнейшей продажи и получения материальной выгоды
Конкурирующие организации	Внешний	Базовый повышенный	Получение конкурентных преимуществ. Причинение имущественного ущерба
Разработчики, производители и поставщики программных и технических средств	Внешний	Базовый повышенный	Причинение имущественного ущерба. Непреднамеренные, неосторожные или неквалифицированные действия
Лица, занимающиеся установкой, наладкой, монтажом, пусконаладочными и другими видами работ	Внутренний	Базовый	Причинение имущественного ущерба. Непреднамеренные, неосторожные или неквалифицированные действия
Лица, обеспечивающие функционирование информационных систем или обслуживание инфраструктуры оператора (охрана, уборщики)	Внутренний	Базовый	Причинение имущественного ущерба. Непреднамеренные, неосторожные или неквалифицированные действия
Пользователи информационной системы	Внутренний	Базовый	Причинение имущественного ущерба. Любопытство или желание самореализоваться. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
Администраторы информационной системы и администраторы безопасности	Внутренний	Базовый повышенный	Причинение имущественного ущерба. Любопытство или желание самореализоваться. Месть за ранее совершенные действия. Идентификация уязвимостей для их дальнейшей продажи и получения материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
Бывшие работники (пользователи)	Внешний	Базовый	Причинение имущественного ущерба. Месть за ранее совершенные действия

6.3 Определение возможных способов реализации угроз безопасности информации

Возможные способы реализации угроз безопасности информации определяются с целью формирования возможных сценариев реализации угроз безопасности информации, в которых описывается последовательность действий нарушителей или групп нарушителей и применяемые ими для реализации угроз безопасности информации средства и методы [13].

Возможные способы реализации угроз безопасности информации зависят от характеристик и особенностей функционирования системы, целей и возможностей нарушителя.

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- несанкционированного доступа или воздействия на компоненты системы на аппаратном уровне (аппаратное обеспечение, микропрограммы чипсетов) (Д1);
- несанкционированного доступа или воздействия на компоненты системы на общесистемном уровне (BIOS, гипервизор, операционная система) (Д2);
- несанкционированного доступа или воздействия на компоненты системы на прикладном уровне (web-приложения, СУБД, другие прикладные программы) (Д3);
- несанкционированного доступа или воздействия на компоненты системы на сетевом уровне (сетевое оборудование, сервисы, сетевые приложения) (Д4);
- несанкционированного физического доступа или воздействия на линии, связи, технические средства, машинные носители информации (Д5);
- воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия) (Д6).

При определении способа реализации угроз следует учитывать, что угрозы могут быть реализованы нарушителем непосредственно, то есть за счет непосредственного доступа к компонентам системы или информации, или опосредованно, то есть за счет создания условий, которые дают такой доступ, или за счет воздействия на обслуживающую инфраструктуру, которую оператор не контролирует. При этом одной из целей нарушителя, который не имеет доступ к информационной системе, чаще всего является получение доступа (в том числе и через сети общего доступа) с максимально возможными привилегиями.

Также необходимо учитывать, что нарушители могут реализовывать угрозы безопасности информации преднамеренно или случайно (непреднамеренно). В свою очередь преднамеренные действия нарушителей могут заключаться в реализации целенаправленных или нецеленаправленных угроз безопасности информации.

Целенаправленная угроза безопасности информации реализуется в отношении интересующей нарушителя системы с заранее известными ему структурой, характеристиками и особенностями функционирования. Нецеленаправленная («Веерная») угроза, напротив, не ориентирована на конкретную систему. Такая угроза реализуется в целях нарушения безопасности как можно большего числа систем. При этом нарушитель не обладает никакой информацией об атакуемой системе.

Реализация преднамеренных угроз безопасности информации, как правило, включает следующие этапы:

- сбор информации о системе, ее структуре, характеристиках и особенностях функционирования (Э1);
- выбор методов и средств, необходимых для реализации угрозы в данной системе (Э2);
- непосредственная реализация угроз безопасности информации (Э3);
- устранение признаков и следов преступных действий (Э4).

Также при определении возможных способов реализации угроз безопасности информации необходимо исходить из следующих условий:

- нарушитель может действовать в одиночку или в составе группы нарушителей (У1);
- внешний нарушитель и внутренний нарушитель могут действовать совместно (У2);
- угрозы могут быть реализованы в любом узле информационной системы и в любое время (У3);
- нарушитель выбирает наиболее слабое звено информационной системы для реализации угрозы (У4).

Возможные способы реализации угроз безопасности информации в закрытом информационном контуре приведены в таблице 5.

Таблица 5 - Возможные способы реализации угроз безопасности информации

Вид нарушителя	Действия нарушителя	Способ реализации угроз	Наличие намерений реализации угроз	Наличие цели у нарушителя	Этапы реализации угроз	Условия реализации угроз
Специальные службы иностранных государств	Д5	Непосредственно	Преднамеренно	Целенаправленно	Э1,Э2,Э3	У2
	Д6	Непосредственно	Преднамеренно	Целенаправленно	Э1,Э2	У2, У3
Конкурирующие организации	Д5	Непосредственно	Преднамеренно	Целенаправленно	Э1, Э2, Э3, Э4	У2, У3, У4
	Д6	Непосредственно	Преднамеренно	Целенаправленно	Э1, Э2	У2
Разработчики, производители и поставщики программных и технических средств	Д1, Д2, Д3, Д4	Непосредственно	Непреднамеренно	-	Э2	У3
Лица, занимающиеся установкой, наладкой, монтажом, пусконаладочными и другими видами работ	Д1, Д2	Опосредованно	Непреднамеренно	-	Э2	У3
	Д1, Д2, Д5	Опосредованно	Преднамеренно	Целенаправленно	Э2, Э3	У1, У2, У4
Лица, обеспечивающие	Д1, Д4, Д5	Непосредственно	Непреднамеренно	-	Э2, Э3	У3

Продолжение таблицы 5

Вид нарушителя	Действия нарушителя	Способ реализации угроз	Наличие намерений реализации угроз	Наличие цели у нарушителя	Этапы реализации угроз	Условия реализации угроз
функционирование информационных систем или обслуживание инфраструктуры оператора (охрана, уборщики)	Д1, Д4, Д5	Опосредованно	Преднамеренно	Целенаправленно	Э2, Э3	У1, У2, У4
Пользователи информационной системы	Д2, Д3, Д4	Непосредственно	Непреднамеренно	-	Э2, Э3	У3
	Д1, Д2, Д5	Опосредованно	Преднамеренно	Целенаправленно	Э2, Э3	У1, У2, У4
Администраторы информационной системы и администраторы безопасности	Д1, Д2, Д3, Д4, Д5	Непосредственно	Непреднамеренно	-	Э2, Э3	У3
	Д1, Д2, Д5	Опосредованно	Преднамеренно	Целенаправленно	Э2, Э3	У1, У2, У4
Бывшие работники (пользователи)	Д5	Непосредственно	Преднамеренно	Целенаправленно	Э1, Э2, Э3	У2, У4

6.4 Определение актуальных угроз безопасности информации в информационной системе

6.4.1 Исходные данные для определения актуальности угрозы.

Угроза безопасности информации считается актуальной для конкретной информационной системы, если существует вероятность ее реализации нарушителем с соответствующим потенциалом, что может привести к нарушению одного из свойств безопасности информации и неприемлемым негативным последствиям (ущербу).

При отсутствии статистических данных о вероятности реализации той или иной угрозы в данной информационной системе или подобных ей информационных системах актуальность угроз определяется на основе оценки возможности их реализации.

Возможность реализации угрозы определяется исходя из уровня защищенности информационной системы и потенциала нарушителя, необходимого для реализации данной угрозы.

При определении актуальности угроз на этапе создания или проектирования информационной системы, когда защитные меры еще не реализованы или не оценена их эффективность, оценка возможности реализации угрозы может проводиться на основе уровня проектной защищенности информационной системы.

6.4.2 Определение уровня проектной защищенности закрытого информационного контура.

Уровень проектной защищенности определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице 3 Методики. На основе данной таблицы были определены показатели, определяющие проектную защищенность закрытого информационного контура. Результаты приведены в таблице 6.

Таблица 6 - Параметры исходной защищенности закрытого информационного контура

Структурно-функциональные характеристики информационной системы Управления, условия ее эксплуатации	Уровень проектной защищенности закрытого информационного контура		
	Высокий	Средний	Низкий
1. По структуре информационной системы: локальная информационная система		+	
2. По используемым информационным технологиям: -			
3. По архитектуре информационной системы: файл-серверные системы использование выделенных каналов связи		+	+
4. По наличию (отсутствию) взаимосвязей с иными информационными системами: не взаимодействующая с системами;		+	
5. По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования: не подключена	+		

Продолжение таблицы 6

Структурно-функциональные характеристики информационной системы Управления, условия ее эксплуатации	Уровень проектной защищенности закрытого информационного контура		
	Высокий	Средний	Низкий
6. По размещению технических средств: расположенные в пределах одной контролируемой зоны	+		
7. По режимам обработки информации в информационной системе: многопользовательский;			+
8. По режимам разграничения прав доступа: с разграничением		+	
9. По режимам разделения функций по управлению информационной системой: без разделения			+
10. По подходам к сегментированию информационной системы: с сегментированием		+	

Информационная система имеет низкий уровень проектной защищенности, поскольку для среднего уровня необходимо, чтобы не менее 90% характеристики имели уровень не ниже среднего, а в рассматриваемой системе таких характеристик только 70%.

6.4.3 Определение потенциала нарушителя, необходимого для реализации угрозы.

Для определения потенциала нарушителя необходимо оценить возможности нарушителя идентифицировать уязвимости и использовать их в информационной системе в ходе подготовки к реализации и непосредственно в ходе реализации угрозы безопасности информации.

Оценка возможностей нарушителя по реализации угрозы в информационной системе проводится по результатам определения следующих показателей:

- время, затрачиваемое нарушителем на идентификацию и использование уязвимости (затрачиваемое время);
- техническая компетентность нарушителя;
- знание нарушителем проекта и информационной системы;
- оснащенность нарушителя;
- возможности нарушителя по доступу к информационной системе.

Числовые значения указанных показателей определяются в соответствии с таблицей 3.1 Методики.

Необходимый для реализации угрозы потенциал был определен для всех идентифицированных угроз. Результаты приведены в таблице 7.

Таблица 7 - Потенциал нарушителя, необходимые для реализации каждой из угроз

Угроза безопасности информации	Показатель возможностей нарушителя					Сумма	Потенциал
	Затрачиваемое время	Техническая компетентность нарушителя	Знание проекта и информационной системы	Возможность доступа к информационной системе	Оснащенность нарушителя		
Угрозы утечки видовой информации	3	5	2	4	5	19	Базовый повышенный
Угрозы утечки информации по каналу ПЭМИН	5	9	4	6	7	31	Высокий
Угрозы, реализуемые во время загрузки операционной системы	3	6	2	6	3	20	Базовый повышенный
Угрозы, реализуемые направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы	3	9	2	6	0	20	Базовый повышенный
Угрозы внедрения вредоносных программ	0	5	2	0	4	11	Базовый
Угрозы анализа сетевого трафика	3	5	4	6	3	21	Базовый повышенный
Угрозы внедрения ложного объекта сети	7	5	4	8	5	29	Высокий
Угрозы навязывания ложного маршрута	5	5	4	6	5	25	Высокий
Угрозы выявления паролей	5	0	0	6	3	14	Базовый
Угрозы типа «Отказ в обслуживании»	5	3	4	4	3	19	Базовый повышенный
Угрозы удаленного запуска приложений	6	9	6	6	7	34	Высокий

6.4.4 Определение возможности реализации угроз.

Возможность реализации угрозы безопасности информации в зависимости от уровня проектной защищенности информационной системы и потенциала нарушителя определяется как высокая, средняя или низкая в соответствии с таблицей 4 Методики.

Возможности реализации угроз безопасности конфиденциальной информации, обрабатываемой в закрытом информационном контуре, приведены в таблице 8.

