

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

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность систем
и технологий»

Специальность 10.05.02 –

Информационная безопасность
телекоммуникационных систем

Специализация -

Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРИ ХРАНЕНИИ, ОБРАБОТКЕ И ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ
ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ
КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В АО «ПО
«ЭЛЕКТРОПРИБОР»

Студент

Храмов Андрей Вячеславович

Руководитель начальник ОТЗИ и ПДТР

АО «ПО «Электроприбор»

_____ Дубин Р.М.

Нормоконтролёр к.т.н., доцент

Фатеев А.Г.

Рецензент ведущий инженер ОТЗИ и ПДТР

АО «ПО «Электроприбор»

Зосимов И.В.

Работа допущена к защите (протокол заседания кафедры от

_____ № _____)

Заведующий кафедрой

С.Л. Зефиоров

Работа защищена с отметкой

(протокол заседания ГЭК

от _____ № _____)

Секретарь ГЭК

А.Г. Фатеев

Пенза 2018

Оглавление

Введение.....	4
1 Анализ нормативно-правовых актов в области защиты информации ограниченного доступа, не составляющей государственную тайну	6
1.1 Понятие и виды информации ограниченного доступа, не составляющей государственную тайну	6
1.2 Понятие и виды защиты информации ограниченного доступа, не составляющей государственную тайну	8
2 Анализ технических каналов утечки информации	10
3 Идентификация целей и задач деятельности АО «ПО «Электроприбор»	14
4 Анализ информационных потоков АО «ПО «Электроприбор».....	18
5 Анализ структуры информационной системы АО «ПО «Электроприбор» организации и идентификация технических средств обработки информации. .	23
6 Классификация информационной системы	27
7 Идентификация источников угроз	30
7.1 Понятие идентификации источников угроз	30
7.2 Оценка возможностей нарушителей	30
7.3 Возможные способы реализации угроз безопасности информации ...	36
8 Определение актуальных угроз безопасности информации в информационной системе	41
8.1 Понятие актуальности угрозы безопасности информации	41
8.2 Оценка уровня проектной защищенности информационной системы	43
8.3 Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в информационной системе	45
8.4 Оценка возможности реализации угрозы безопасности информации и актуальности угроз	50
9 Определение требований к системе защиты информации информационной системы	53

9.1Порядок определения требований к системе защиты информации информационной системы.....	53
9.2 Выбор мер защиты информации информационной системы	56
10 Разработка организационных и организационно-технических мер при обработке информации в информационной системе.....	73
11 Обзор существующих технических и программных средств защиты информации.....	77
12 Выбор и обоснование технических и программных средств защиты информации для информационной системы	86
13 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	88
Заключение.....	91
Список используемых источников.....	92
Приложение А Модель угроз безопасности информации	94
Приложение Б Акт о внедрении.....	100
Приложение В Протокол проверки ВКР в системе Антиплагиат	102

Введение

Сегодня почти не осталось предприятий где бы отсутствовала система обработки информации, которая бы не обрабатывала информацию, для осуществления своей профессиональной деятельности.

Защита информационной безопасности для системы осуществляется защитой аппаратных и программных компонентов, где последние еще являются информационными ресурсами компьютерной системы. От защиты программных компонентов зависит насколько безопасна передача, хранение и обработка информации в информационной системе.

Но такой взгляд на проблему безопасности компьютерных систем является ограниченным. Люди так же являются частью информационной системы и во время своей деятельности разрабатывают, обслуживают и используют. Данные специалисты обладают информацией и знаниями о системе и имеют свободный доступ к ней. Поэтому защите от несанкционированных воздействий должны подвергаться не только технические и программные компоненты, но и персонал работающий с информационной системой.

Поэтому, систему обработки информации, как объект защиты предоставляет рассмотренный ниже комплекс компонентов:

- информации на машинных носителях;
- средств передачи и обработки информации;
- программное обеспечение обрабатывающее информацию согласно установленным технологии, методам и алгоритмам;
- обслуживающего персонала и пользователей системы, объединенных по организационному, предметно-тематическому, технологическому и другим принципам для выполнения автоматизированной обработки информации с целью удовлетворения информационных потребностей субъектов информационных отношений.

Целью выпускной квалификационной работы является разработка подсистемы обеспечивающей информационную безопасность средствами криптографической защиты в АО «ПО «Электроприбор» в соответствии с действующим законодательством Российской Федерации по защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке, хранении и передаче по каналам связи.

Задачами выпускной квалификационной работы являются:

- анализ нормативно-правовых актов в области защиты информации ограниченного доступа, не составляющей государственную тайну;
- анализ технических каналов утечки информации;
- идентификация перечня угроз безопасности информации;
- разработка модели нарушителя безопасности информации;
- разработка модели угроз безопасности информации;
- разработка организационных и организационно-технических мер при обработке информации в информационной системе;
- обзор существующих технических и программных средств защиты информации;
- выбор и обоснование технических и программных средств защиты информации для информационной системы;
- исследование вредных психофизиологических факторов, влияющих на органы зрения специалиста по защите информации, а так же методов и средств физической культуры, снижающих их воздействие.

1 Анализ нормативно-правовых актов в области защиты информации ограниченного доступа, не составляющей государственную тайну

1.1 Понятие и виды информации ограниченного доступа, не составляющей государственную тайну

Информация может являться субъектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения [1].

В зависимости от категории доступа информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [1].

Классификация информации по категориям доступа представлена на рисунке 1.



Рисунок 1 - Классификация информации по категориям доступа

Федеральный закон РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет подразделение информации (в зависимости от категории доступа к ней) на общедоступную информацию и информацию, доступ к которой ограничен федеральными законами) [1].

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» [2]. К видам конфиденциальной информации, согласно этому указу относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. N 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации [3];

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами;

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

1.2 Понятие и виды защиты информации ограниченного доступа, не составляющей государственную тайну

В ГОСТ Р 50922-2006 определено, что защита информации - это деятельность, которая направлена на предотвращение утечки защищаемых данных, непреднамеренных и несанкционированных воздействий на защищаемые данные [4]. Выделяются следующие виды защиты информации:

- правовая защита информации - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением [4];

- техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [4];

- криптографическая защита информации - защита информации с помощью ее криптографического преобразования [4];

- физическая защита информации - обеспечение безопасности информации благодаря применению организационных мероприятий и технических средств, создающих препятствия для получения физического доступа к объекту защиты посторонних лиц [4].

Организационные мероприятия, направленные на обеспечение физической защиты информации, предполагают установление режимных, временных, территориальных, пространственных ограничений на доступ к объекту защиты [4].

Защита информации осуществляется от:

- утечки - неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на

исключение (затруднение) получения защищаемой информации разведками и другими заинтересованными субъектами [4];

- несанкционированного воздействия - несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [4];

- непреднамеренного воздействия - воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [4];

- разглашения - несанкционированного доведения защищаемой информации до заинтересованных субъектов, не имеющих права доступа к этой информации [4];

- несанкционированного доступа - получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации [4];

- разведки - перехвата защищаемой информации технической, агентурной разведкой [4].

2 Анализ технических каналов утечки информации

Конфиденциальная информация – это документированная информация, доступ к которой ограничен законодательством Российской Федерации. Это могут быть сведения, которые составляют коммерческую тайну предприятия, персональные данные сотрудников или клиентов, служебная информация, сведения о сущности изобретения, тайна следствия и судопроизводства и профессиональная тайна, могут стать объектом интереса злоумышленников [5]. Исходя из вышеперечисленного требуется осуществлять деятельность по предотвращению или уменьшению вероятности утечки информации конфиденциального характера.

Утечка — неконтролируемое распространение защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение получения защищаемой информации разведками и другими заинтересованными субъектами [4]. Утечка конфиденциальных данных происходит каналам утечки информации. Канал утечки информации - это канал коммуникации, через который происходит передача или доступ к информации, из-за чего происходит нарушение безопасности системы.

Существуют три способа утечки информации:

- разглашение информации;
- утечка по техническим каналам;
- несанкционированный доступ к информации.

Существуют прямые и косвенные каналы утечки информации по которым происходит нарушение безопасности информации. Косвенные каналы утечки, это такие каналы. Под косвенными каналами понимают такие каналы, по которым происходит доступ к информации ограниченного доступа не составляющей государственную тайну, без проникновения на объект или в помещение, с расположенными в них компонентами системы. К способам утечки информации по косвенным каналам можно отнести утерю носителей

информации, прослушивание, перехват ПЭМИН. Утечка по прямым каналам возможна при непосредственном доступе к сегментам системы..

Важным фактором возможности утечки информации является либо ее интерес для злоумышленника, либо существование условий, которые позволяют получить информацию. Доступа к конфиденциальной информации возможен при случайном факторе и возможном стечении обстоятельств или при умышленных действиях противника. Основными источниками утечки конфиденциальной информации являются:

- сотрудники организации, которые имеют допуск к информации конфиденциального характера в силу своих служебных полномочий;
- средства обработки и передачи информации;
- сообщение содержащие конфиденциальную информацию и передаваемые по каналам связи;
- документы, изделия или другие материальные носители информации ограниченного доступа.

На основании вышеизложенного можно установить, что информация конфиденциального характера может быть получена третьим лицом в ходе:

- утери документа на каком-либо носителе или пакета с документами, на которых находились конфиденциальные записи;
- нарушения сотрудником организации требований по защите информации конфиденциального характера;
- разговоров сотрудников о конфиденциальных сведениях, в местах не предназначенных для этого;
- обработки информации конфиденциального характера в присутствии третьих лиц;
- незаконной передачи информации ограниченного доступа другому сотруднику;
- отсутствия грифов секретности на документах, нанесения маркировки на носителях.

Утечка конфиденциальной информации может произойти в результате атак со стороны злоумышленника.

Наличие специальных технических средств, позволяет получить доступ к информации без прямого контакта с сотрудниками, документами или другими носителями информации. Канал утечки возникающий в результате действий специальных технических средств называется техническим каналом утечки информации. Технический канал утечки информации представляет собой физический путь от носителя информации к злоумышленнику, в результате которого последний получает доступ к защищаемой информации. Данная утечка информации возможна при наличии необходимых пространственных, энергетических и временных условий, и при наличии у злоумышленника соответствующих технических средств. Возможны следующие каналы утечки информации, по которым возникают нарушения целостности и конфиденциальности информации:

- побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;
- наводки информативного сигнала на провода, элементы отопления, цепи заземления и электропитания, выходящих за пределы контролируемой зоны;
- модуляция информативного сигнала, возникающего при наличии паразитной генерации в узлах или при работе различных генераторов;
- модуляция информативным сигналом радиоизлучения высокочастотных сигналов, создаваемых с помощью специальных технических средств;
- внедрение устройств («закладок») для последующей модуляции информативным сигналом радиоизлучения или электрических сигналов;
- перехват информации при подключении к каналам связи или техническим средствам обработки информации;
- отражающая поверхность помещения, вибрирующих под действием акустического речевого сигнала и облученная лазерным лучом;

- перехват акустического излучение речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- вибрационные сигналы на элементах строительных конструкций и коммуникации выделенных помещений, возникающие при воздействии на них акустического сигнала;
- визуальный просмотр информации с помощью оптических средств с экранов дисплеев и других средств ее отображения;
- воздействие на технические, программные средства и посредством внедрения специальных электронных и программных средств («закладок»).

К основным угрозам конфиденциальной информации относятся разглашение, утечка, несанкционированный доступ. Угроза безопасности информации конфиденциального характера представляет собой комплекс различных факторов и условий, в результате действия которых возникает потенциальная или реально существующая опасность утечки конфиденциальных сведений или непреднамеренными действиями с ней.

Эти действия направлены на нарушение конфиденциальности и целостности информации ограниченного доступа, что приводит к получению организацией материального и репутационного ущерба. Угрозы сведений конфиденциального характера возникающие в отношении к объекту делятся на внутренние и внешние.

К внутренним нарушителями потенциально относят сотрудников предприятия, администрацию, лиц, имеющих доступ к системе обработки информации предприятия, обслуживающий персонал. К источникам внешних угроз конфиденциальной информации причисляют клиентов, посетителей,

нарушителей пропускного режима предприятия, а также любые лица, не имеющие допуск к контролируемой территории.

Так как возникает вероятность утечки информации ограниченного доступа, не составляющей государственную тайну, в частности конфиденциальной информации, при обработке ее в информационных системах, требуется разработка и принятие мер по предотвращению доступа к ней сторонних лиц. Это произойдет в результате анализа возможных источников угроз безопасности информации, и принятия решения о применении необходимых средств защиты информации.

3 Идентификация целей и задач деятельности АО «ПО «Электроприбор»

Акционерное общество «Пензенское производственное объединение «Электроприбор» (АО «ПО «Электроприбор») является одним из ведущих предприятий России по изготовлению и поставке средств телекоммуникации и связи специального назначения, которые обеспечивают надежную криптографическую защиту конфиденциальной речевой, документальной, графической информации и применяются на стационарных и подвижных (на колесной и гусеничной базе, на вертолетах, самолетах, космических аппаратах, на надводных и подводных объектах морского базирования) пунктах управления различного назначения.

Главной целью деятельности предприятия является разумное ведение производственно-хозяйственной деятельности с последующим получением прибыли и использования ее в интересах предприятия, а так же для повышения благосостояния его членов.

Для выполнения своих, предприятие решает следующие задачи:

- производство продукции и обеспечение процесса производства;
- обеспечение персонала всем необходимым для выделенной работы;
- обеспечение информационного взаимодействия между подразделениями предприятия, между начальством предприятия и персоналом, между предприятием и поставщиками, клиентами.

Для достижения поставленной цели предприятие сохранило за собой возможность вести следующие виды деятельности:

- производство средств связи, выполняющих функцию систем коммутации;
- производство электромонтажных работ;
- деятельность консультативная и работы в области компьютерных технологий;
- производство оружия и боеприпасов;
- производство средств связи, выполняющих функцию цифровых

транспортных систем;

- производство средств связи, выполняющих функцию систем управления и мониторинга;

- производство оборудования, используемого для учета объема оказанных услуг связи;

- производство радиоэлектронных средств связи;

- производство оборудования средств связи, в том числе программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий;

- производство радио- и телевизионной передающей аппаратуры;

- производство коммуникационного оборудования;

- производство транспортных средств и оборудования, не включенных в другие группировки;

- разработка компьютерного программного обеспечения;

- деятельность по техническому контролю, испытаниям и анализу;

- научные исследования и разработки в области естественных и технических наук;

- исследование конъюнктуры рынка;

- предоставление консультационных услуг по вопросам безопасности;

- деятельность в области защиты информации;

- ремонт коммуникационного оборудования.

В соответствии с возложенными задачами основными функциями предприятия, связанными с созданием и внедрением автоматизированных рабочих мест и систем информационно-аналитического обеспечения, являются:

- формирование внутренних информационных ресурсов на основе поставленных задач структурными подразделениями предприятия;

- подключение пользователей предприятия к внутренним и внешним информационным ресурсам;

- методическая помощь работникам предприятия в сфере доступа к внешним информационным ресурсам с использованием информационных

технологий;

- создание, внедрение, сопровождение и развитие автоматизированной программно-технической и коммуникационной системы, обеспечивающей эффективное информационное взаимодействие пользователей на предприятии между собой, а также другими организациями;

- организация самостоятельных разработок и внедрения новых проектов, а также участие в разработках и внедрении проектов, программ и автоматизированных систем, направленных на обеспечение эффективной работы всех направлений деятельности предприятия.

4 Анализ информационных потоков АО «ПО «Электроприбор»

Для выполнения поставленных задач предприятие создает, получает и обрабатывает большое количество информации.

Информационная система АО «ПО «Электроприбор» предназначена для автоматизации процессов производства, планирования и учета, бухгалтерского учета, управления данными персонала и, документооборота, конструкторско-технологической подготовки производства.

В информационной системе обрабатываются сведения конфиденциального характера, перечень которых представлен в таблице 1. Таблица 1 – Перечень сведений, составляющих конфиденциальную информацию

№	Перечень сведений
Сведения в области защиты КИ	
1	Сведения, раскрывающие организацию системы защиты конфиденциальной информации (общее описание, структура и режим функционирования), в том числе, в части применяемых средств защиты информации при передаче информации конфиденциального характера по открытым телекоммуникационным каналам связи.
2	Сведения, содержащие описание структуры локальной вычислительной сети и полномочий пользователей, обрабатывающих информацию конфиденциального характера.
3	Сведения о ключах, кодах, паролях и идентификаторах пользователей осуществляющих обработку конфиденциальной информации.
4	Сведения об организации и технических решениях по системе охраны (система контроля доступа) производственных помещений.
5	Документация, содержащая сведения по защите информации конфиденциального характера
5.1	Технические задания на разработку системы защиты информации конфиденциального характера или ее компонент.
5.2	Концепции, технические решения, руководства, инструкции, положения, методические указания по защите информации конфиденциального характера.
5.3	Система и матрица разграничения доступа пользователей к информации конфиденциального характера.
5.4	Технические предложения, эскизные, технические и рабочие проекты по защите информации конфиденциального характера.
5.5	Описание модели возможного нарушителя в автоматизированной системе, обрабатывающей информацию конфиденциального характера.
5.6	Описание технологического процесса функционирования. Программы и методики испытаний, технические паспорта на объекты информатизации, заключения по результатам аттестационных испытаний и аттестаты на объекты информатизации по требованиям безопасности информации.

Продолжение таблицы 1

№	Перечень сведений
6	Сводные сведения о потребностях, поставках средств защиты и программно-технических комплексов, предназначенных для обработки информации конфиденциального характера по организации в целом.
7	Сведения о порядке передачи информации конфиденциального характера другим организациям.
8	Сведения о фактах ведения переговоров, предметах и целях совещаний и заседаний по защите информации конфиденциального характера и сторонних участников. Итоговые протоколы (решения).
9	Сведения, полученные при выполнении работ с другими организациями, содержащие информации конфиденциального характера этих организаций.
Сведения по средствам криптографической защиты информации	
10	Сведения о закрытом ключе уполномоченного лица удостоверяющего центра.
11	Сведения о закрытом ключе владельца сертификата открытого ключа подписи.
13	Персональная и корпоративная информация пользователей, содержащаяся в Удостоверяющем центре, за исключением информации, используемой для идентификации владельцев сертификатов открытых ключей и заносимой в изготавливаемые сертификаты.
14	Журналы аудита Удостоверяющего центра, материалы по разбору конфликтных ситуаций.
15	Базы данных центров сертификации, центра регистрации и администратора Удостоверяющего центра.
16	Сводная документация на средства криптографической защиты информации на объектах информатизации.
17	Отчетные материалы по проверке деятельности Удостоверяющего центра.
Сведения в области персональных данных	
18	Персональные данные о сотрудниках (ст.3. п.1 №152 – ФЗ «О персональных данных»)
Сведения в области бухгалтерского учета	
19	Содержание внутренне бухгалтерской отчетности (ст. 10 ФЗ №129 «О бухгалтерском учете»)
20	Сведения, содержащие списки клиентуры, покупателей, представителей и посредников, данные о поставщиках и потребителях, коммерческие связи.
21	Условия по сделкам и соглашениям, условия контрактов.
22	Сведения об элементах и расчетах цен, структура цены и продажной калькуляции, затраты.
23	Данные о предполагаемом конкурсе или торгах до их опубликования. Материалы и приложения к предложениям на публичных торгах.