Таблица 8 - Возможности реализации угроз безопасности конфиденциальной информации

Угроза безопасности информации	Потенциал нарушителя	Уровень защищённости	Возможность реализации УБИ
Угрозы утечки видовой информации	Базовый повышенный	Низкий	Высокая
Угрозы утечки информации по каналу ПЭМИН	Высокий		Высокая
Угрозы, реализуемые во время загрузки операционной системы	Базовый повышенный		Высокая
Угрозы, реализуемые направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы	Базовый повышенный		Высокая
Угрозы внедрения вредоносных программ	Базовый		Высокая
Угрозы анализа сетевого трафика	Базовый повышенный		Высокая
Угрозы внедрения ложного объекта сети	Высокий		Высокая
Угрозы навязывания ложного маршрута	Высокий		Высокая
Угрозы выявления паролей	Базовый		Высокая
Угрозы типа «Отказ в обслуживании»	Базовый повышенный		Высокая
Угрозы удаленного запуска приложений	Высокий		Высокая

6.4.5 Определение актуальных угроз.

Решение об актуальности угрозы безопасности информации для информационной системы с заданными структурно-функциональными характеристиками

и условиями функционирования принимается на основе возможности реализации угрозы и степени возможного ущерба в соответствии с таблицей 8 Методики.

Перечень угроз с решением об их актуальности приведен в таблице 9.

Таблица 9 - Угрозы безопасности информации, обрабатываемой в закрытом информационном контуре

Угроза безопасности информации	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность УБИ
Угрозы утечки видовой информации	Высокая	Высокая	Актуальная
Угрозы утечки информации по каналу ПЭМИН	Высокая		Актуальная
Угрозы, реализуемые во время загрузки операционной системы	Высокая		Актуальная
Угрозы, реализуемые направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы	Высокая		Актуальная
Угрозы внедрения вредоносных программ	Высокая		Актуальная
Угрозы анализа сетевого трафика	Высокая		Актуальная
Угрозы внедрения ложного объекта сети	Высокая		Актуальная
Угрозы навязывания ложного маршрута	Высокая		Актуальная
Угрозы выявления паролей	Высокая		Актуальная
Угрозы типа «Отказ в обслуживании»	Высокая		Актуальная
Угрозы удаленного запуска приложений	Высокая		Актуальная

7 Определение требований к системе защиты информации, обрабатываемой в закрытом информационном контуре

7.1 Порядок определения требований к системе защиты информации информационной системы

Порядок определения требований к системе защиты информации информационной системы определяется разделом III «Требования к мерам защиты информации, содержащейся в информационной системе» Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом №17 ФСТЭК от 11.02.2017 [12] (далее - Требования).

Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и актуальных угроз безопасности информации.

Организационные и технические меры, составляющие систему защиты информационной системы, в зависимости от актуальных угроз и используемых в системе технологий должны включать в себя следующие виды защитных мер:

- меры по идентификации и аутентификации субъектов и объектов доступа, которые должны обеспечивать присвоение этим субъектам и объектам уникального идентификатора, сравнение предъявляемого субъектом при входе в систему идентификатора с перечнем зарегистрированных идентификаторов, а также проверку принадлежности предъявляемого идентификатора предъявляющему его субъекту;
- меры по управлению доступом субъектов доступа к объектам доступа, которые должны обеспечивать разграничение доступа субъектов доступа к объектам доступа в соответствии с установленными в системе правилами разграничения доступа, а также контроль за соблюдением этих правил;

– меры по ограничению программной среды, которые должны обеспечивать установку и использование только разрешенного в информационной системе программного обеспечения и не допускать установку и запуск запрещенного в информационной системе программного обеспечения;

– меры по защите машинных носителей информации, которые должны исключать возможность неправомерного доступа к информации, хранящейся на этих носителях, а также не позволять неправомерное использование этих носителей;

– меры по регистрации событий безопасности, которые должны обеспечивать сбор, хранение, защиту и предоставление информации о происходящих в информационной системе событиях, в том числе событиях, связанных с нарушением безопасности информации, а также гибкие возможности по анализу такой информации;

– меры по антивирусной защите, которые должны обеспечивать обнаружение в информационной системе вредоносного программного обеспечения, направленного на неправомерное уничтожение, ознакомление или модификацию обрабатываемой в системе информации или на нейтрализацию средств защиты информации, а также реагирование на обнаружение такого программного обеспечения;

– меры по обнаружению (предотвращению) вторжений, которые должны обеспечивать обнаружение действий в информационной системе, направленных на неправомерное ознакомление, модификацию или уничтожение обрабатываемой в ней информации, а также предотвращение таких действий;

– меры по контролю (анализу) защищенности информации, которые должны обеспечивать выявление новых уязвимостей в информационной системе путем проведения анализа защищенности и тестирования защитных средств, а также нейтрализацию выявленных уязвимостей;

– меры по обеспечению целостности информационной системы и информации, которые должны обеспечивать обнаружение фактов нарушения целост-

ности программных или аппаратных средств информационной системы или обрабатываемой в ней информации, а также своевременное восстановление поврежденных активов;

- меры по обеспечению доступности информации, которые должны обеспечивать доступ любых пользователей системы, имеющих право на такой доступ, к обрабатываемой в системе информации, в штатном режиме функционирования;

- меры по защите среды виртуализации, которые должны исключать несанкционированный доступ к информации, обрабатываемой в среде виртуализации, и к компонентам среды виртуализации, а также к средствам управления средой виртуализации;

- меры по защите технических средств, которые должны исключать несанкционированный физический доступ к техническим средствам, обрабатывающим информацию, и средствам, обеспечивающим функционирование информационной системы, доступ в помещения, в которых эти средства расположены, а также защиту информации от утечки по техническим каналам;

- меры по защите информационной системы, ее средств, систем связи и передачи данных, которые должны обеспечивать защиту обрабатываемой в информационной системе информации при ее взаимодействии с внешними информационно-телекоммуникационными системами.

Состав защитных мер, а также их базовые наборы для каждого из классов информационных систем приведены в приложении №2 к Требованиям.

Содержание приведенных выше защитных мер, а также требования к их реализации и усилению приведены в методическом документе ФСТЭК «Меры защиты информации в государственных информационных системах», утвержденном 11.02.2014 г. [15].

Выбор защитных мер, реализация которых требуется в соответствии с методической документацией, включает следующие этапы:

- определение базового набора защитных мер исходя из класса защищенности системы;

- адаптацию базового набора исходя из структурно-функциональных характеристик системы (исключение из базового набора защитных мер, непосредственно связанных с не используемыми в системе информационными технологиями);
- уточнение адаптированного базового набора защитных мер путем добавления к нему не предусмотренных базовым набором мер для нейтрализации всех угроз безопасности информации, актуальных для данной системы;
- дополнение уточненного адаптированного базового набора защитных мер в соответствии с иными нормативно-правовыми актами по защите информации.

Защитные меры реализуются в рамках системы защиты информации информационной системы с учетом всех актуальных для нее угроз для всех субъектов и объектов доступа на аппаратном, системном, прикладном и сетевом уровнях.

7.2 Выбор мер защиты для закрытого информационного контура

7.2.1 Определение базового набора мер защиты информации.

Базовый набор защитных мер был определен в соответствии с приложением №2 Требованиям для информационных систем 1 класса защищенности. Базовый набор защитных мер приведен в таблице 10.

Таблица 10 - Базовый набор защитных мер для информационных систем 1 класса защищенности

Условное обозначение и номер меры	Меры защиты информации в информационных системах
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся сотрудниками оператора
ИАФ.2	Идентификация и аутентификация стационарных, мобильных и портативных устройств
ИАФ.3	Управление идентификаторами (создание, присвоение, уничтожение)
ИАФ.4	Управление средствами аутентификации (выдача, регистрация, блокирование) и принятие мер в случае утраты и (или) компрометации средств аутентификации

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в информационных системах
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся сотрудниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление учетными записями внутренних и внешних пользователей (заведение, активация, блокирование и уничтожение)
УПД.2	Реализация необходимых методов (дискреционный, ролевой, мандатный), типов (запись, чтение, выполнение или другой тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, однонаправленная передача, контроль соединений и другие способы управления) информационными потоками между устройствами, сегментами информационной системы, между информационными системами
УПД.4	Разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых прав и привилегий
УПД.6	Ограничение попыток входа в информационную систему
УПД.9	Ограничение числа одновременных сеансов доступа для всех пользователей информационной системы
УПД.10	Прекращение сеанса доступа в систему после установленного времени бездействия пользователя или по его запросу
УПД.11	Управление действиями пользователей, разрешенными до идентификации и аутентификации
УПД.13	Обеспечение защищенного удаленного доступа субъектов доступа к объектам доступа по внешним информационно-телекоммуникационным сетям
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Контроль взаимодействия с внешними информационными системами
УПД.17	Обеспечение доверенной загрузки СВТ
III. Ограничение программной среды (ОПС)	
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
ОПС.2	Управление установкой компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка только разрешенного к использованию программного обеспечения и его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в информационных системах
ЗНИ.2	Контроль доступа к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода и вывода информации на машинные носители информации
ЗНИ.8	Уничтожение информации на машинных носителях при передаче их между пользователями или в сторонние организации (например для ремонта или утилизации)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение подлежащих регистрации событий безопасности и сроков их хранения
РСБ.2	Определение состава и содержания информации о подлежащих регистрации событиях безопасности
РСБ.3	Обеспечение сбора, записи и хранения информации о событиях безопасности в течение установленного срока хранения
РСБ.4	Реагирование на сбои регистрации событий безопасности (аппаратные и программные ошибки, сбои в механизмах регистрации событий, переполнение объема памяти)
РСБ.5	Мониторинг результатов регистрации событий безопасности и реагирование на них
РСБ.6	Синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Обеспечение антивирусной защиты
АВЗ.2	Обеспечение актуальности базы данных признаков вредоносного программного обеспечения
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обеспечение актуальности базы решающих правил
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Идентификация, анализ уязвимостей информационной системы и своевременное устранение выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения и средств защиты информации
АНЗ.3	Контроль работоспособности, настроек и правильности функционирования приложений и средств защиты информации
АНЗ.4	Контроль состава аппаратного и программного обеспечения и средств защиты информации
АНЗ.5	Контроль исполнения правил заведения и удаления учетных записей, генерации и смены паролей, реализации правил разграничения доступом пользователей в информационной системе
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, в том числе средств защиты информации
ОЦЛ.2	Контроль целостности информации, хранящейся в базах данных
ОЦЛ.3	Обеспечение восстановления программного обеспечения и средств защиты информации в случае возникновения аварийной ситуации

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в информационных системах
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
ОЦЛ.6	Ограничение прав пользователей на ввод информации в информационную систему
X. Обеспечение доступности информации (ОДТ)	
ОДТ.1	Использование отказоустойчивых технических средств
ОДТ.2	Резервирование технических и программных средств, каналов передачи данных, средств обеспечения функционирования информационной системы
ОДТ.3	Контроль стабильного функционирования технических средств, своевременное обнаружение и локализация отказов функционирования, восстановление отказавших средств
ОДТ.4	Резервное копирование критической информации на машинные носители информации
ОДТ.5	Обеспечение возможности восстановления критической информации с машинных носителей в течение установленных сроков
ОДТ.7	Контроль состояния и качества предоставления вычислительных ресурсов, в том числе по передаче информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов и объектов доступа в виртуальной среде
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной среде
ЗСВ.3	Обеспечение регистрации событий безопасности в виртуальной инфраструктуре
ЗСВ.4	Управление (маршрутизация, фильтрация, однонаправленная передача, контроль соединений) потоками информации между компонентами виртуальной среды
ЗСВ.6	Управление перемещением виртуальных машин и обрабатываемых на них данных
ЗСВ.7	Контроль целостности виртуальной среды и ее конфигураций
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9	Реализация антивирусной защиты в виртуальной среде
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты для обработки информации отдельным пользователем или группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.2	Создание контролируемой зоны, в которой размещаются стационарные технические средства системы и средства обеспечения их функционирования
ЗТС.3	Ограничение доступа посторонних лиц к техническим средствам системы, средствам обеспечения их функционирования и в помещения, в которых такие средства установлены
ЗТС.4	Размещение устройств отображения информации, исключающее ее неправомерный просмотр