Информационные потоки на предприятии являются смешанными, рассмотренные документы могут существовать как в бумажном, так и в электронном виде, соответственно, документ может содержаться как на бумажном, так и на цифровом носителе и обрабатываться с помощью технических средств.

Заказчик заключает договор на предоставление соответствующих услуг. Заключением договоров на оказание той или иной услуги занимается

юридический отдел. Реквизиты юридических лиц, персональные данные их руководителей, сотрудников, а также персональные данные физических лиц вбиваются в базу данных на сервер предприятия.

Договора подготавливаются в двух экземплярах. Затем, после утверждения генеральным директором АО «ПО «Электроприбор», договора либо лично забирают непосредственно заказчики, либо отправляются по почте. После утверждения заказчиком, один экземпляр договора АО «ПО «Электроприбор» получает по почте, либо непосредственно от самих заказчиков. Затем в базу данных бухгалтерией добавляются соответствующие сведения о клиенте.

После подписания договора обеими сторонами, соответствующие отделы АО «ПО «Электроприбор» приступают к оказанию услуг.

Технологический отдел передает сведения о новых, а также перспективных технологических и конструкторских решениях в конструкторский отдел. Разрабатываемые в отделе программы для оборудования под числовым программным управлением (ЧПУ) загружаются на файловый сервер предприятия.

Конструкторский отдел передает сведения о конструируемых изделиях и разрабатываемом ПО на файловый сервер предприятия.

Отдел производства мелких серий, как и отделы механо-сборочного и монтажно-сборочного производства запрашивают с файлового сервера сведения о конструируемых изделиях, разрабатываемого ПО и программы для станков с ЧПУ. ПО завершению работ сведения о производимой продукции и их объемах загружаются в базу данных предприятия.

Отдел снабжения передает подрядчику сведения о необходимом сырье материалах и их количестве. Работники отдела также записывают в базу данных предприятия сведения о материалах и комплектующих, которые имеются в наличии.

Отдел технологической документации запрашивает сведения о конструируемых изделиях и разрабатываемом ПО на файловом сервере

предприятия. Сотрудники отдела разрабатывают техническую документацию на реализованные изделия и передает ее заказчику.

Отдел маркетинга передает сведения об объемах реализуемой продукции в планово-экономический отдел.

Планово экономический отдел запрашивает сведения об объемах реализуемой продукции у отдела маркетинга, о прибыли предприятия из бухгалтерии, а также объемы производимой продукции.

Отдел информационных технологий осуществляет администрирование системы.

Отдел информационной безопасности передает информацию о рисках и уязвимостях системы в отдел информационных технологий.

После оказания услуг предприятием, бухгалтерия подготавливает бухгалтерские документы на оплату услуги, которые в свою очередь почтой передаются заказчику. После оплаты клиентом, подписанные бухгалтерские документы возвращаются предприятию. Затем обеими сторонами утверждается акт оказанных услуг, подписав который, заказчик соглашается с выполнением всех услуг в полном объеме.

На предприятии ведется обмен информацией ведется между сотрудниками и бухгалтерией. Документы, поступающие от сотрудников к главному бухгалтеру, заносятся в базу данных «1С: Предприятие».

База данных предприятия ведет учет сотрудников, а также создает карточку для бумажного дела сотрудника. После увольнения данные о сотруднике удаляются из базы, а бумажное дело передается в архив и хранится согласно закону об архивном деле.

После обработки документов главный бухгалтер формирует отчеты, которые передает директору для выдачи заработной платы сотрудникам, в Пенсионные и Налоговые органы. Информационные потоки, протекающие во время деятельности АО «ПО «Электроприбор» представлены на рисунке 2.

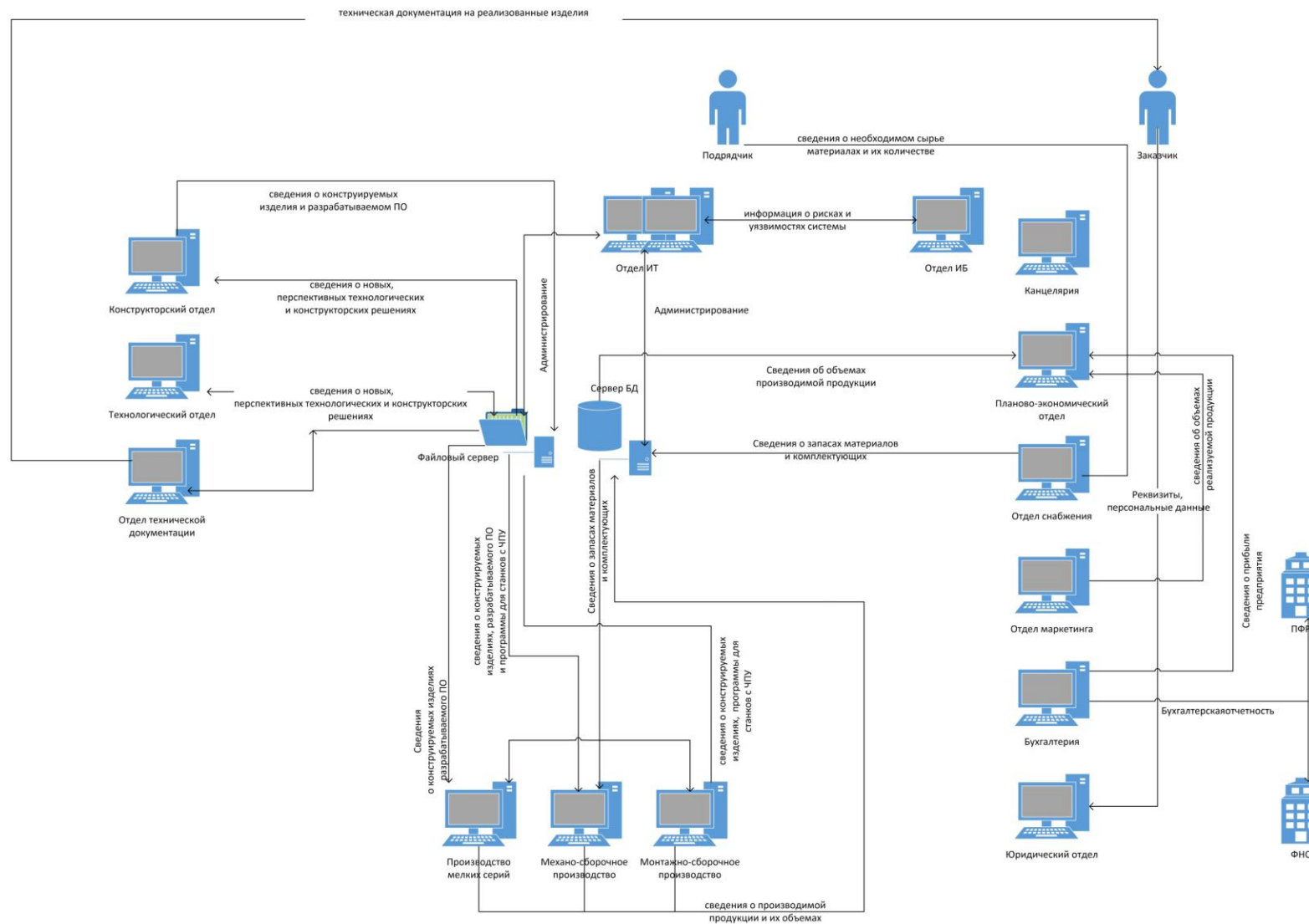


Рисунок 2 – Информационные потоки предприятия

5 Анализ структуры информационной системы АО «ПО «Электроприбор» организации и идентификация технических средств обработки информации

В АО «ПО «Электроприбор» телекоммуникационная сеть состоит из 7 серверов и 797 автоматизированных рабочих мест (АРМ). Все оборудование находится в пределах контролируемой зоны.

На сервере 1 установлен первичный контроллер домена, который используется для создания, настройки и управления учетными записями пользователей и компьютеров телекоммуникационной сети. Для избежание выхода из строя первичного контроллера домена, был создан резервный контроллер. Он носит имя вторичного контроллера домена и установлен на сервере 2. Периодически происходит синхронизация данных учетных записей и прав доступа, поэтому в случае выхода из строя первичного контроллера. Программное обеспечение обоих серверов представлено Microsoft Windows Server 2008.

Сервер 3 выполняет функции почтового и прокси-сервера. Для работы сервера используется ОС Microsoft Windows Server 2008 и Microsoft Windows Server 2010. Также для работы почтового сервера установлено ПО Courier Mail Server 1.56. Выполнение функций прокси-сервера осуществляется при помощи универсального шлюза безопасности Traffic Inspector. Traffic Inspector осуществляет фильтрацию спама, баннеров, графики и другого нежелательного медиа-контента, запрещает доступ к нежелательным веб-сайтам, фильтрует нежелательную почту перед тем как она попадет на почтовый сервер организации.

На сервере 4 установлено программное обеспечение «1С:Предприятие 8.2», предназначенное для автоматизации бухгалтерского и управленческого учётов. Так же на сервере находятся «Комплекс решений Аскон 2011». Данное ПО используется для управления инженерными и проектными данными, циркулирующими в единой информационной системе предприятия.

На сервере 5 находится программное обеспечение «1С:Предприятие 8.2» для резервирования сервера 4. Для работы сервера 4 и 5 используется ОС Microsoft Windows Server 2008.

Сервер 6 представляет собой систему управления базы данных (СУБД) Microsoft SQL Server 2008. СУБД представляет собой реляционную архитектуру, т.е. данные выражены в виде таблиц. Сервер не имеет доступа к внешним сетям. Сервер 6 резервирован на сервере 7.

Сервер 8 осуществляет работу с электронно-цифровой подписью, антивирусную защиты, контроль входящего трафика, централизованное управление системой защиты, мониторинг и аудит безопасности, на сервере установлено следующее ПО:

- Kaspersky Endpoint Security 8;
- Secret Net 7.0;
- Удостоверяющий Центр ViPNet.

На предприятии имеется 797 АРМ. АРМ сотрудников состоят из ПК, представленных в виде стационарных компьютеров, на которых обрабатываются данные бухгалтерского и финансового учета, данные персонала и конструкторско-технологическая информация, необходимые для осуществления деятельности предприятия.

На ПК сотрудников установлены операционные системы Windows XP и Windows 7 с установленным ПО для работы с базами данных «1С:Предприятие 8.2», системой автоматизированного проектирования радиоэлектронных средств Altium Designer, графическим редактором CorelDRAW Graphics Suite X5, текстовыми процессорами LibreOffice и Microsoft Office 2007 и почтовым клиентом Microsoft Office Outlook 2010. Для защиты обрабатываемых данных установлено СЗИ Secret Net 7.0, межсетевой экран и антивирус «Kaspersky Anti-Virus».

Для разграничения прав доступа к информации передаваемой внутри подсистемы был установлен АПКШ «Континент» 3.6. Комплекс так же служит

для криптографической защиты информации передаваемой между сегментами сети и отдельными компьютерами.

Для объединения АРМ и серверов в локальную сеть используются 4 коммутатора Cisco WS-C3550-12T и маршрутизатор Cisco RVS4000.

На предприятии используются волоконно-оптические линии и кабели UTP категории 5. Все кабели находятся в пределах контролируемой зоны. Единственным передающим каналом во вне является подключение провайдера ПАО «Ростелеком» к сетевому оборудованию внутренней сети Интернет. Скорость канала 100 Мб/с.

АО «ПО «Электроприбор» имеет официальный сайт, находящимся на оборудовании сторонней организации по договору хостинга.

Структура информационной системы АО «ПО «Электроприбор» представлены на рисунке 3.

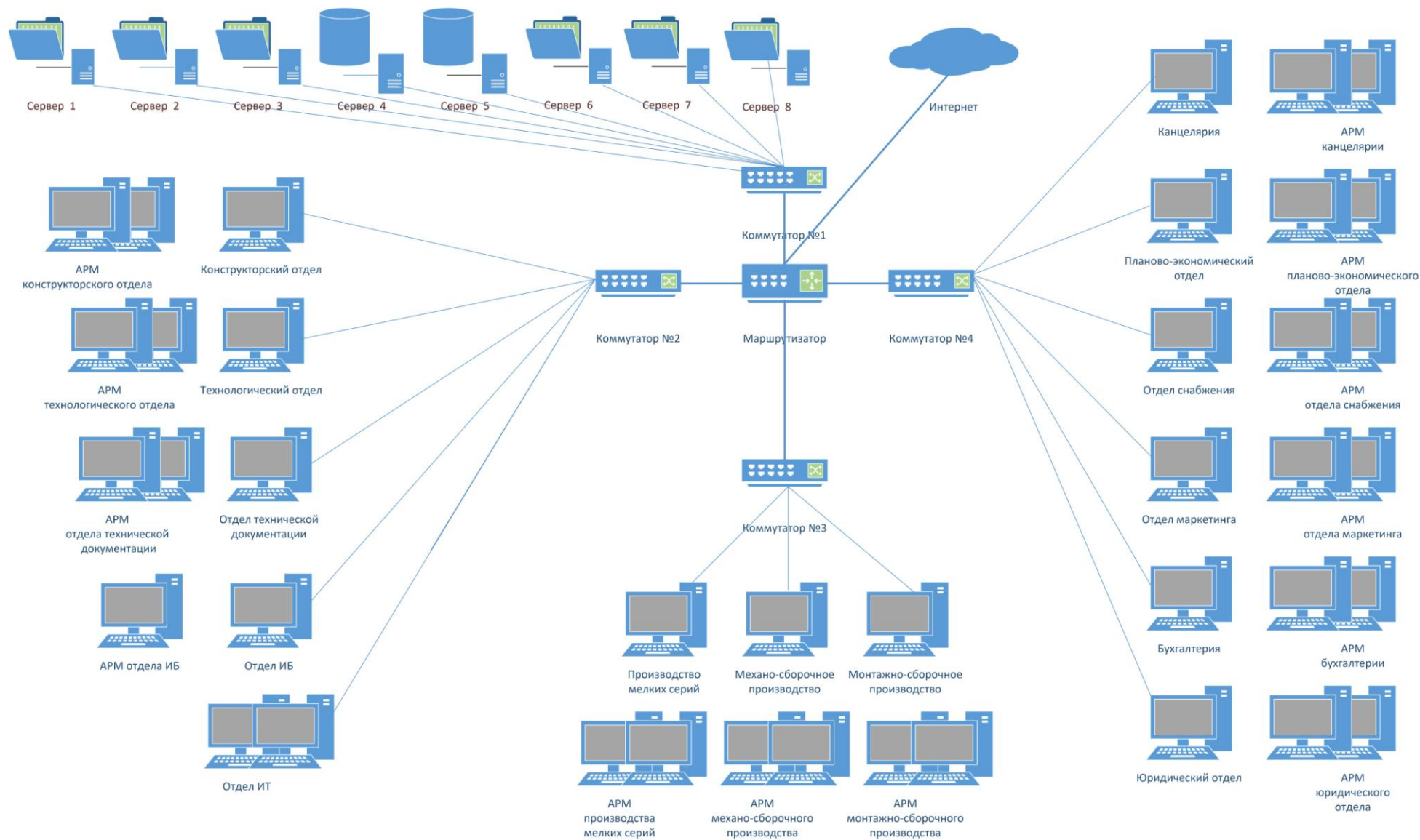


Рисунок 3 - Структура информационной системы АО «ПО «Электроприбор»

6 Классификация информационной системы

В информационной системе АО «ПО «Электроприбор» обрабатывается информация относящаяся к служебной тайне, коммерческой тайне и персональным данным. Поэтому необходимо определить класс системы с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным Приказом №17 ФСТЭК от 11.02.2017 [6].

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системы, и масштаба информационной системы: федеральный, региональный, объектовый.

Уровень значимости информации определяется степенью возможного ущерба от нарушения конфиденциальности, целостности или доступности информации, где степень возможного ущерба определяется самостоятельно экспертным или иными методами и может быть:

- высокой, если в результате нарушения одного из свойств безопасности информации возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

- средней, если в результате нарушения одного из свойств безопасности информации возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

- низкой, если в результате нарушения одного из свойств безопасности информации возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях

деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Степени ущерба для свойств безопасности информации ограниченного доступа, обрабатываемой на предприятии, приведены в таблице 2.

Таблица 2 - Степени ущерба для свойств безопасности информации

Вид информации ограниченного доступа	Свойство безопасности информации	Степень ущерба
Служебная тайна	Конфиденциальность	С
	Целостность	С
	Доступность	С
Коммерческая тайна	Конфиденциальность	С
	Целостность	С
	Доступность	Н
Персональные данные	Конфиденциальность	С
	Целостность	Н
	Доступность	С

Согласно таблице 2 уровень значимости для информации обрабатываемой на предприятии определен как средний.

Масштаб информационной системы определяется назначением и распределенностью сегментов ИС:

- информационная система имеет федеральный масштаб, если она функционирует на территории РФ (в пределах федерального округа) и имеет сегменты в субъектах РФ, муниципальных образованиях и (или) организациях;

- информационная система имеет региональный масштаб, если она функционирует на территории субъекта РФ и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях;

- информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной

власти, органа государственной власти субъекта РФ, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Информационная система АО «ПО «Электроприбор» действует только в пределах предприятия, то она имеет объектовый масштаб.

Класс защищенности информационной системы определяется в соответствии с таблицей 3.

Таблица 3 - Класс защищенности информационной системы

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Исходя из того, что уровень возможного ущерба от нарушения целостности, конфиденциальности и доступности определен как средний, то класс защищенности, в связи с масштабом информационной системы – К2.

7 Идентификация источников угроз

7.1 Понятие идентификации источников угроз

Важным этапом в процессе определения угроз безопасности информации является идентификация лиц или событий, в результате действий которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и возникновение неприемлемых негативных последствий.

Источники угроз безопасности информации могут быть следующих типов:

- антропогенные угрозы;
- техногенные угрозы;
- угрозы стихийных бедствий, иных природных явлений.

В качестве источников антропогенных угроз безопасности информации могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);
- лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

7.2 Оценка возможностей нарушителей

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-

функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

Виды нарушителей, имеющие возможность реализации угрозы в ИС и цели их действий, а также последствия от них (ущерб) приведены в таблице 4.