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в информационных системах
ЗТС.5	Защита технических средств от внешних воздействий, таких как нестабильность электропитания, температура и других воздействий окружающей среды
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.1	Разделение в информационной системе функций по администрированию информационной системы, администрированию системы защиты, обработке информации и других функций информационной системы
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания при ее передаче по каналам связи, выходящим за пределы контролируемой зоны или по беспроводным каналам связи
ЗИС.5	Запрет неправомерной удаленной активации видеокамер, микрофонов и других периферийных устройств, которые возможно активировать удаленно, и оповещение пользователей об активации этих устройств
ЗИС.7	Контроль правомерного и исключение неправомерного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.8	Контроль правомерного и исключение неправомерного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи
ЗИС.9	Контроль правомерной и исключение неправомерной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации
ЗИС.11	Обеспечение подлинности сетевых соединений для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Обеспечение невозможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Обеспечение невозможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита данных, не подлежащих изменению в ходе обработки информации, таких как параметры и настройки средств защиты информации и другого программного обеспечения
ЗИС.17	Разбиение информационной системы на сегменты и обеспечение защиты периметров этих сегментов
ЗИС.20	Защита беспроводных соединений, используемых в информационной системе
ЗИС.21	Исключение возможности доступа пользователя к информации, созданной в результате действий предыдущего пользователя через реестры, оперативную память и другие общие ресурсы
ЗИС.22	Защита аппаратных и программных средств информационной системы от угроз типа «отказ в обслуживании»
ЗИС.23	Защита периметра информационной системы при ее взаимодействии с другими информационными системами и информационно-телекоммуникационными сетями

Продолжение таблицы 10

Условное обозначение и номер меры	Меры защиты информации в информационных системах
ЗИС.24	Прерывание сетевых соединений по истечении заданного администратором срока неактивности
ЗИС.30	Защита мобильных средств, используемых в информационной системе

7.2.2 Адаптация базового набора мер защиты информации.

Адаптация базового набора защитных мер, как правило, подразумевает исключение из базового набора мер, непосредственно связанных с не используемыми в информационной системе информационными технологиями.

В результате адаптации базового набора были исключены следующие защитные меры:

- ИАФ.6 в связи с отсутствием в закрытом информационном контуре внешних пользователей;
- УПД.13-УПД.16, ЗИС.23, СОВ.1-СОВ.2, ОЦЛ.4, ОДТ.7 в связи с отсутствием в закрытом информационном контуре подключений к внешним сетям;
- ЗСВ.1-ЗСВ.10 в связи с отсутствием в закрытом информационном контуре технологий виртуализации;
- ЗИС.3, ЗИС.20 в связи с отсутствием в закрытом информационном контуре беспроводных каналов связи, а также проводных каналов связи, имеющих выход за пределы контролируемой зоны;
- ЗИС.5, ЗИС.7-ЗИС.9 в связи с отсутствием в информационной системе технологий передачи речи и видеоинформации;
- ЗИС.30 в связи с отсутствием в информационной системе мобильных средств.

7.2.3 Уточнение адаптированного базового набора мер защиты информации.

Уточнение адаптированного базового набора защитных мер проводится с учетом оценки возможности адаптированного базового набора защитных проти-

востоять всем угрозам безопасности информации, актуальным для данной информационной системы.

В результате уточнения адаптированного базового набора были добавлены защитные меры, приведенные в таблице 11.

Таблица 11 - Защитные меры, добавленные в результате уточнения адаптированного базового набора

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Обоснование
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	Добавлены в связи с широким применением машинных носителей для хранения конфиденциальной информации. Направлены на снижение вероятности реализации угроз несанкционированного доступа к конфиденциальной информации.
ЗНИ.4	Исключение возможности неправомерного ознакомления с информацией, хранящейся на машинных носителях, или использования носителей информации в других информационных системах	
ЗНИ.7	Контроль подключения машинных носителей информации	
XII. Защита технических средств (ЗТС)		
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам	Добавлена для защиты от угроз утечки видовой информации, угроз утечки информации по каналу ПЭМИН

7.2.4 Дополнение уточненного адаптированного базового набора мер защиты информации.

Дополнение уточненного адаптированного базового набора мер защиты информации не требуется, поскольку никакими нормативными актами и политикой обеспечения безопасности информации организации не установлены дополнительные требования.

7.3 Определение необходимых средств защиты информации

Итоговый перечень требуемых защитных мер приведет в таблице 12. Кроме того, для всех защитных мер в таблице 12 определены средства, которыми они реализуются.

Таблица 12 - Итоговый перечень требуемых защитных мер

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Чем обеспечивается
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся сотрудниками оператора	СЗИ от НСД, АПМДЗ
ИАФ.2	Идентификация и аутентификация стационарных, мобильных и портативных устройств	СЗИ от НСД
ИАФ.3	Управление идентификаторами (создание, присвоение, уничтожение)	СЗИ от НСД, АПМДЗ, организационные меры
ИАФ.4	Управление средствами аутентификации (выдача, регистрация, блокирование) и принятие мер в случае утраты и (или) компрометации средств аутентификации	СЗИ от НСД, АПМДЗ, организационные меры
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	СЗИ от НСД, АПМДЗ
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление учетными записями внутренних и внешних пользователей (заведение, активация, блокирование и уничтожение)	СЗИ от НСД, АПМДЗ
УПД.2	Реализация необходимых методов (дискреционный, ролевой, мандатный), типов (запись, чтение, выполнение или другой тип) и правил разграничения доступа	СЗИ от НСД
УПД.3	Управление (фильтрация, маршрутизация, односторонняя передача, контроль соединений и другие способы управления) информационными потоками между устройствами, сегментами информационной системы, между информационными системами	СЗИ от НСД
УПД.4	Разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	СЗИ от НСД
УПД.5	Назначение пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых прав и привилегий	организационные меры
УПД.6	Ограничение попыток входа в информационную систему	СЗИ от НСД, АПМДЗ
УПД.9	Ограничение числа одновременных сеансов доступа для всех пользователей информационной системы	СЗИ от НСД
УПД.10	Прекращение сеанса доступа в систему после установленного времени бездействия пользователя или по его запросу	СЗИ от НСД, АПМДЗ
УПД.11	Управление действиями пользователей, разрешенными до идентификации и аутентификации	СЗИ от НСД, АПМДЗ
УПД.17	Обеспечение доверенной загрузки СВТ	АПМДЗ
III. Ограничение программной среды (ОПС)		

Продолжение таблицы 12

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Чем обеспечивается
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	СЗИ от НСД
ОПС.2	Управление установкой компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	Сканер безопасности
ОПС.3	Установка только разрешенного к использованию программного обеспечения и его компонентов	Сканер безопасности, организационные меры
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет машинных носителей информации	СЗИ от НСД, организационные меры
ЗНИ.2	Контроль доступа к машинным носителям информации	СЗИ от НСД, организационные меры
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	организационные меры
ЗНИ.4	Исключение возможности неправомерного ознакомления с информацией, хранящейся на машинных носителях, или использования носителей информации в других информационных системах	СЗИ от НСД, организационные меры
ЗНИ.5	Контроль использования интерфейсов ввода и вывода информации на машинные носители информации	СЗИ от НСД
ЗНИ.7	Контроль подключения машинных носителей информации	СЗИ от НСД
ЗНИ.8	Уничтожение информации на машинных носителях при передаче их между пользователями или в сторонние организации (например для ремонта или утилизации)	СЗИ от НСД, организационные меры
V. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение подлежащих регистрации событий безопасности и сроков их хранения	СЗИ от НСД, АПМДЗ
РСБ.2	Определение состава и содержания информации о подлежащих регистрации событиях безопасности	СЗИ от НСД
РСБ.3	Обеспечение сбора, записи и хранения информации о событиях безопасности в течение установленного срока хранения	СЗИ от НСД, АПМДЗ
РСБ.4	Реагирование на сбои регистрации событий безопасности (аппаратные и программные ошибки, сбои в механизмах регистрации событий, переполнение объема памяти)	СЗИ от НСД, АПМДЗ
РСБ.5	Мониторинг результатов регистрации событий безопасности и реагирование на них	СЗИ от НСД, АПМДЗ

Продолжение таблицы 12

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Чем обеспечивается
РСБ.6	Синхронизация системного времени в информационной системе	СЗИ от НСД
РСБ.7	Защита информации о событиях безопасности	СЗИ от НСД, АПМДЗ
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Обеспечение антивирусной защиты	САЗ
АВЗ.2	Обеспечение актуальности базы данных признаков вредоносного программного обеспечения	САЗ
VIII. Контроль (анализ) защищенности информации (АНЗ)		
АНЗ.1	Идентификация, анализ уязвимостей информационной системы и своевременное устранение выявленных уязвимостей	сканер безопасности, организационные меры
АНЗ.2	Контроль установки обновлений программного обеспечения и средств защиты информации	сканер безопасности, организационные меры
АНЗ.3	Контроль работоспособности, настроек и правильности функционирования приложений и средств защиты информации	СЗИ от НСД, АПМДЗ, организационные меры
АНЗ.4	Контроль состава аппаратного и программного обеспечения и средств защиты информации	СЗИ от НСД, АПМДЗ, организационные меры
АНЗ.5	Контроль исполнения правил заведения и удаления учетных записей, генерации и смены паролей, реализации правил разграничения доступом пользователей в информационной системе	СЗИ от НСД, организационные меры
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.1	Контроль целостности программного обеспечения, в том числе средств защиты информации	СЗИ от НСД, АПМДЗ
ОЦЛ.2	Контроль целостности информации, хранящейся в базах данных	СЗИ от НСД, АПМДЗ
ОЦЛ.3	Обеспечение восстановления программного обеспечения и средств защиты информации в случае возникновения аварийной ситуации	СЗИ от НСД, АПМДЗ, средство резервного копирования
ОЦЛ.6	Ограничение прав пользователей на ввод информации в информационную систему	СЗИ от НСД
X. Обеспечение доступности информации (ОДТ)		
ОДТ.1	Использование отказоустойчивых технических средств	организационные меры

Продолжение таблицы 12

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Чем обеспечивается
ОДТ.2	Резервирование технических и программных средств, каналов передачи данных, средств обеспечения функционирования информационной системы	СЗИ от НСД, организационные меры
ОДТ.3	Контроль стабильного функционирования технических средств, своевременное обнаружение и локализация отказов функционирования, восстановление отказавших средств	СЗИ от НСД, организационные меры
ОДТ.4	Резервное копирование критической информации на машинные носители информации	организационные меры
ОДТ.5	Обеспечение возможности восстановления критической информации с машинных носителей в течение установленных сроков	средство резервного копирования, организационные меры
XII. Защита технических средств (ЗТС)		
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам	технические меры
ЗТС.2	Создание контролируемой зоны, в которой размещаются стационарные технические средства системы и средства обеспечения их функционирования	организационные меры
ЗТС.3	Ограничение доступа посторонних лиц к техническим средствам системы, средствам обеспечения их функционирования и в помещения, в которых такие средства установлены	организационные меры
ЗТС.4	Размещение устройств отображения информации, исключаящее ее неправомерный просмотр	организационные меры
ЗТС.5	Защита технических средств от внешних воздействий, таких как нестабильность электропитания, температура и других воздействий окружающей среды	организационно-технические меры
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.1	Разделение в информационной системе функций по администрированию информационной системы, администрированию системы защиты, обработке информации и других функций информационной системы	организационные меры
ЗИС.11	Обеспечение подлинности сетевых соединений для защиты от подмены сетевых устройств и сервисов	СЗИ от НСД
ЗИС.12	Обеспечение невозможности отрицания пользователем факта отправки информации другому пользователю	СЗИ от НСД
ЗИС.13	Обеспечение невозможности отрицания пользователем факта получения информации от другого пользователя	СЗИ от НСД
ЗИС.15	Защита данных, не подлежащих изменению в ходе обработки информации, таких как параметры и настройки средств защиты информации и другого программного обеспечения	СЗИ от НСД, АПМДЗ

Продолжение таблицы 12

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Чем обеспечивается
ЗИС.17	Разбиение информационной системы на сегменты и обеспечение защиты периметров этих сегментов	СЗИ от НСД, организационные меры
ЗИС.21	Исключение возможности доступа пользователя к информации, созданной в результате действий предыдущего пользователя через реестры, оперативную память и другие общие ресурсы	СЗИ от НСД
ЗИС.22	Защита аппаратных и программных средств информационной системы от угроз типа «отказ в обслуживании»	организационные меры
ЗИС.24	Прерывание сетевых соединений по истечении заданного администратором срока неактивности	СЗИ от НСД

Таким образом, система закрытого информационного контура будет иметь вид, представленный на рисунке 5.