Таблица 4 – Виды нарушителей, цели и ущерб

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации	Вероятность проявления активности нарушителя в Министерстве
1	Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций	Низкая, в связи с недостаточной актуальностью информации, обрабатываемой в ИС
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические и политические мотивы. Дестабилизация деятельности органов государственной власти	Низкая, в связи с недостаточной актуальностью информации, обрабатываемой в ИС
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Средняя, в связи с актуальностью, но сложной реализацией и большими затратами на специалистов соответствующего уровня и необходимое оборудование
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации	Средняя, в связи с актуальностью, но сложной реализацией и большими затратами на специалистов соответствующего

Продолжение таблицы 4

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации	Вероятность проявления активности нарушителя в Министерстве
			(подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	уровня и необходимое оборудование
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием	Средняя, в связи с актуальностью, но сложной реализацией и большими затратами на специалистов соответствующего уровня и необходимое оборудование
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Высокая, в связи с актуальностью, и наличием большинства требуемых ресурсов для перехвата информации
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Средняя, в связи с актуальностью, но сложной реализацией и большими затратами на специалистов соответствующего уровня и необходимое оборудование
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Высокая, в связи с актуальностью, и наличием большинства требуемых ресурсов для перехвата информации

Продолжение таблицы 4

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации	Вероятность проявления активности нарушителя в Министерстве
	инфраструктур у оператора (администрация, охрана, уборщики и т.д.)			
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Средняя, в связи с актуальностью, но сложной реализацией и большими затратами на специалистов соответствующего уровня и необходимое оборудование
10	Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Высокая, в связи с актуальностью, и наличием большинства требуемых ресурсов для перехвата информации
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия	Средняя, в связи с актуальностью, но сложной реализацией и большими затратами на специалистов соответствующего уровня и необходимое оборудование

Для повышения своих возможностей нарушители 1 вида могут вступать в сговор с нарушителями 3, 4, 6, 7, 8, 9 и 10 видов. Нарушители 2 вида могут

вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. Нарушители 3 вида могут вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. В случае принятия таких предположений цели (мотивация) и возможности нарушителей подлежат объединению.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации в ИС нарушители обладают различными возможностями, приведёнными в таблице 5.

Таблица 5 – Потенциал, требуемый для реализации угроз безопасности информации в ИС

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации	Вероятность проявления активности нарушителя в Министерстве
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), обеспечивающие функционирование ИС или обслуживающих инфраструктуру оператора, пользователи ИС, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент ИС, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на ИС	Высокая, так как в данную группу входят большинство пользователей ИС, обслуживающего персонала и потенциальные внешние нарушители
2	Нарушители	Террористические,	Обладают всеми	Средняя, так как

Продолжение таблицы 5

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации	Вероятность проявления активности нарушителя в Министерстве
	с базовым повышенным (средним) потенциалом	экстремистские группировки, Преступные группы (криминальные структуры), Конкурирующие организации, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы ИС и администраторы безопасности	возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы	в данную группу входят часть пользователей ИС и потенциальных внешних нарушителей. Вхождение в данную группу обслуживающего персонала маловероятно
3	Нарушители с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов системному и	Средняя, так как в данную группу входят часть пользователей ИС администраторы ИС и потенциальные внешние нарушители. Вхождение в данную группу обслуживающего персонала маловероятно

Продолжение таблицы 5

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации	Вероятность проявления активности нарушителя в Министерстве
			<p>прикладному ПО, телекоммуникационному оборудованию и другим программно-техническим средствам ИС для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в ИС, об алгоритмах, аппаратных и программных средствах, используемых в ИС. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа ПО. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее.</p>	

7.3 Возможные способы реализации угроз безопасности информации

Угрозы безопасности информации могут быть реализованы нарушителями различных групп за счет одного из следующих действий:

- несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)) (НСД1);
- несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы) (НСД2);
- несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения) (НСД3);
- несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы) (НСД4);
- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации (НСД5);
- воздействия на пользователей, администраторов безопасности, администраторов ИС или обслуживающий персонал (социальная инженерия) (НСД6).

При определении способа реализации угроз безопасности информации необходимо учитывать то, что угрозы безопасности информации могут быть реализованы непосредственно за счет доступа к компонентам информационной системы и (или) информации или опосредовано (косвенно) за счет создания условий и (или) средств, обеспечивающих такой доступ, а также за счет доступа или воздействия на обслуживающую инфраструктуру, за которую оператор не отвечает. При этом локальной целью нарушителя, не имеющего доступа (прав доступа) к компонентам информационной системы и (или) информации, как правило, является получение доступа к информационной системе (в том числе через внешние сети связи общего пользования) и получение максимально возможных прав и привилегий при таком доступе.

Нарушители могут совершать действия, следствием которых является нарушение безопасности информации, преднамеренно (преднамеренные угрозы безопасности информации) или случайно (непреднамеренные угрозы безопасности информации).

Преднамеренные действия нарушителей могут заключаться в реализации целенаправленных или нецеленаправленных угроз безопасности информации.

Целенаправленная угроза безопасности информации направлена на интересующую нарушителя ИС с заранее известными ему структурно-функциональными характеристиками и особенностями функционирования. Целенаправленная угроза безопасности информации адаптирована к структурно-функциональным характеристикам ИС. При подготовке и реализации целенаправленных угроз безопасности информации нарушитель может использовать методы социальной инженерии, которые позволяют ему изучить поведение пользователей и их реакцию на поступающие к ним внешние данные.

Нецеленаправленная («веерная») угроза безопасности информации не ориентирована на конкретную информационную систему. Целями такой угрозы могут являться НСД, перехват управления или воздействие на как можно большее количество ИС. В данном случае нарушителю заранее не известны структурно-функциональные характеристики и условия функционирования ИС.

Реализация преднамеренных угроз безопасности информации, как правило, включает:

- сбор информации об информационной системе, ее структурно-функциональных характеристиках, условиях функционирования (К1);
- выбор (разработка, приобретение) методов и средств, используемых для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и условиями функционирования (К2);
- непосредственная реализация угроз безопасности информации в информационной системе (проникновение в информационную систему,

закрепление в информационной системе, реализация неправомерных действий) (К3);

- устранение признаков и следов неправомерных действий в информационной системе (К4).

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

- нарушитель может действовать один (У11) или в составе группы нарушителей (У12);

- в отношении информационной системы внешний нарушитель может действовать совместно с внутренним нарушителем (У2);

- угрозы могут быть реализованы в любое время и в любой точке информационной системы (на любом узле или хосте) (У3);

- для достижения своей цели нарушитель выбирает наиболее слабое звено информационной системы (У4).

В таблице 6 приведена модель нарушителя безопасности информации для информационной системы АО «ПО «Электроприбор».

Таблица 6 – Модель нарушителя безопасности информации ИС АО «ПО Электроприбор»

Нарушитель	Действия нарушителя	Способ реализации угроз	Вид намерений	Тип угрозы	Компоненты преднамеренной реализации угрозы	Условия способа реализации угрозы	Вероятность модели
Пользователь ИС Тип II	НСД5	Непосредств	Корыстные /случ	Целенаправл / случ	К2, К3	У11, У12, У4	Низ
	НСД1	Непосредств	Корыстные /случ	Целенаправл / случ	К1, К2, К3	У11, У4	Сред
	НСД3	Опосред	Корыстные /случ	Целенаправл / случ	К1, К2, К3	У11, У4	Низ
Администра- торы ИС Тип II	НСД5	Непосредств	Корыстные	Целенаправл	К1, К2, К3, К4	У11, У12, У3, У4	Выс
	НСД2	Непосредств	Корыстные	Целенаправл	К1, К2, К3, К4	У11, У3, У4	Выс
	НСД3	Непосредств	Корыстные	Целенаправл	К1, К2, К3, К4	У11, У3, У4	Выс
Внешний нарушитель II (для физического) I (для остальных)	НСД6	Опосред	Корыстные	Целенаправл	К2	У11, У12, У3, У4	Сред
	НСД1	Опосред	Корыстные	Целенаправл	К2	У11, У3, У4	Сред
	НСД4	Опосред	Корыстные	Целенаправл	К1, К2	У11, У3, У4	Сред

8 Определение актуальных угроз безопасности информации в информационной системе

8.1 Понятие актуальности угрозы безопасности информации

Идентифицированная угроза безопасности информации подлежит нейтрализации, если она является актуальной для информационной системы, то есть в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям [7].

Актуальность угроз безопасности информации определяется в отношении угроз, для которых экспертным методом определено, что:

- возможности (потенциал) нарушителя достаточны для реализации угрозы безопасности информации;
- в информационной системе могут иметься потенциальные уязвимости, которые могут быть использованы при реализации угрозы безопасности информации;
- структурно-функциональные характеристики и особенности функционирования информационной системы не исключают возможности применения способов, необходимых для реализации угрозы безопасности информации (существует сценарий реализации угрозы безопасности);
- реализация угрозы безопасности информации приведет к нарушению конфиденциальности, целостности или доступности информации, в результате которого возможно возникновение неприемлемых негативных последствий (ущерба).

Под вероятностью реализации угрозы безопасности информации понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация угрозы безопасности информации в

информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования. Вводятся три вербальные градации этого показателя:

- низкая вероятность – отсутствуют объективные предпосылки к реализации угрозы безопасности информации, отсутствует требуемая статистика по фактам реализации угрозы безопасности информации (возникновения инцидентов безопасности), отсутствует мотивация для реализации угрозы, возможная частота реализации угрозы не превышает 1 раза в 5 лет;

- средняя вероятность – существуют предпосылки к реализации угрозы безопасности информации, зафиксированы случаи реализации угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на возможность реализации угрозы безопасности информации, существуют признаки наличия у нарушителя мотивации для реализации такой угрозы, возможная частота реализации угрозы не превышает 1 раза в год;

- высокая вероятность – существуют объективные предпосылки к реализации угрозы безопасности информации, существует достоверная статистика реализации угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на высокую возможность реализации угрозы безопасности информации, у нарушителя имеются мотивы для реализации угрозы, частота реализации угрозы – чаще 1 раза в год.

В случае отсутствия требуемых данных для оценки вероятности реализации угрозы безопасности информации или наличия сомнений в объективности экспертных оценок при определении вербальных градаций вероятности реализации угроз безопасности информации, актуальность угрозы безопасности информации определяется на основе оценки возможности ее реализации [8]. Возможность реализации угрозы безопасности информации оценивается исходя из уровня защищенности информационной системы и

потенциала нарушителя, необходимого для реализации этой угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

8.2 Оценка уровня проектной защищенности информационной системы

При определении угроз безопасности информации на этапе создания информационной системы в случае, когда меры защиты информации не реализованы или не проведена оценка их достаточности и эффективности, оценка возможности реализации угрозы безопасности информации проводится относительно уровня проектной защищенности информационной системы.

Под уровнем проектной защищенности понимается исходная защищенность информационной системы, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования. Уровень проектной защищенности определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице 7.

Таблица 7 - Показатели, характеризующие проектную защищенность ИС

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы		
	Высокий	Средний	Низкий
1. По структуре информационной системы: локальная информационная система		+	
2. По используемым информационным технологиям: системы на основе виртуализации		+	
3. По архитектуре информационной системы: файл-серверные системы		+	
4. По наличию (отсутствию) взаимосвязей с иными информационными системами: взаимодействующая с системами;	+		
5. По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего	+		

Продолжение таблицы 7

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы		
	Высокий	Средний	Низкий
пользования: подключенная			
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: выделение рабочих мест для администрирования в отдельный домен;		+	
10. По подходам к сегментированию информационной системы: с сегментированием		+	

В ходе создания информационной системы социального управления администрации города ее проектной защищенности определяется следующим образом:

а) информационная система имеет высокий уровень проектной защищенности, если не менее 80% характеристик информационной системы соответствуют уровню «высокий» (суммируются положительные решения по второму столбцу, соответствующему высокому уровню защищенности), а остальные — среднему уровню защищенности (положительные решения по третьему столбцу);

б) информационная система имеет средний уровень проектной защищенности, если не выполняются условия по пункту а) и не менее 90% характеристик информационной системы соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по третьему столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности;

в) информационная система имеет низкий уровень проектной защищенности, если не выполняются условия по пунктам а) и б).

Так как 90% характеристик информационной системы соответствуют уровню не ниже среднего, то информационная система имеет средний уровень проектной защищенности.

8.3 Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в информационной системе

Потенциал, требуемый нарушителю для реализации угрозы безопасности информации, может быть базовым, базовым повышенным или высоким. Данная методика применяется для оценки потенциала, необходимого для реализации угрозы безопасности информации.

Приведенный подход к оценке потенциала нарушителя направлен на снижение уровня субъективности и неопределенности при оценке потенциала нарушителя, который требуется для реализации угрозы безопасности информации в телекоммуникационной системе (ТС) с заданными структурно-функциональными характеристиками и особенностями функционирования.

При оценке потенциала нарушителя необходимо исходить из того, что для успешного достижения целей реализации угроз безопасности информации, нарушителю необходимо осуществить подготовку к реализации угрозы и непосредственно реализацию угрозы безопасности информации. При этом не единственным, но необходимым условием на этапе подготовки к реализации угрозы безопасности информации является идентификация уязвимостей в информационной системе, а на этапе реализации угрозы безопасности информации – использование уязвимостей ТС.

Таким образом, 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. Для

проведения указанной оценки делается предположение о наличии уязвимостей, которые потенциально содержатся в ТС и могут быть использованы для реализации угрозы безопасности информации.

Оценка возможностей нарушителя по идентификации и использованию уязвимости в информационной системе проводится по результатам определения следующих показателей:

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

Полученные значения характеристик потенциала нарушителя суммируются. Полученная сумма значений характеристик соотносится с диапазонами значений, приведенных в таблице 8, в соответствии с которой определяется потенциал нарушителя, необходимый для реализации угрозы безопасности информации.

Таблица 8 – Определение потенциала нарушителя

Диапазон значений	Потенциал нарушителя
менее 10	Потенциал недостаточен для реализации угрозы
10-17	Базовый (низкий)
18-24	Базовый повышенный (средний)
более 24	Высокий

Потенциал нарушителя, необходимый для реализации угрозы УБИ.008 приведен в таблице 9.

Таблица 9 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.008

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	4
Техническая компетентность нарушителя	Специалист	3
Знание проекта и информационной системы	Ограниченные знания	2
Возможность доступа к информационной системе	За часы	3
Оснащенность нарушителя	Стандартное оборудование	4

Сумма значений равна 16, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя, необходимый для реализации угрозы УБИ.031 Угроза использования механизмов авторизации для повышения привилегий приведен в таблице 10.

Таблица 10 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.031

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	4
Техническая компетентность нарушителя	Специалист	4
Знание проекта и информационной системы	Ограниченные знания	3
Возможность доступа к информационной системе	За минуты	2
Оснащенность нарушителя	Стандартное оборудование	3

Сумма значений равна 16, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя, необходимый для реализации угрозы УБИ.038 Угроза исчерпания вычислительных ресурсов хранилища больших данных приведен в таблице 11.

Таблица 11 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.038

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	2
Техническая компетентность нарушителя	Специалист	3
Знание проекта и информационной системы	Ограниченные знания	2
Возможность доступа к информационной системе	За часы	4
Оснащенность нарушителя	Стандартное оборудование	3

Сумма значений равна 14, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя необходимый для реализации угрозы УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией приведен в таблице 12.

Таблица 12 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.067

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	2
Техническая компетентность нарушителя	Специалист	3
Знание проекта и информационной системы	Ограниченные знания	3
Возможность доступа к информационной системе	За часы	4
Оснащенность нарушителя	Стандартное оборудование	3

Сумма значений равна 15, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя, необходимый для реализации угрозы УБИ.074 приведен в таблице 13.

Таблица 13 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.074

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	2
Техническая компетентность нарушителя	Специалист	3
Знание проекта и информационной системы	Ограниченные знания	2
Возможность доступа к информационной системе	За часы	3
Оснащенность нарушителя	Стандартное оборудование	3

Сумма значений равна 13, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя, необходимый для реализации угрозы УБИ.091 приведен в таблице 14

Таблица 14 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.091

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	2
Техническая компетентность нарушителя	Специалист	4
Знание проекта и информационной системы	Ограниченные знания	4
Возможность доступа к информационной системе	За часы	4
Оснащенность нарушителя	Стандартное оборудование	2

Сумма значений равна 16, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя, необходимый для реализации угрозы УБИ.162 Угроза неправомерного ознакомления с защищаемой информацией приведен в таблице 15.

Таблица 15 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.162

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	2
Техническая компетентность нарушителя	Специалист	2
Знание проекта и информационной системы	Ограниченные знания	3
Возможность доступа к информационной системе	За часы	2
Оснащенность нарушителя	Стандартное оборудование	3

Сумма значений равна 12, значит потенциал нарушителя определен как базовый (низкий).

Потенциал нарушителя, необходимый для реализации угрозы УБИ.187 Угроза несанкционированного воздействия на средство защиты информации приведен в таблице 16.

Таблица 16 – Потенциал нарушителя, необходимый для реализации угрозы УБИ.187

Показатель возможности нарушителя		Значения
Затрачиваемое время	За часы	2
Техническая компетентность нарушителя	Специалист	3
Знание проекта и информационной системы	Ограниченные знания	3
Возможность доступа к информационной системе	За часы	2
Оснащенность нарушителя	Стандартное оборудование	3

Сумма значений равна 13, значит потенциал нарушителя определен как базовый (низкий).

8.4 Оценка возможности реализации угрозы безопасности информации и актуальности угроз

Возможность реализации угрозы безопасности информации в зависимости от уровня защищенности информационной системы и потенциала нарушителя определяется как высокая, средняя или низкая в соответствии с таблицей 17.

Таблица 17 – Возможность реализации угроз безопасности информации

Потенциал нарушителя	Уровень защищенности		
	Высокий	Средний	Низкий
Базовый (низкий)	Низкая	Средняя	Высокая
Базовый повышенный (средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

На основании данной таблицы была определена возможность реализации каждой из угроз. Возможности реализации угроз приведены в таблице 18.