Рисунок 5 - Система защиты информации в закрытом информационном контуре

8 Сравнительный анализ и выбор системы защиты информации закрытого информационного контура

8.1 Выбор системы защиты информации от несанкционированного доступа

8.1.1 Общие сведения о системах защиты информации от несанкционированного доступа.

Система защиты информации от несанкционированного доступа (СЗИ от НСД) представляет собой комплекс программных или программно-аппаратных средств, исключающих или существенно затрудняющих несанкционированный доступ к конфиденциальной информации. Основными функциями таких продуктов является обеспечение независимо от операционной системы идентификации и аутентификации пользователей, контроль доступа пользователей к информации, контроль целостности, управление подключенными устройствами и т.п.

Современный рынок средств защиты информации от несанкционированного доступа представлен различными программными и программно-аппаратными комплексами. Продукты различаются по цене, функциональности и настройкам. Наиболее популярными СЗИ от НСД, имеющими сетевые версии, являются Secret Net, Страж NT и Dallas Lock.

8.1.2 Secret Net - сертифицированная система защиты информации от несанкционированного доступа для АРМ под управлением операционной системы Windows компании ООО «Код безопасности». Последней версией на момент написания работы является Secret Net 7.7. 635. Основные возможности актуальной версии по данным, представленным разработчиком:

- усиленная аутентификация пользователей по паролю и/или электронному идентификатору. Поддерживаются eToken PRO, eToken PRO (Java), iKey, Rutoken S, Rutoken ЭЦП, Rutoken Lite, JaCarta, ESMART и iButton;
- централизованное управление паролями и идентификаторами пользователей, имеющих доступ к компьютерам с установленной СЗИ Secret Net LSP (версия для Linux);

- полномочное управление доступом пользователей к файлам и ресурсам системы на основе их конфиденциальности и прав доступа пользователя;
- контроль печати и отчуждение информации ограниченного доступа;
- теневое копирование отчуждаемой информации;
- замкнутая программная среда;
- гарантированное уничтожение данных на накопителях;
- программное обеспечение доверенной загрузки;
- контроль целостности системных файлов;
- самодиагностика подсистем Secret Net;
- централизованное управление параметрами СЗИ, мониторинг и аудит;
- управление политиками и учетными записями пользователей без необходимости внесения изменений в Active Directory;
- поддержка систем управления базами данных Oracle Database и MS SQL Server;
- мониторинг в реальном времени с возможностью просмотра состояния отдельных АРМ, серверов с учетом критичности событий;
- контроль неизменности аппаратной конфигурации АРМ в процессе работы;
- широкие возможности по работе с журналами безопасности и формирование различных отчетов о состоянии системы;
- возможность взаимодействия с компьютерами под управлением ОС Linux, защищенных Secret Net LSP;
- широкие возможности по контролю внешних устройств;
- разграничение доступа к принтерам;
- ограничение возможности печати документов определенного уровня конфиденциальности на конкретном принтере;
- теневое копирование и маркировка печатаемых документов;
- работа в терминальном режиме;
- работа в виртуальных инфраструктурах.

СЗИ от НСД Secret Net 7 имеет сертификат ФСТЭК, позволяющий использовать ее для защиты АС до класса 1Б включительно, ИСПДн до 1 уровня защищенности включительно и ГИС до 1 класса включительно.

Стоимость для одного АРМ составляет 8195 рублей [16].

Компания ООО «Код безопасности» с апреля 2018 года прекращает продажи Secret Net 7 и переходит на расширенную версию Secret Net Studio. Стоит отметить, что поддержка Secret Net 7 не прекратиться, пользователи будут получать актуальные обновления и исправления.

Secret Net Studio представляет собой комплексное решение для защиты автоматизированных рабочих мест и серверов на уровне приложений, сети, операционной системы и периферийного оборудования. Актуальной версией на момент написания статьи является Secret Net 8.2.1156.

Помимо возможностей Secret Net 7 в Secret Net Studio имеются следующие возможности:

- антивирусная защита серверов и АРМ с использованием технологий ESET;
- возможность выполнения антивирусной проверки по расписанию, а также по требованию администратора или пользователя;
- межсетевое экранирование;
- контроль сетевой активности АРМ;
- фильтрация трафика по различным протоколам в соответствии с заданными политиками для отдельных приложений и пользователей;
- режим обучения межсетевого экрана с возможностью автоматической генерации правил;
- обнаружение подозрительной активности приложений;
- широкие настройки правил защиты для отдельных приложений и групп приложений;
- обнаружение сетевых атак сигнатурными и эвристическими методами;
- автоматическая блокировка атакующих хостов при обнаружении аномальных пакетов, сканировании портов, DoS-атаках;

- создание защищенного соединения с удаленными компьютерами;
- шифрование контейнеров данных любого размера по алгоритму ГОСТ 28147-89, гарантирующее защиту данных в случае несанкционированного доступа к носителям информации, их утери или кражи;
- использование аппаратных идентификаторов для доступа к шифрованным контейнерам;
- размещение шифрованных контейнеров на съемных носителях или жестком диске;
- централизованная установка продукта на АРМ контролируемого домена;
- настройка сквозных и групповых политик для всех защитных механизмов производится с помощью единого агента безопасности;
- групповой мониторинг работы;
- расследование инцидентов безопасности.

СЗИ от НСД Secret Net Studio имеет сертификат ФСТЭК, позволяющий использовать ее для защиты АС до класса 1Г включительно, ИСПДн до 1 уровня защищённости включительно, ГИС до 1 класса включительно.

Стоимость для одного АРМ составляет 10875 рублей. При этом срок действия для модулей «Антивирус» и «СОВ» - 1 год. Продление данных модулей на год обойдется в 1775 рублей для одного АРМ [17].

8.1.3 Страж NT - система защиты информации от несанкционированного доступа компании ООО «Рубинтех», предназначенная для использования в многопользовательских информационных системах, построенных на базе персональных ЭВМ.

Основные возможности актуальной на момент написания работы версии Страж NT 4.0 по данным разработчика:

- усиленная аутентификация до начала загрузки операционной системы с использованием различных аппаратных идентификаторов (USB-идентификаторов Guardant ID, Рутокен, eToken, JaCarta, ESMART Token, смарт-карт Рутокен, eToken, JaCarta, ESMART, электронных ключей iButton, дискет 3,5»);

- дискреционное управление доступом к ресурсам системы;
- мандатное управление доступом к ресурсам системы;
- одновременная работа с документами, имеющими разные грифы, в одном сеансе;
- замкнутая программная среда для пользователей, в которой им разрешен запуск только определенных приложений;
- регистрация всех событий безопасности, в том числе действий администратора;
- нанесение грифа на печатаемые документы независимо от печатающего приложения;
- гарантированная очистка оперативной памяти и файла подкачки;
- гарантированное удаление файлов, содержащих конфиденциальную информацию;
- контроль целостности системных ресурсов и компонентов системы защиты информации;
- широкие возможности по управлению пользователями, внешними носителями информации и устройствами;
- тестирование и самодиагностика системы защиты информации;
- поддержка сетевого развёртывания;
- настройка системы защиты с любого автоматизированного рабочего места в сети;
- поддержка последних версий операционных систем Microsoft Windows;
- возможность работы в терминальном режиме;
- широкие возможности настройки подсистемы регистрации событий и замкнутой программной среды;
- возможность экспорта настроек системы защиты для автоматического применения их на другом АРМ;
- поддержка UEFI;
- автоматическая архивация журналов событий и настроек системы защиты;

- поддержка аппаратных средств доверенной загрузки;
- формирование различных отчетов о событиях безопасности настройках системы защиты;
- возможность аварийного восстановления работоспособности компьютера с помощью специального диска восстановления в случае выхода из строя либо утраты электронных идентификаторов, паролей.

СЗИ от НСД Страж NT имеет сертификат ФСТЭК, позволяющий использовать ее для защиты АС до класса 1Б включительно, ИСПДн до 1 уровня защищенности включительно, ГИС до 1 класса включительно.

Стоимость для одного АРМ составляет 7750 рублей [18].

8.1.4 Dallas Lock - программный комплекс средств защиты информации от несанкционированного доступа компании ООО «Конфидент», предназначенный для работы в ОС Windows, с возможностью подключения аппаратных идентификаторов.

Основные возможности актуальной на момент написания работы версии Dallas Lock 8.0-К (редакция К предназначена для защиты конфиденциальной информации, не составляющей государственную тайну) по данным разработчика:

- усиленная идентификация пользователей с использованием электронных идентификаторов (USB-Flash-накопителей, электронных ключей iButton, USB-ключей Aladdin eToken Pro/Java, Rutoken (Рутокен), смарт-карт Aladdin eToken Pro/SC, JaCarta, ESMART Token, NFC-меток);
- разграничение прав доступа пользователей при работе на АРМ;
- разграничение доступа к внешним носителям как по их типу, так и к конкретным экземплярам;
- теневое копирование файлов, отправляемых на съемные накопители;
- блокировка компьютера при отключении аппаратного идентификатора пользователя;
- гибкие настройки парольной политики;
- проверка количества активных сессий для конкретной учетной записи пользователя в настоящий момент на текущем компьютере;

- авторизация пользователя до загрузки ОС (реализуется отдельным модулем «Загрузчик DL»);
- дискреционный принцип управления доступом к ресурсам системы и файлам;
- мандатный принцип управления доступа к ресурсам системы и файлам;
- замкнутая программная среда;
- автоматическая настройка мандатного доступа;
- возможность включения вместо стандартной графической оболочки Windows защищенной оболочки Dallas Lock;
- разграничение доступа для процессов к буферу обмена;
- проверка целостности системных ресурсов и аппаратной конфигурации при загрузке, по расписанию, по требованию администратора;
- проверка целостности объектов файловой системы при загрузке, по расписанию, по требованию администратора;
- блокировка входа в ОС компьютера при обнаружении нарушения целостности;
- восстановление системных файлов и веток реестра в случае выявления нарушения их целостности;
- очистка остаточной информации;
- ведение 11-и различных электронных журналов, в которых фиксируются все действия пользователей;
- добавление штампов на распечатываемые с данного компьютера документы;
- разграничение доступа к возможности печати;
- преобразование передаваемых по каналам связи данных в файл-контейнер, расшифровать который может только другой компьютер с Dallas Lock 8.0;
- шифрование данных на жестких дисках;
- удаленное администрирование;
- самодиагностика основного функционала СЗИ;
- экспорт конфигурации;

– межсетевое экранирование.

СЗИ от НСД Dallas Lock 8.0 имеет сертификат ФСТЭК, позволяющий использовать ее для защиты АС до класса 1Г включительно, ИСПДн до 1 уровня защищенности включительно и ГИС до 1 класса включительно.

Стоимость для одного АРМ составляет 8900 рублей [19].

8.1.5 Сравнение рассматриваемых СЗИ от НСД.

Сравнение основных характеристик актуальных на момент написания статьи версий рассматриваемых СЗИ от НСД приведено в таблице 13. Представленные цены могут варьироваться в зависимости от поставщика и комплектации.