Таблица 18 – Возможности реализации угроз

Угроза	Уровень защищенности	Потенциал нарушителя	Возможность реализации угрозы
УБИ.008 Угроза восстановления аутентификационной информации	Средний	Базовый (низкий)	Средняя
УБИ.031 Угроза использования механизмов авторизации для повышения привилегий	Средний	Базовый (низкий)	Средняя
УБИ.038 Угроза исчерпания вычислительных ресурсов хранилища больших данных	Средний	Базовый (низкий)	Средняя
УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией	Средний	Базовый (низкий)	Средняя
УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	Средний	Базовый (низкий)	Средняя
УБИ.091 Угроза несанкционированного удаления защищаемой информации	Средний	Базовый (низкий)	Средняя
УБИ.162: Угроза эксплуатации цифровой подписи программного кода	Средний	Базовый (низкий)	Средняя
УБИ.187: Угроза несанкционированного воздействия на средство защиты информации	Средний	Базовый (низкий)	Средняя

Актуальность угрозы безопасности информации определяется на основе оценки возможности реализации угрозы безопасности информации и степени ущерба.

Степень возможного ущерба была определена как средняя.

Была определена актуальность угроз на основе степени ущерба и возможности реализации угроз по таблице 19.

Таблица 19 – Определение актуальности угроз

Вероятность (возможность) реализации угрозы	Степень возможного ущерба		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

На основании таблицы 20 была определена актуальность каждой идентифицированной угрозы. Результат приведен в таблице 8.

Таблица 20 – Определение актуальности угроз

Угроза	Возможность реализации угрозы (Yj)	Степень возможного ущерба (Xj)	Актуальность угрозы
УБИ.008 Угроза восстановления аутентификационной информации	Низкая	Низкая	Актуальная
УБИ.031 Угроза использования механизмов авторизации для повышения привилегий	Средняя	Средняя	Актуальная
УБИ.038 Угроза исчерпания вычислительных ресурсов хранилища больших данных	Низкая	Низкая	Актуальная
УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией	Средняя	Средняя	Актуальная
УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	Низкая	Средняя	Актуальная
УБИ.091 Угроза несанкционированного	Средняя	Средняя	Актуальная

Продолжение таблицы 20

Угроза	Возможность реализации угрозы (Yj)	Степень возможного ущерба (Xj)	Актуальность угрозы
удаления защищаемой информации			
УБИ.162: Угроза эксплуатации цифровой подписи программного кода	Средняя	Средняя	Актуальная
УБИ.187: Угроза несанкционированного воздействия на средство защиты информации	Средняя	Средняя	Актуальная

На основании полученной информации была разработана Модель угроз информационной системы АО «ПО «Электроприбор», которая приведена в Приложении А.

9 Определение требований к системе защиты информации информационной системы

9.1 Порядок определения требований к системе защиты информации информационной системы

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

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17 [7].

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в

информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной

инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

9.2 Выбор мер защиты информации информационной системы

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

- определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации;
- адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы;
- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование всех угроз безопасности информации, включенных в модель угроз безопасности информации;
- дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 [8].

Выбор мер защиты информации осуществляется исходя из класса защищенности информационной системы, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз безопасности информации, включенных в модель угроз безопасности информационной системы, а также с учетом структурно-функциональных характеристик информационной системы, к которым относятся структура и состав информационной системы, физические, логические, функциональные и

технологические взаимосвязи между сегментами информационной системы, взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

Правила и процедуры по реализации требований о защите информации и мер защиты информации в конкретной информационной системе определяются в эксплуатационной документации на систему защиты информации и организационно-распорядительных документах по защите информации.

Эксплуатационная документация на систему защиты информации разрабатывается с учетом национальных стандартов и, как правило, включает руководства пользователей и администраторов, инструкцию по эксплуатации комплекса средств защиты информации и иных технических средств, описание технологического процесса обработки информации, общее описание информационной системы, формуляр и паспорт информационной системы.

Организационно-распорядительные документы по защите информации включают, как правило, политики, стандарты организации, положения, планы, перечни, инструкции или иные виды документов, разрабатываемые оператором для регламентации процедур защиты информации в информационной системе в ходе ее эксплуатации.

Информационной системе АО «ПО «Электроприбор» по требованиям защиты информации рассматриваемой информационной системы присвоен класс К2. В соответствии с данным классом, согласно приказа ФСТЭК России от 11 февраля 2013 г. N 17 выбраны следующие меры защиты, приведённые в таблице 21 [7].

Таблица 21 — ЗМ соответствующего класса защищенности

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационной системы
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа	
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+
УПД.7	Предупреждение пользователя при его входе в	

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
	информационную систему о том, что в информационной системе реализованы меры защиты информации, и о Необходимости соблюдения им установленных оператором правил обработки информации	
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему	
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+
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	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	+
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 (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+
ОПС.4	Управление временными файлами, в том числе запрет,	

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
	разрешение, перенаправление записи, удаление временных файлов	
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет машинных носителей информации	+
ЗНИ.2	Управление доступом к машинным носителям информации	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах	
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	
ЗНИ.7	Контроль подключения машинных носителей информации	
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+
V. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+
РСБ.7	Защита информации о событиях безопасности	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	
VI. Антивирусная защита (ABЗ)		
ABЗ.1	Реализация антивирусной защиты	+

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+
VII. Обнаружение вторжений (COB)		
COB.1	Обнаружение вторжений	+
COB.2	Обновление базы решающих правил	+
VIII. Контроль (анализ) защищенности информации (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+
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.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы	
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	
ОЦЛ.7	Контроль точности, полноты и правильности данных,	

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
	вводимых в информационную систему	
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	
X. Обеспечение доступности информации (ОДТ)		
ОДТ.1	Использование отказоустойчивых технических средств	
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации	+
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала	+
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов	
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации	+
XI. Защита среды виртуализации (ЗСВ)		
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	+

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	+
XII. Защита технических средств (ЗТС)		
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы	+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным	+

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
	каналам связи	
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)	
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами	
ЗИС.7	Контроль санкционированного и исключение несанкционированного 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 санкционированного и исключение несанкционированного 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 санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	+
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам	
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	+
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	+
ЗИС.14	Использование устройств терминального доступа для обработки информации	
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного	+

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
	обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов	
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения	
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти	
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы	
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	+
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	+
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	+
ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)	
ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем	
ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации	
ЗИС.28	Воспроизведение ложных и (или) скрывание истинных	

Продолжение таблицы 21

Условное обозначение и номер меры	Меры защиты информации в информационной системе	Класс защищенности информационно й системы
	отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы	
ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновения отказов (сбоев) в системе защиты информации информационной системы	
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	+

Знак «+» означает, что мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы.

Далее была проведена адаптация и уточнение набора мер.

Адаптированный и уточненный набор мер приведен в таблице 22.

Таблица 22 — Уточненный перечень ЗМ

Мера по обеспечению безопасности ПДн	Адаптаци я	Уточнени е	Обоснование
ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+		Исключена из набора мер в связи с отсутствием внешних пользователей, не являющихся сотрудником предприятия.
УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+		Исключена из набора мер в связи с отсутствием технологий беспроводного доступа в организации.
ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения		+	Добавлена для контроля за внедрением вредоносного ПО.
ЗНИ.4 Исключение возможности несанкционированного		+	Добавлена для предотвращения утечки

Продолжение таблицы 22

Мера по обеспечению безопасности ПДн	Адаптаци я	Уточнени е	Обоснование
ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах			персональных данных путем несанкционированного доступа к ним.
ОЦЛ.7 Контроль точности, полноты и правильности данных, вводимых в информационную систему		+	Добавлена для предотвращения введения ложной информации.
ЗСВ Защита среды виртуализации	+		Исключены все меры, связанные со средой виртуализации в связи с ее отсутствием.
ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования		+	Добавлена для предотвращения утечки данных путем несанкционированного доступа к стационарным техническим средствам, обрабатывающим информацию, и средствам защиты информации, а также средствам обеспечения функционирования.
ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе	+		Исключена из набора мер в связи с отсутствием беспроводных соединений в организации.

Было определено какие защитные меры из адаптированного набора мер нейтрализуют угрозы для ИС, что приведено в таблице 23.

Таблица 23 — Уточненный и адаптированный набор мер защиты с нейтрализуемыми угрозами

Условное обозначение и номер меры	Меры защиты информации в информационной системе
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в

Продолжение таблицы 23

Условное обозначение и номер меры	Меры защиты информации в информационной системе
	случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, односторонняя передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники
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 (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или)

Продолжение таблицы 23

Условное обозначение и номер меры	Меры защиты информации в информационной системе
	использования носителей информации в иных информационных системах
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
V. Регистрация событий безопасности (РСБ)	
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов)

Продолжение таблицы 23

Условное обозначение и номер меры	Меры защиты информации в информационной системе
	и иной информации, не относящихся к функционированию информационной системы (защита от спама)
X. Обеспечение доступности информации (ОДТ)	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
ЗИС.7	Контроль санкционированного и исключение несанкционированного 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 санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация

Продолжение таблицы 23

Условное обозначение и номер меры	Меры защиты информации в информационной системе
	событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи
ЗИС.9	Контроль санкционированной и исключение несанкционированной 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 (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения

10 Разработка организационных и организационно-технических мер при обработке информации в информационной системе

Организационные и организационно-технические меры по защите информации предполагают мероприятия и действия по эффективному применению и использованию технических средств регламентации и управления доступом к защищаемой информации, а также по порядку и режимам работы технических средств защиты информации.

Регламентация обеспечивает безопасность информации установлением ограничений режима, времени и территории в деятельности сотрудников и работе технических средств.

Регламентация предусматривает:

- определение и установка границ контролируемых и охраняемых зон;
- определение уровней защиты информации;
- регламентация деятельности работников предприятия и посетителей;
- определение режимов работы средств обработки, сбора и хранения защищаемой информации на АРМ, других технических средств, а так же передачи документов содержащих информацию ограниченного доступа.