Таблица 13 - Сравнение основных возможностей СЗИ от НСД

Возможность	СЗИ от НСД			
	Secret Net 7	Secret Net Studio	Страж NT	Dallas Lock
Усиленная идентификация и аутентификация пользователей	+	+	+	+
Дискреционное управление доступом	+	+	+	+
Мандатное (полномочное) управление доступом	+	+	+	+
Обеспечение доверенной загрузки (аутентификация до загрузки ОС)	+	+	+	+
Замкнутая программная среда	+	+	+	+
Контроль машинных носителей информации	+	+	+	+
Регистрация событий безопасности	+	+	+	+
Антивирусная защита	-	+	-	-
Система обнаружения вторжений	-	+	-	+
Контроль целостности системных ресурсов и аппаратной конфигурации	+	+	+	+
Шифрование контейнеров жесткого диска	-	+	-	+
Межсетевое экранирование	-	+	-	+
Удаленное управление	-	+	+	+
Возможность сетевого развертывания	+	+	+	+
Возможность экспорта настроек системы защиты	+	+	+	+
Номер сертификата ФСТЭК	2707	3745	3553	2720
Срок действия сертификата	07.09.2018	16.05.2020	20.04.2019	25.09.2018
Класс защищаемых АС	1Б	1Г	1Б	1Г
Уровень защищаемых ИСПДн	1	1	1	1
Класс защищаемых ГИС	1	1	1	1
Цена на 1 АРМ	8195	10875	7750	8900

Как видно из таблицы, все продукты примерно равны по характеристикам. Secret Net Studio является наиболее функциональным продуктом из представленных. Помимо стандартных функций защиты от НСД он содержит в себе функции системы обнаружения вторжений, межсетевого экрана и антивируса, что весьма удобно. Dallas Lock уступает отсутствием антивирусной защиты, зато дает возможность отказаться от встроенной системы обнаружения вторжений и (или) межсетевого экрана в пользу сторонних производителей. Страж NT и Secret Net 7 выполняют только функции защиты от НСД, что может позволить сэкономить, когда не нужны такие функции как система обнаружения вторжений и (или) межсетевой экран, например в случае, когда компьютер не подключен ни к каким сетям.

8.2 Выбор АПМДЗ

8.2.1 Общие сведения об АПМДЗ.

Доверенная загрузка - это обеспечение загрузки операционной системы только с заранее определенного носителя (например, конкретного жесткого диска) с предварительной идентификацией и аутентификацией пользователя и проверкой целостности аппаратных и программных средств.

Идентификация и аутентификация пользователя может осуществляться как с помощью логина и пароля, так и с помощью аппаратных идентификаторов. При этом хранение идентификационных данных (ключей, контрольных сумм) выполняется на базе аппаратных средств.

Аппаратно-программные модули доверенной загрузки имеют следующие преимущества перед программными:

- собственная аппаратная база для выполнения алгоритмов защиты и шифрования;
- невозможность запустить ПК без вскрытия;
- невозможность запуска ПК при извлечении АПМДЗ за счет шифрования загрузочного сектора.

Наиболее распространенными отечественными АПМДЗ, имеющими сертификацию органов ФСТЭК, на сегодняшний день являются АПМДЗ «МАКСИМ-М1», «Криптон-замок», «Блокхост-АМДЗ 2.0», «Соболь».

8.2.2 АПМДЗ «Максим-М1» компании АО «НПО РусБИТех».

АПМДЗ «Максим-М1» - аппаратно-программный модуль доверенной загрузки, который может использоваться на территории Российской Федерации в качестве средства защиты от НСД к техническим, программным и информационным ресурсам ПЭВМ, обрабатывающих конфиденциальную информацию, в том числе содержащую сведения, составляющие государственную тайну, со степенью секретности до «совершенно секретно» включительно.

АПМДЗ «Максим-М1» имеет следующие основные возможности:

- двухфакторная идентификацию и аутентификация пользователей до передачи управления ОС с использованием электронных идентификаторов iButton;
- ведение журнала событий безопасности в собственной энергонезависимой памяти;
- контроль сроков действия ключей с использование часов с автономным питанием;
- контроль целостности оперативной памяти, загрузочных секторов жестких дисков и значений реестра Windows;
- физический датчик случайных чисел для формирования пароля аутентификации.

АПМДЗ «Максим-М1» может применяться в системах обработки персональных данных до 1 уровня защищенности, государственных информационных системах до 1 класса защищенности и автоматизированных системах до класса 1Б включительно [20].

8.2.3 АПМДЗ «Криптон-замок» компании ООО «Анкад».

АПМДЗ «Криптон-замок» - сертифицированный аппаратно-программный комплекс, предназначенный для обеспечения контроля доступа пользователей к серверам и АРМ, на которых будет обрабатываться информация ограниченного доступа.

Основные возможности АПМДЗ «Криптон-замок»:

- двухфакторная идентификация и аутентификация пользователя до запуска BIOS компьютера с использованием электронного идентификатора iButton или смарт-карты собственного производства;
- аппаратная защита от несанкционированной загрузки операционной системы с гибких дисков, USB устройств и других съемных носителей;
- контроль целостности установленной на компьютере программной среды под любые ОС, использующие файловые системы NTFS, FAT12, FAT16, FAT32, EXT2, EXT3;
- блокировка компьютера при обнаружении попытки НСД или извлечении модуля;
- регистрация событий безопасности и ведение электронного журнала событий в собственной энергонезависимой памяти;
- аппаратный датчик случайных чисел;
- защита от электрического воздействия на тракт ввода идентифицирующей информации.

Продукт сертифицирован по требованиям ФСБ к аппаратно-программным модулям доверенной загрузки ЭВМ и дополнению к ним по классу защиты 1Б. Сертификата ФСТЭК не имеет [21].

8.2.4 ПАК «Блокхост-АМДЗ 2.0» компании ООО «Газинформсервис».

Аппаратно-программный комплекс «Блокхост-АМДЗ 2.0» предназначен для обеспечения доверенной загрузки операционных систем семейства Windows и Linux. Комплекс позволяет предотвратить несанкционированный доступ к программным и техническим ресурсам компьютера до загрузки операционной системы.

Основные возможности ПАК «Блокхост-АМДЗ 2.0»:

- идентификация и аутентификация пользователей до загрузки ОС с использованием паролей и (или) персональных идентификаторов iButton, SafeNet eToken, eToken, ESMART Token, JaCarta, USB, Рутокен-ЭЦП;

- контроль неизменности системных файлов и файлов пользователей, объектов реестра ОС Windows, загрузочных секторов устройств хранения данных и аппаратной конфигурации ЭВМ до загрузки ОС;
- регистрация всех действий пользователей и администратора безопасности в журнале аудита.;
- блокировка загрузки ОС при обнаружении попыток обхода процедуры доверенной загрузки с помощью аппаратного сторожевого таймера;
- локальное и удаленное администрирование политик безопасности комплекса;
- блокировка загрузки ОС при нарушении установленных политик безопасности.

ПАК «Блокхост-АМДЗ 2.0» является средством доверенной загрузки уровня платы расширения 2 класса защиты согласно «Требованиям к средствам доверенной загрузки», что позволяет его использовать для защиты ГИС 1 класса защищенности [22].

8.2.5 ПАК «Соболь» компании ООО «Код Безопасности».

ПАК «Соболь» представляет собой аппаратно-программный модуль доверенной загрузки, обеспечивающий защиту от несанкционированного доступа до загрузки ОС.

Основные возможности ПАК «Соболь»:

- идентификация и аутентификация пользователей с использованием персональных электронных идентификаторов, таких как iButton, Rutoken, Rutoken RF, iKey 2032, eToken PRO и смарт-карты eToken PRO, до загрузки операционной системы;
- запрет загрузки с внешних носителей (USB, FDD, DVD/CD-ROM, LPT, SCSI-порты и др.);
- регистрация попыток доступа к компьютеру и хранение журнала в специальной энергонезависимой памяти;
- блокировка доступа к компьютеру при обнаружении попытки отключения ПАК «Соболь» (механизм сторожевого таймера);

- контроль целостности программной среды и реестра Windows;
- контроль аппаратной конфигурации компьютера.;
- аппаратный датчик случайных чисел.

ПАК «Соболь» может применяться в системах обработки персональных данных до 1 уровня защищенности, государственных информационных системах до 1 класса защищенности и автоматизированных системах до класса 1Б включительно [23].

8.2.7 Сравнение рассматриваемых АПМДЗ.

Сравнение основных характеристик рассматриваемых АПМДЗ приведено в таблице 14. Представленные цены могут варьироваться в зависимости от поставщика и комплектации.

Таблица 14 - Сравнение основных характеристик рассматриваемых АПМДЗ

Возможность	АПМДЗ			
	АПМДЗ «Максим-М1»	АПМДЗ «Криптон- замок»	ПАК «Блокхост- АМДЗ 2.0»	ПАК «Соболь»
Усиленная идентификация и аутентификация	+	+	+	+
Защита от загрузки с внешних носителей	+	+	+	+
Регистрация событий	+	+	+	+
Аппаратный датчик случайных чисел	+	+	+	+
Контроль целостности аппаратной конфигурации	+	-	+	+
Контроль целостности программной среды	+	+	+	+
Сторожевой таймер	+	-	+	+
Встроенная энергонезависимая память	+	+	+	+
Наличие версии для ноутбука	-	+	+	+
Номер сертификата ФСТЭК	3732	Не имеет	3700	1574
Срок действия сертификата	12.04.2020	-	08.02.2020	14.03.2020
Класс защищаемых АС	1Б	-	1Б	1Б
Уровень защищаемых ИС-ПДн	1	-	1	1
Класс защищаемых ГИС	1	-	1	1
Цена на 1 АРМ	16697	13700	10000	10350

Как видно из таблицы, модули имеют одинаковый основной функционал. Не все производители включают в свой модельный ряд версию для ноутбуков. Также продукты отличаются поддерживаемыми электронными идентификаторами. Поэтому вопрос о выборе аппаратно-программного модуля доверенной загрузки решается либо на основе предпочтений к тому или иному производителю, либо на основе взаимоотношений с поставщиками. Например, при использовании в системе продукции компании Код безопасности целесообразно использовать ПАК «Соболь» ее же производства для лучшей совместимости и удобства технической поддержки и обслуживания.

8.3 Выбор средств защиты от несанкционированного доступа.

Из рассматриваемых СЗИ от НСД наиболее распространенной является Secret Net Studio. Кроме того, помимо возможностей защиты от несанкционированного доступа, она может выполнять возможности межсетевого экрана, системы обнаружения вторжений и антивируса. С учетом того, при этом стоимость данного продукта не сильно выше стоимости конкурентов, Secret Net Studio является оптимальным выбором для закрытого информационного контура.

Поскольку рассматриваемые АМПДЗ, как сказано выше, имеют одинаковые возможности, определяющую роль при выборе играют стоимость и производитель. В закрытом информационном контуре решено применять ПАК «Соболь», поскольку он имеет сравнительно невысокую стоимость и при этом будет обладать наилучшей совместимостью с выбранной СЗИ от НСД Secret Net Studio.

9 Разработка комплекса организационно-технических мер защиты информации в закрытом информационном контуре

9.1 Организационные меры защиты информации

9.1.1 Общие сведения об организационных мерах.

Организационные меры защиты информации представляют собой мероприятия по защите информации, не требующие применения специальных технических средств. Они представляют собой регламентацию деятельности и взаимоотношений сотрудников, имеющих доступ к конфиденциальной информации, исключающую или существенно затрудняющую несанкционированное ознакомление с такой информацией. Организационные меры включают в себя:

- организацию режима охраны;
- регламентацию работы сотрудников с документами и техническими средствами;
- выявление и анализ новых угроз и уязвимостей информационной системы.

9.1.2 Организационные меры защиты информации в закрытом информационном контуре.

В соответствии с необходимым перечнем защитных мер, определенным в главе 7, в закрытом информационном контуре должны быть обеспечены следующие организационные меры защиты информации:

- должно быть регламентировано хранение, выдача, блокирование электронных идентификаторов операторов системы, а также определена ответственность в случае утраты и (или) компрометации таких идентификаторов или другой аутентифицирующей информации;
- должны быть однозначно определены и зафиксированы роли пользователей, их должностные обязанности и соответствующие им минимально необходимые права и привилегии;

- должен быть определен перечень лиц, допущенных к настройке системы, средств защиты информации, установке ПО (администратор информационной системы);
- должны быть организованы хранение, учет, выдача и прием машинных носителей информации. Машинные носители не должны перемещаться за пределы контролируемой зоны. Также должен быть определен перечень лиц, имеющих доступ к машинным носителям. При передаче машинного носителя в другую организацию (например для ремонта или утилизации) должно производиться полное стирание информации на нем;
- должна быть составлена экспертная группа для анализа и выявления новых уязвимостей и угроз.
- администраторы должны производить проверку работоспособности и состава технических и программных средств и установку обновлений с определенной периодичностью;
- должна быть определена и парольная политика для пользователей системы (требования к паролю, периодичность смены пароля). Администраторами должен обеспечиваться контроль за исполнением политики;
- должно контролироваться использование ресурсов системы пользователями по назначению;
- закупка программных и технических средств должна проводиться только у проверенных производителей;
- должно быть регламентировано резервное копирование критической информации на съемные носители и обеспечение восстановления такой информации в установленные сроки;
- должен быть ограничен доступ посторонних лиц в помещения, в которых установлены технические средства закрытого информационного контура, путем установки кодовых замков на двери таких помещений;
- все технические средства и каналы связи системы должны находиться в пределах контролируемой зоны;

- средства отображения информации (мониторы, принтеры) должны располагаться таким образом, чтобы был невозможен просмотр выводимой информации через окна.

Все перечисленные требования должны быть документально оформлены, сотрудники должны быть с ними ознакомлены. Также должна быть определена ответственность за нарушение данных требований и организован контроль за их соблюдением.

9.2 Технические меры защиты информации

9.2.1 Общие сведения о технических мерах.

Технические меры защиты информации представляют собой мероприятия, предусматривающие использование специальных технических средств и реализацию различных технических решений. В основном они направлены на закрытие технических каналов утечки информации путем ослабления уровня информативных сигналов или уменьшением отношения «сигнал/шум» в местах возможного размещения средств разведки. Технические меры проводятся с использованием пассивных и активных средств. К пассивным средствам защиты относятся:

- экранирование ОТСС и каналов связи;
- звукоизоляция выделенных помещений;
- использование устройств гарантированного питания ОТСС;
- установка помехоподавляющих фильтров в цепях электропитания и заземления.

К активным средствам относятся:

- средства пространственного зашумления (акустического и электромагнитного);
- использование подавителей диктофонов;
- линейное зашумление линий электропитания;

– уничтожение закладных устройств специальными генераторами импульсов.

9.2.2 Технические меры защиты информации в закрытом информационном контуре.

В соответствии с необходимым перечнем защитных мер, определенным в главе 7, в закрытом информационном контуре с помощью технических мер должна обеспечиваться защита информации от утечки по техническим каналам. Для этого необходимо применять следующие меры:

- оборудовать окна жалюзи для исключения утечки видовой информации;
- оборудовать входные двери в помещения с техническими средствами кодовыми замками и приспособлениями для опечатывания;
- оборудовать помещения с техническими средствами сигнализацией;
- оборудовать каждое АРМ источником бесперебойного питания;
- оборудовать помещения генераторами электромагнитного шума;
- использовать экранированные кабели для организации каналов связи между помещениями.

В закрытом информационном контуре допускается не применять средства защиты информации от утечки по акустическому каналу, поскольку в помещениях не будет вестись конфиденциальных переговоров, а помещения находятся в пределах контролируемой зоны и окна выходят на территорию организации.

Кроме того, в закрытом информационном контуре в соответствии с требованиями ФСТЭК не требуются средства криптографической защиты каналов связи, поскольку все они проводные и проходят внутри контролируемой зоны.

10 Выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации закрытого информационного контура

10.1 Выбор средства анализа защищенности

10.1.1 Общие сведения о средствах анализа защищенности.

Средства анализа защищенности (сканеры уязвимостей, сканеры безопасности) - это программные средства, служащие для диагностики и мониторинга систем защиты информации, позволяющие сканировать сети, компьютеры, приложения на предмет обнаружения возможных уязвимостей, а также устранять эти уязвимости.

Наиболее известными отечественными сканерами безопасности, имеющими сертификаты ФСТЭК, являются Redcheck и MaxPatrol.

10.1.2 Сканер безопасности Redcheck.

Сканер безопасности Redcheck компании ЗАО «АЛТЭКС-СОФТ» представляет собой комплексное решение для анализа защищенности и управления информационной безопасностью предприятия любого масштаба, обеспечивающее поиск и устранение уязвимостей, вызванных ошибками в коде программного обеспечения, некорректными настройками безопасности, слабостью парольной защиты, несанкционированной установкой программного и аппаратного обеспечения, несвоевременной установкой критических обновлений, нарушением политик информационной безопасности.

Основными возможностями актуальной на момент написания работы версии по данным разработчика являются:

- аудит уязвимостей;
- управление обновлениями;
- контроль конфигурации и оценка соответствия политикам и стандартам безопасности;
- аудит защищенности СУБД;

- аудит серверов приложений;
- аудит платформ виртуализации;
- инвентаризация сети;
- проверка сложностей паролей;
- формирование детализированных отчетов по каждому виду аудита.

Сканер безопасности Redcheck имеет сертификат ФСТЭК, позволяющий использовать его для защиты АС до класса 1Г включительно, ИСПДн до 1 уровня защищённости включительно, ГИС до 1 класса включительно.

Лицензия на использование программы для одного IP-адреса сроком на 1 год стоит 1440 рублей [24].

10.1.3 Сканер безопасности MaxPatrol 8.

Сканер безопасности MaxPatrol 8 компании ЗАО «Позитив Текнолоджиз» представляет собой систему, основанную на известном сканере сетевых уязвимостей XSpider (той же компании), существенно расширенном за счет добавления модуля анализа безопасности баз данных и модуля системных проверок. Сочетание в одном продукте функций сканера сетевой и системной безопасности, а также средств анализа защищенности СУБД и Web-приложений позволяет получить наиболее полную картину защищенности сети. Основным отличием данного сканера от других является то, что его не нужно разворачивать на узлах, все проверки осуществляются с использованием технологий удаленного администрирования.

Основными возможностями актуальной на момент написания работы версии по данным разработчика являются:

- автоматический мониторинг информационной безопасности;
- инвентаризация широкого спектра ресурсов, серверов приложений и СУБД, АРМ, сетевого оборудования и средств защиты;
- контроль обновлений популярных операционных систем, СУБД и приложений;
- управление обновлениями;
- анализ настроек и конфигураций;

- анализ прав доступа;
- проверка соответствия системы защиты международным стандартам или собственным политикам организации;
- контроль событий, таких как запуск критических модулей, создание или удаление пользователей, попытки НСД;
- формирование различных отчетов.

Сканер безопасности MaxPatrol 8 имеет сертификат ФСТЭК, позволяющий использовать его для защиты АС до класса 1Г включительно, ИСПДн до 1 уровня защищённости включительно, ГИС до 1 класса включительно.

Цена продукта зависит от количества контролируемых адресов [25].

10.1.4 Сравнение рассматриваемых сканеров безопасности.

Сравнение основных возможностей рассматриваемых сканеров безопасности приведено в таблице 15.

Таблица 15 - Сравнение основных возможностей рассматриваемых сканеров безопасности

Возможность	Сканер безопасности	
	Redcheck	MaxPatrol 8
Сканирование узлов	+	+
Сканирование СУБД	+	+
Сканирование Web-приложений	-	+
Системные проверки	+	+
Обнаружение уязвимостей	+	+
Контроль соблюдения политик	+	+
Управление обновлениями	+	+
Поддержка виртуализации	+	+
Исправление уязвимостей	+	+
Регистрация событий	+	+
Проверка актуальности антивирусных баз	-	+
Формирование отчетов	+	+
Номер сертификата ФСТЭК	3172	2922
Срок действия сертификата	23.06.2020	08.07.2019
Класс защищаемых АС	1Б	1Б
Уровень защищаемых ИСПДн	1	1
Класс защищаемых ГИС	1	1

Основной функционал рассматриваемых сканеров безопасности одинаковый. MaxPatrol имеет преимущество в виду наличия дополнительных функций, таких как проверка Web-приложений и проверка актуальности антивирусных баз. Несмотря на то, что MaxPatrol устанавливается в единственном экземпляре, его стоимость в пересчете на одно АРМ выше, чем стоимость Redcheck для одного АРМ, особенно с учетом скидок на него при покупке нескольких лицензий.

10.1.5 Выбор средства анализа защищенности.

Для использования в закрытом информационном контуре был выбран сканер безопасности Redcheck. Он обладает всем необходимым функционалом для выполнения требований по защите информации, но при этом цена на него ниже, чем цена конкурента. Кроме того, срок действия его сертификата ФСТЭК заканчивается позже.

10.2 Выбор средства резервного копирования

10.2.1 Общие сведения о средствах резервного копирования.

Резервное копирование - это создание копии данных на машинном носителе с целью восстановления этих данных в первоначальном или новом месте в случае повреждения или уничтожения. Резервное копирование необходимо для быстрого и недорогого восстановления программного обеспечения, настроек, документов в случае утраты рабочей копии по какой-либо причине.

Средства резервного копирования сами по себе не являются средствами защиты информации, но поскольку они используются для реализации некоторых из защитных мер, они должны быть сертифицированы ФСТЭК. На отечественном рынке представлены два сертифицированных решения для резервного копирования: Acronis Backup & Recovery 11 и Veeam Backup & Replication 9. Функционал второго направлен на работу со средами виртуализации, поэтому оно исключено из рассмотрения.

10.2.2 Средство резервного копирования Acronis Backup & Recovery 11.

Acronis Backup & Recovery 11 - сертифицированное ФСТЭК решение для резервного копирования и аварийного восстановления информации в физических и виртуальных средах для АРМ и серверов под управлением операционных систем Windows и Linux. Данное средство выпускается в двух редакциях: Advanced Workstation и Advanced Server - предназначенных для резервирования АРМ и серверов соответственно.

Принято решение в закрытом информационном контуре выполнять резервное копирование только для сервера, поскольку только на нем хранится критически важная информация и от него зависит выполнение отделом своих должностных обязанностей. А отказ одного АРМ не нанесет существенного ущерба производственному процессу. Поэтому в закрытом информационном контуре будет использоваться Acronis Backup & Recovery 11 Advanced Server.

Основными особенностями Acronis Backup & Recovery 11 Advanced Server по данным компании-дистрибьютора ЗАО «АЛТЭКС-СОФТ» являются:

- технология восстановления Universal Restore, позволяющая в короткие сроки восстановить файлы, конфигурации, программы или целые операционные системы на любую машину независимо от платформы;
- возможность инкрементного резервного копирования, при котором сохраняются только измененные данные;
- единая консоль централизованного управления и отчетности;
- резервное копирование полных образов дисков с пропуском неиспользуемых блоков;
- восстановление любого физического сервера в качестве виртуальной машины;
- поддержка большого количества приложений для тонкой настройки их резервирования;
- резервное копирование баз данных.

Acronis Backup & Recovery 11 Advanced Server имеет сертификат ФСТЭК, позволяющий использовать его для защиты АС до класса 1Г включительно, ИС-ПДн до 1 уровня защищённости включительно, ГИС до 1 класса включительно.

Стоимость одной лицензии Acronis Backup & Recovery 11 Advanced Server у дистрибьютора ЗАО «АЛТЭКС-СОФТ» составляет 95900 рублей [26].

10.3 Выбор генератора электромагнитного шума

10.3.1 Общие сведения о генераторах электромагнитного шума.

Генераторы электромагнитного шума являются активным средством защиты от утечки информации за счет ПЭМИН.

Для исключения возможности перехвата побочных электромагнитных излучений применяют пространственное зашумление, а для исключения возможности съема наводок с проводников - линейное зашумление.

К системам пространственного зашумления предъявляются следующие требования:

- система должна создавать помехи во всем диапазоне частот возможных излучений ОТСС;
- создаваемые помехи не должны повторяться по структуре;
- отношение «сигнал/шум» на границе контролируемой зоны должно быть меньше допустимого значения;
- создаваемые помехи должны иметь горизонтальную и вертикальную поляризацию.

Пространственное зашумление считается успешным, если удовлетворяет приведенным выше требованиям. Допустимы значения рассчитываются по специальным методикам.

Системы пространственного зашумления чаще всего генерируют синфазные помехи, напоминающие защищаемый сигнал, (так называемые «имитационные помех») или белый шум, представляющий собой широкополосный сигнал с

равномерным энергетическим спектром, мощность которого существенно превышает мощность информативного сигнала.

Генераторы шума могут быть выполнены как в виде отдельного блока, так и в виде платы для компьютера.

Системы линейного зашумления подключаются непосредственно к линиям и подают в них шум с заданными характеристиками.

Линейное зашумление в закрытом информационном контуре не требуется, поскольку отсутствуют выходящие за пределы контролируемой зоны линии.

Одними из распространённых генераторов шума, имеющих сертификат ФСТЭК являются Гном-3, ГШ-2500М и Соната-Р2.

10.3.2 Генератор шума Гном-3.

Генератор шума Гном-3 предназначен для защиты конфиденциальной информации от утечки, вызываемой паразитными электромагнитными излучениями и наводками. Генератор имеет гибкую рамочную антенну, которая устанавливается стационарно в защищаемом помещении. Антенна в комплект не входит. Она представляет собой три рамки, расположенных во взаимно-перпендикулярных плоскостях, и позволяет защитить помещения площадью до 50 квадратных метров. Внешний вид устройства представлен на рисунке 6.



Рисунок 6 - Генератор шума Гном-3

Основные технические характеристики:

- диапазон частот шумового сигнала - от 10 кГц до 1 ГГц;
- спектральная плотность шума - от 45 до 75 дБ;

- индикация работы - световая;
- питание - 220 В, 50 Гц;
- длина - 307 мм;
- ширина - 95 мм;
- высота - 48,5 мм;
- номер сертификата ФСТЭК - 149/2;
- срок действия сертификата - 09.04.2019.

Стоимость генератора шума Гном-3 составляет 28000 рублей. Цена может изменяться в зависимости от поставщика [27].

10.3.3 Генератор шума ГШ-2500М.

Стационарный генератор шума ГШ-2500М предназначен для маскировки ПЭМИН компьютеров, АРМ и оргтехники путем излучения в пространство электромагнитного белого шума и наведения такого шума в отходящие цепи. Один генератор способен защитить помещение площадью до 40 квадратных метров. Внешний вид устройства приведен на рисунке 7.



Рисунок 7 - Генератор шума ГШ-2500М

Основные технические характеристики:

- диапазон частот шумового сигнала - от 100 кГц до 2 ГГц;
- спектральная плотность шума - от 45 до 75 дБ;
- индикация работы - световая и звуковая;
- питание - 220 В, 50 Гц;

- длина - 700 мм (с антенной);
- ширина - 600 мм (с антенной);
- высота - 35 мм;
- номер сертификата ФСТЭК - 2999;
- срок действия сертификата - 14.10.2019.

Стоимость генератора шума ГШ-2500М составляет 20000 рублей. Цена может изменяться в зависимости от поставщика [28].

10.3.4 Генератор шума Соната-Р2.

Генератор шума Соната-Р2 предназначен для защиты объектов вычислительной техники от утечки за счет побочных электромагнитных излучений ЭВМ и наводок их на отходящие линии. Может использоваться с антенной «Веер» или без нее. В первом случае характеристики значительно выше. Внешний вид устройства с антенной представлен на рисунке 8.



Рисунок 8 - Генератор шума Соната-Р2

Основные технические характеристики (с антенной):

- диапазон частот шумового сигнала - от 10 кГц до 2 ГГц;
- спектральная плотность шума - от 50 до 90 дБ;
- индикация работы - световая и звуковая;
- питание - 220 В, 50 Гц;
- диаметр - 65 мм;
- высота - 325 мм;
- номер сертификата ФСТЭК - 1129;
- срок действия сертификата - 16.01.2021.

Стоимость генератора шума Соната-Р2 составляет 16000 рублей. Стоимость антенны 6000 рублей. Цена может изменяться в зависимости от поставщика [29].

10.3.5 Выбор генератора электромагнитного шума для закрытого информационного контура.

На практике генератор шума ГШ-2500М применяется для защиты одиночных или рядом стоящих АРМ. В условиях, когда в помещении расположены несколько АРМ на расстоянии друг от друга, это может повлечь большие расходы. Для защиты помещений в целом чаще применяют генераторы шума Гном-3 и Соната-Р2. Соната-Р2 по сравнению с Гном-3 обладает более широким диапазоном шумового сигнала и, при использовании антенны «Веер», более высокой плотностью шума. При этом стоимость генератора шума Соната-Р2 вместе с антенной «Веер» ниже, чем стоимость Гном-3. Поэтому для использования в закрытом информационном контуре был выбран генератор шума Соната-Р2.

10.4 Структура закрытого информационного контура

Выбранные средства защиты полностью обеспечивают выполнение защитных мер, которые были определены в главе 7. Программно-аппаратные средства защиты информации, выбранные для закрытого информационного контура, представлены на рисунке 9.



Рисунок 9 - Программно-аппаратные средства защиты информации, выбранные для закрытого информационного контура

Таким образом закрытый информационный контур имеет структуру, представленную на рисунке 10.

В помещениях отдела остаются только АРМ, предназначенные для обработки конфиденциальной информации. Исключение составляет кабинет начальника отдела, в нем находится один компьютер, не предназначенный для обработки конфиденциальной информации, подключенный к локальной вычислительной сети предприятия и сети Интернет. Данный компьютер предназначен для получения электронной почты, адресованной данному отделу, а также для загрузки обновлений для технических средств закрытого информационного контура и последующей ручной установки этих обновлений.

Все основные и вспомогательные технические средства и системы, а также специальные технические средства прошли спецпроверку и специсследование.

На каждом АРМ, предназначенном для обработки конфиденциальной информации, установлены СЗИ от НСД Secret Net Studio, АПМДЗ «Соболь», сканер безопасности Redcheck.



Рисунок 10 - Структура закрытого информационного контура

На сервере кроме этих средств установлено средство для резервного копирования Acronis Backup & Recovery 11 Advanced Server.

Линии электропитания и заземления, а также каналы связи закрытого информационного контура не выходят за пределы контролируемой зоны. Защиту от наводок на другие линии, в том числе на линии подключения открытого компьютера к сети предприятия, а также от побочных электромагнитных излучений обеспечивают генераторы шума Соната-Р2, установленные в каждом помещении.

Двери всех помещений оборудованы кодовыми замками. Все окна оборудованы жалюзи. Расположение средств отображения информации соответствует рисунку 10 и обеспечивает невозможность утечки видовой информации.

11 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

11.1 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации

Согласно ГОСТ 12.0.003-2015 среди производственных факторов, оказывающих отрицательное психофизиологическое воздействие на организм человека, выделяют:

- физические перегрузки, определяемые тяжестью трудового процесса;
- нервно-психические перегрузки, определяемые напряженностью трудового процесса. [1]

К физическим перегрузкам относятся:

- статические нагрузки, определяемые рабочей позой;
- динамические нагрузки, определяемые массой поднимаемого и перемещаемого вручную груза;
- динамические нагрузки, определяемые повторением монотонных рабочих движений [30].

В своей работе специалист по защите информации связан только с одним видом вредных психофизиологических факторов - статическими перегрузками, определяемые рабочей позой, так как проводит большую часть рабочего времени за компьютером в одном положении.

Среди нервно-психических перегрузок выделяют:

- умственное перенапряжение, в том числе связанное с информационной нагрузкой;
- чрезмерное напряжение анализаторов, также вызванное информационной перегрузкой;

- монотонность труда, способствующая формированию монотонии, то есть снижению работоспособности в результате выполнения однообразной работы, связанной с частым повторением стереотипных действий;
- эмоциональные перегрузки [30].

Специалист по защите информации подвержен всем видам нервно-психических перегрузок, так как его деятельность включает работу с большим количеством информации и высокую степень ответственности. Ухудшению психоэмоционального состояния в этом случае способствует повышенное зрительное перенапряжение, умственные и нервно-эмоциональные нагрузки, продолжительная концентрация внимания, монотонность трудового процесса, большой объем информации, нерациональная организация рабочего места.

Таким образом, нервно-психические перегрузки в работе специалиста по защите информации - это следствие информационного взаимодействия в системе «пользователь – ПЭВМ». Они определяются некачественными условиями передачи изображения, несоответствием некоторых параметров информационных систем психофизиологическими особенностями человека, необходимостью внимательного наблюдения за информационными знаками, быстрого анализа постоянно изменяющейся информации, принятия продуктивных решений и выполнения определённых корректирующих действий.

Как правило, операторы ПЭВМ жалуются к концу рабочего дня на зрительное переутомление, головную боль, ноющие боли в мышцах шеи, плечевого пояса и спины, снижение способности к концентрации внимания.

Ухудшение самочувствия пользователя ПЭВМ при длительной работе связано также повышением пульсации потоков света от источников искусственного освещения и монитора. Пульсации потоков света способствуют повышению общего и зрительного переутомления, ухудшению зрительной и общей работоспособности. При уменьшении частоты световых пульсаций вредное воздействие усиливается. К нервно-психическим факторам относится также низкочастотное мерцание экрана (до 200 Гц), то есть кажущееся изменение яркости свечения [31]. Оно возникает из-за взаимодействия пульсирующих потоков света экрана и

источников света. Даже на начальном этапе компьютеризации общества было обнаружено специфическое зрительное утомление при работе за дисплеем, которое было названо «компьютерный зрительный синдром. Это объясняется тем, что у человека зрительная система по ходу эволюции приспособилась для восприятия изображения в отраженном свете (напечатанная информация, тексты, рисунки), а не для работы за монитором компьютера. Изображение на дисплее сильно отличается от привычного глазу объектов внешнего мира — оно светится, мерцает, состоит из дискретных точек, кроме этого цвета компьютерного изображения отличаются от естественных цветов. Однако зрительное переутомление вызывают не только особенности изображения на экране. Сильная нагрузка на глаза оказывается при введении информации, так как пользователю необходимо переводить часто взгляд с экрана на набираемый текст и клавиатуру, которые находятся на разном расстоянии от монитора и по-разному освещены. Зрительное переутомление обычно проявляется при затуманивании зрения, сопровождается трудностями при переносе взгляда с близких предметов на дальние и с дальних на близкие, кажущееся изменение цвета предметов, двоение предметов, чувством жжения, «песка» в глазах, болезненными ощущениями при движении глаз, покраснением век.

Специфическое воздействие электромагнитного поля выражается в биохимических изменениях, происходящие в клетках и тканях. Наиболее подвержены данным воздействиям центральная и сердечно-сосудистая системы. Могут наблюдаться отклонения в работе эндокринной системы. В начале воздействия отмечается повышение возбудимости нервной системы, проявляющееся повышением раздражительности, нарушением сна, эмоциональной неуравновешенностью. Затем развиваются астенические проявления, т.е. физическая и нервно-психическая слабость. В целом хроническое воздействие ЭМП проявляется следующими симптомами: головная боль, повышенная утомляемость, ухудшение самочувствия, брадикардия (урежение пульса), а также гипотония (понижение артериального давления), боли в сердце. Данные негативные симптомы могут выражаться в разной степени [32].

11.2 Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов

Для нормального функционирования мозга необходимо, чтобы к нему поступали нервные импульсы от всех систем организма, в том числе и от мышц, которые составляют половину от массы всего организма. Движения мышц создают огромный поток нервных импульсов, способствующих обогащению мозга разнообразными ощущениями, поддерживающих его в хорошем рабочем состоянии. Именно поэтому умственная работоспособность непосредственно связана с общим состоянием здоровья, в укреплении которого важная роль отводится физической культуре.

При умственном труде, который лежит в основе деятельности специалиста по защите информации, в коре головного мозга формируются замкнутые циклы возбуждения, которые характеризуются большой устойчивостью и инертностью. Поэтому, если после прекращения физической нагрузки человек практически сразу может переключиться на новый вид деятельности, то при умственном труде интенсивная работа мозга не заканчивается продолжительное время и после завершения интеллектуальной нагрузки [33].

В основе организации отдыха при умственных перегрузках лежит принцип активного отдыха, который предусматривает систему организованных движений до, в процессе и по окончании умственной деятельности, что оказывает благоприятный эффект не только в сохранении, но и повышении умственной работоспособности. Ежедневные и регулярные физические упражнения способствуют формированию в коре больших полушарий «доминанты движения», которая оказывает положительное воздействие на состояние дыхательной, мышечной, сердечно-сосудистой систем организма, активизирует зону сенсомоторной активности в коре головного мозга, способствует повышению тонуса всего организма.

Перед началом интенсивной умственной работы, для сокращения периода вработывания, рекомендуются в течении 5 минут произвольные движения уме-

ренной или средней интенсивности, направленные на дополнительное напряжение мышц конечностей. При этом чем ниже исходное нервно-психическое и мышечное напряжение человека, и чем быстрее необходимо включиться в работу, тем интенсивнее должны быть упражнения на напряжение скелетных мышц. В процессе напряженной продолжительной умственной деятельности, сопровождаемой к тому же эмоциональным стрессом, рекомендуется проделать производные упражнения на общее расслабление и снижение тонуса скелетных мышц, желательно в сочетании с ритмичным сокращением небольших мышечных групп (разгибателей и сгибателей пальцев кисти, мимических мышц лица и т. п.).

Для повышения работоспособности мозга на фоне мышечного расслабления, улучшения функций дыхания и кровообращения, необходимо регулярно выполнять кратковременные физические упражнения. Например, раз в час при работе за компьютером проделать познотонические упражнения в течение нескольких минут, а через каждые 2 ч желательно проводить минутные динамические упражнения, такие как бег на месте, с ритмичным, глубоким дыханием [34].

Для снижения напряжения глаз каждые 2 часа рекомендуется выполнять упражнения для глаз. Гимнастику для глаз за компьютером лучше выполнять в расслабленном состоянии. При наличии боли в области шеи или спины, необходимо сначала выполнить упражнения для этих зон. При выполнении упражнений для глаз надо глубоко дышать, так как при работе глазные мышцы должны активно насыщаться кислородом.

Правильно подобранный комплекс упражнений повышает общий эмоциональный тонус работника, создавая устойчивое настроение, которое станет благоприятным фоном для активной умственной деятельности и необходимо для предупреждения раннего развития утомления. Физическая нагрузка выстроенная на основе принципа активного отдыха, оказывает благоприятное воздействие на повышение умственной работоспособности специалиста по защите информации.

Заключение

В ходе выполнения выпускной квалификационной работы была проанализирована нормативно-правовая база в области защиты конфиденциальной информации, изучены технические каналы утечки информации и источники угроз безопасности информации, определено понятие информационного контура организации. В рамках проектирования структуры закрытого информационного контура была построена структура незащищенного информационного контура, определена ее проектная защищенность, проведена классификация закрытого информационного контура по требованиям защиты информации, определены актуальные угрозы безопасности информации, обрабатываемой в закрытом информационном контуре и определены защитные меры, которые необходимо использовать. Все действия выполнялись в соответствии с требованиями и методиками ФСТЭК. Для всех требуемых защитных мер были определены средства, которыми они реализуются: проведен сравнительный анализ систем защиты информации от несанкционированного доступа и аппаратно-программных модулей доверенной загрузки, определены организационно-технические меры защиты информации, выбраны дополнительные программные и технические средства, которые должны использоваться при эксплуатации закрытого информационного контура. В заключении была разработана структура закрытого информационного контура с указанием рекомендуемого расположения технических средств и используемых защитных мер.

Кроме того, по результатам дипломного проектирования была написана статья «Актуальный рынок средств защиты ПЭВМ от несанкционированного доступа» для участия в международной научно-практической конференции «Особенности современного этапа развития естественных и технических наук», проводимой Агентством перспективных научных исследований. Статья опубликована в сборнике научных трудов по материалам данной конференции [35].

Таким образом задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

1 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // «Консультант Плюс» - законодательство РФ. с изм. и допол. в ред. от 1.01.2018.

2 Указ Президента Российской Федерации «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 № 188 // «Консультант Плюс» - законодательство РФ. с изм. и допол. в ред. от 13.07.2015.

3 Постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» от 03.11.1994 № 1233 // «Консультант Плюс» - законодательство РФ. с изм. и допол. в ред. от 18.03.2016.

4 Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ // «Консультант Плюс» - законодательство РФ. с изм. и допол. в ред. от 12.03.2014.

5 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Введ. 01.02.2008 // Сайт юридической фирмы «Интернет и Право». 1998-2017. URL: <http://www.internet-law.ru/gosts/gost/5737/> (дата обращения: 14.10.2017).

6 Ковалева Н.Н. Информационное право России. М.: Дашков и К, 2008.

7 Терминология в области защиты информации: Справочник. М.: ВНИИ «Стандарт», 1993.

8 Лунегов А.Н., Рыжов А.Л. Технические средства и способы добывания и защиты информации. М.: ВНИИ «Стандарт», 1993.

9 Ярочкин В.И. Безопасность информационных систем. М.: Ось-89, 1996.

10 Норткат С., Новак Д. Обнаружение нарушений безопасности в сетях. пер. с англ. В.С. Иващенко. 3-е изд. М.: Вильямс, 2003.

11 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. 2-е изд. М.: Радио и связь, 2001.

12 Приказ ФСТЭК «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17 // ФСТЭК России. с изм. и допол. в ред. от 15.02.2017.

13 Методический документ «Методика определения угроз безопасности информации в информационных системах (проект)» ФСТЭК России, 2015.

14 Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 ФСТЭК России.

15 «Методический документ «Меры защиты информации в государственных информационных системах» от 11.02.2014 ФСТЭК России.

16 СЗИ от НСД - Разграничение доступа Secret Net // Код Безопасности: официальный сайт. 2008-2018. URL: https://www.securitycode.ru/products/secret_net/ (дата обращения: 17.11.2017).

17 Secret Net Studio // Код Безопасности: официальный сайт. 2008-2017. URL: <https://www.securitycode.ru/products/secret-net-studio/> (дата обращения: 17.11.2017).

18 Системы защиты информации Страж NT // РУБИНТЕХ: официальный сайт. 2009-2017 URL: http://www.guardnt.ru/gnt_40.html (дата обращения: 17.11.2017).

19 СЗИ Dallas Lock 8.0-K // Dallas Lock – линейка сертифицированных средств защиты информации: официальный сайт. 2017 URL: <https://www.dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/> (дата обращения: 17.11.2017).

20 АПМДЗ «Максим-M1» // URL: <http://www.astralinux.com/products/maxim.html> (дата обращения: 19.11.2017).

21 Комплекс аппаратно-программных средств защиты компьютера от несанкционированного доступа НСД - КРИПТОН-ЗАМОК // АНКАД: официальный сайт. 2000–2017. URL: <https://ancud.ru/crzam.html> (дата обращения: 19.11.2017).

22 Блокхост-АМДЗ 2.0 // Газинформсервис - информационная безопасность: официальный сайт. 2004–2017. URL: <http://www.gaz-is.ru/produkty/zashchita-rabochih-stancii-i-serverov/blockhost-amdz.html> (дата обращения: 19.11.2017).

23 Аппаратно-программный модуль доверенной загрузки (АПМДЗ psi) Соболь // Код Безопасности: официальный сайт. 2008-2017. URL: https://www.securitycode.ru/products/pak_sobol/ (дата обращения: 19.11.2017).

24 Сканер безопасности (средство анализа защищенности) - RedCheck // URL: <https://www.redcheck.ru/> (дата обращения: 1.12.2017).

25 MaxPatrol 8 // Positive Technologies — безопасность, консалтинг, compliance management: официальный сайт. 2002-2017. URL: <https://www.ptsecurity.com/ru-ru/products/mp8/> (дата обращения: 1.12.2017).

26 Acronis True Image Echo Workstation // АЛТЭКС-СОФТ: официальный сайт. 2008-2017. URL: <https://www.altx-soft.ru/groups/page-67.htm> (дата обращения: 1.12.2017).

27 Генератор шума «Гном-3» // Центр безопасности информации. URL: <http://www.cbi-info.ru/groups/page-83.htm> (дата обращения: 15.12.2017).

28 Генератор шума «ГШ-2500» // Центр безопасности информации. URL: <http://www.cbi-info.ru/groups/page-80.htm> (дата обращения: 15.12.2017).

29 Генератор шума «Соната - Р2» с модулем ИК // Центр безопасности информации. URL: <http://www.cbi-info.ru/groups/page-1078.htm> (дата обращения: 15.12.2017).

30 ГОСТ 12.0.003-2015. Система стандартов по безопасности труда. Опасные и вредные производственные факторы. Классификация. Введ. 01.03.2013 // Сайт юридической фирмы «Интернет и Право». 1998-2017. URL: <http://www.internet-law.ru/gosts/gost/62075/> (дата обращения: 14.11.2017).

31 Опасные и вредные факторы при работе с ПЭВМ // РГРТУ Рязанский Государственный Радиотехнический Университет Группа 640 URL: <http://rgrtu-640.narod.ru/bezopasnost-zhiznedeyatelnosti/45.html> (дата обращения: 14.11.2017).

32 Вредные и опасные факторы при работе с компьютером // Энциклопедия Экономиста URL: <http://www.grandars.ru/shkola/bezopasnost-zhiznedeiatelnosti/vrednye-factory-pri-rabote-na-pk.html> (дата обращения: 14.11.2017).

33 Экзамен по физической культуре в вузе / Коваль Л.Н., Богданов О.Г., Ярошенко Е.В., Алексеева Е.Н., М.-Берлин: Директ-Медиа, 2015.

34 Физическая культура студента / Под ред. Ильинича В.И. М.: Гардарики, 2000.

35 Яшин Е.В., Тихомиров П.А. Актуальный рынок средств защиты ПЭВМ от несанкционированного доступа // 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. С. 216-220.

Приложение А

(обязательное)

Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ»

Ректору Пензенского
государственного университета
А. Д. Гулякову
студента 6 курса ФПИТЭ
очной формы обучения
Тихомирова Павла Александровича

ЗАЯВЛЕНИЕ

Я, Тихомиров Павел Александрович, студент 6 курса очной формы обучения направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Закрытый информационный контур, обеспечивающий сбор, хранение, обработку, обмен и предоставление конфиденциальной информации», выполненного мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.


«10» 01 2018 г

ВКР представлена на проверку «__» _____ 20__ г

Руководитель ВКР  Е.В. Яшин



Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Закрытый информационный контур, обеспечивающий сбор, хранение, обработку, обмен и предоставление конфиденциальной информации» студента 6 курса П.А. Тихомирова направления подготовки 10.05.02 - «Информационная безопасность телекоммуникационных систем».

Руководитель ВКР инженер 3-й категории АО «НПП «Рубин» Яшин Евгений Валерьевич.

Отчет о проверке на заимствования

Автор: Тихомиров Павел Александрович tikhomirovpa95@gmail.com / ID: 625

Проверяющий: Фатеев Алексей Григорьевич (fbst@pnzgu.ru) / ID: 393

Организация: Пензенский гос. Университет

Отчет предоставлен сервисом «Антиплагиат» - <http://pnzgu.antiplagiat.ru>

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 29
Начало загрузки: 12.01.2018 09:28:35
Длительность загрузки: 00:00:09
Имя исходного файла:
ВКР_12ПТ1_Тихомиров
Размер текста: 2518 кБ
Символов в тексте: 164630
Слов в тексте: 18491
Число предложений: 896

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 12.01.2018 09:28:46
Длительность проверки: 00:00:12
Комментарии: не указано
Модули поиска: Модуль поиска ЭБС "БиблиоРоссика", Модуль поиска ЭБС "BOOK.ru", Коллекция РГБ, Цитирование, Модуль поиска ЭБС "Университетская библиотека онлайн", Коллекция eLIBRARY.RU, Модуль поиска ЭБС "Айбукс", Модуль поиска Интернет, Модуль поиска ЭБС "Лань", Модуль поиска "ПГУ", Кольцо вузов

ЗАИМСТВОВАНИЯ

28,47%

ЦИТИРОВАНИЯ

0,12%

ОРИГИНАЛЬНОСТЬ

71,41%



«15» 01 2018 г

Е.В. Яшин

Подпись руководителя заверено
Заместитель ВКР
С.А. Козлов