Мероприятия по управлению доступом к информации включают:

- идентификацию лиц и обращений;
- проверку полномочий лиц и обращений;
- регистрацию обращений к защищаемой информации;
- реагирование на обращения к информации.

Для опознавания пользователей, сотрудников, посетителей либо иных лиц при обращении к информационной системе происходит их идентификация.

Проверка полномочий представляет собой проверку прав лиц и обращений по каналам связи на доступ к информации доступ к которой ограничен. В случае если уровень полномочий для доступа к информации ниже разрешенного, то в доступе должно быть отказано. Регистрация и протоколирование обращений к носителям с информацией ограниченного

доступа осуществляется путем записи в карточках, журналах и в электронных носителях, что обеспечивает контроль их прохождения.

При запросе к защищаемой информации требуется либо выдача разрешения на доступ к информации, либо в отказе. Если отказ на выдачу был получен в результате попытки злоумышленником несанкционированного доступа к защищаемой информации то должно произойти включение сигнализации, оповещение охраны, службы безопасности или правоохранительных органов.

Контроль эффективности защиты - важное и необходимое направление работ по защите информации ограниченного доступа. Эти работы силы службы безопасности, а также руководители структурных подразделений проводят своими силами. Контроль защиты информации на предприятии включает в себя контроль организационно-технических мер защиты и подразумевает установление (определение) и измерения показателей эффективности мер защиты техническими средствами и сравнении их с нормативными.

Контроль бывает трех видов:

- предварительный;
- периодический;
- постоянный.

Любые изменения состава, структуры, алгоритма работы системы защиты информации требуют проведения предварительного контроля. Предварительный контроль так же проводится после:

- установки нового технического средства защиты;
- изменения организационных мер;
- проведения работ по ремонту и профилактики средств защиты информации;
- устранения выявленных нарушений в системе защиты.

Цель периодического контроля состоит в организации систематического контроля уровней защиты. Периодический контроль проводится выборочно по

планам, утвержденным вышестоящими органами или руководителем организации.

Контроль производится самими сотрудниками организации в части источников информации, с которыми они работают.

Целью общего периодического контроля является тщательная проверка работоспособности всех частей, элементов и системы защиты информации в целом. Общий периодический контроль проводится в рамках всей организации 2 раза в год.

Силами службы безопасности и сотрудников предприятия осуществляется постоянный контроль с целью установления объективной оценки уровня мер защиты информации и в обнаружении уязвимостей информационной безопасности в системе защиты предприятия. Помимо этого, такой контроль оказывает сильное психологическое влияние на сотрудников, требуя от них более тщательного выполнения требований по обеспечению защиты информации.

Как и меры защиты, меры контроля представляют совокупность организационных и технических мероприятий, цель проведения которых заключается в проверке выполнения установленных требований и норм по обеспечению защиты информации. Организационные меры контроля включают:

- проверку выполнения сотрудниками требований руководящих документов по защите информации;

- проверку работоспособности средств охраны и защиты информации от наблюдения, подслушивания, перехвата и утечки информации по техническим каналам (наличие занавесок, штор, жалюзей на окнах, чехлов на разрабатываемых изделиях, состояние звукоизоляции, экранов, средств подавления опасных сигналов и зашумления, емкостей для сбора отходов с демаскирующими веществами и т. д.);

- контроль за выполнением инструкций по защите информации о разрабатываемой продукции;

- оценку эффективности применяемых мер и средств защиты информации.

Технические меры контроля проводятся с использованием технических средств радио - и электроизмерений, анализа физического состояния и обеспечивают проверку:

- напряженности полей с информацией на границах контролируемой зоны;

- уровней опасных сигналов и помех возникающих в проводах, элементах конструкций, средств заземления и экранах кабелей, выходящих за пределы контролируемой зоны;

- степени зашумления генераторами помех информативного сигнала при обработке защищаемой информации.

11 Обзор существующих технических и программных средств защиты информации

Средства защиты от несанкционированного доступа - программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации. В соответствии с законодательством Российской Федерации, в информационных системах ряда организаций использование сертифицированных программных продуктов является обязательным. К таким организациям относятся:

- государственные организации;
- негосударственные организации, работающие со служебной информацией государственных органов;
- организации, работающие с персональными данными.

В большинстве случаев выбор средств защиты информации осуществляться в рамках множества сертифицированных решений различных брендов. На самом деле сертифицированы сотни программных и программно-аппаратных средств защиты, однако большая часть была сертифицирована в единичном экземпляре или в составе партии, и приобрести их не представляется возможным. В таблице 24 приведены некоторый из СЗИ от НСД с описанием их функциональных возможностей.

Таблица 24 - СЗИ от НСД с описанием функциональных возможностей

Название технического средства	Возможности технического средства	Наличие сертификата соответствия
КРИПТОН-ЗАМОК	<ul style="list-style-type: none">– идентификация и аутентификация пользователей до запуска BIOS компьютера (большой выбор типов ключевых носителей (смарт-карты с открытой и защищенной памятью, микропроцессорные смарт-карты, Touch Memory) [9];– создание нескольких профилей защиты, надежное разграничение ресурсов компьютера, принудительная загрузка операционной системы (ОС) с выбранного	ФСБ России СФ/527-3207 Срок действия до 31.03.2021 г.

Название технического средства	Возможности технического средства	Наличие сертификата соответствия
	<p>устройства в соответствии с индивидуальными настройками администратора для каждого пользователя;</p> <ul style="list-style-type: none"> – блокировка компьютера при НСД, накопление и ведение электронного журнала событий (в собственной энергонезависимой памяти); – подсчет эталонных значений контрольных сумм объектов и проверка текущих значений контрольных сумм (рассчитываются по алгоритму вычисления хэш-функции по ГОСТ Р34.11-94), экспорт/импорт списка проверяемых объектов на гибкий магнитный диск; – интеграция в другие системы безопасности (сигнализация, пожарная охрана и пр.); – организация бездисковых рабочих мест на основе встроенного Флеш-диска 16 Мбайт; 	
Secret Disk (версия 5)	<ul style="list-style-type: none"> – шифрование системного раздела, разделов на жестких дисках, томов на динамических дисках, виртуальных дисков и съемных носителей; – аутентификация пользователя по USB-ключу eToken для загрузки операционной системы и для доступа к зашифрованным данным; – запрет доступа по сети к зашифрованным данным для всех пользователей, включая системного администратора; – восстановление доступа к данным в случае утери USB-ключа; – защита данных от сбоев во время операций шифрования, включая перебои электропитания; – режим энергосбережения для ноутбуков; – динамическое распределение скорости шифрования. 	<p>ФСТЭК России №3742 Срок действия до 12.05.2020г.</p>
Аккорд-АМДЗ	<ul style="list-style-type: none"> – защита ресурсов АРМ от лиц, не допущенных к работе; – аутентификацию пользователей; – блокировку загрузки с отчуждаемых носителей; – контроль целостности аппаратной платформы; – контроль целостности программ и данных; – доверенную загрузку системного и 	<p>ФСТЭК России №246/7 Срок действия до 13.08.2019 г.</p>

Название технического средства	Возможности технического средства	Наличие сертификата соответствия
	<p>прикладного ПО;</p> <ul style="list-style-type: none"> – регистрацию пользователей на ПЭВМ; – регистрацию контролируемых событий в системном журнале; – возможность физической коммутации устройств; – администрирование встроенного ПО комплекса; – аудит событий; – разграничение доступа пользователей и программ. 	
ПАК «Соболь»	<ul style="list-style-type: none"> – идентификация и аутентификация пользователей по электронным идентификаторам Touch Memory; – регистрация попыток доступа к ПЭВМ; – запрет загрузки ОС с внешних носителей (FDD, CD-ROM, ZIP, LPT, SCSI-порты) на аппаратном уровне; – контроль целостности операционной системы (ОС), прикладного программного обеспечения и файлов пользователя до загрузки ОС. 	<p>ФСТЭК России №1574 Срок действия до 14.03.2020 г.</p>
Secret Net 7.0	<ul style="list-style-type: none"> – аутентификация пользователей [10]; – разграничение доступа пользователей к информации и ресурсам автоматизированной системы; – доверенная информационная среда; – контроль утечек и каналов распространения конфиденциальной информации; – контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации; – затирание остаточной информации при освобождении и удалении областей памяти компьютера и запоминающих устройств; – централизованное управление системой защиты, оперативный мониторинг и аудит безопасности; – масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов; – защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов (VDI); 	<p>ФСТЭК России №2707 Срок действия до 07.09.2018г.</p>

Название технического средства	Возможности технического средства	Наличие сертификата соответствия
Dallas Lock 7.7	<ul style="list-style-type: none"> – защита информации от несанкционированного доступа на ПЭВМ в ЛВС через терминальный и сетевой вход [11]; – разграничение полномочий пользователей по доступу к ресурсам файловой системы; – контроль доступа к реестру, контроль целостности, аудит событий; – очистка остаточной информации; – защита данных путем преобразования диска (кодирования); – разграничение доступа к устройствам, контроль аппаратной конфигурации; – возможность создания замкнутой программной среды; – разграничение доступа при сетевом взаимодействии; – сетевое администрирование, включая удаленную настройку и просмотр журналов. 	ФСТЭК России №2209 Срок действия до 19.11.2019г.
ПАК ViPNet IDS 2.0	<ul style="list-style-type: none"> – безопасное хранение конфиденциальных материалов на жестких дисках компьютеров; – разграничение доступа к информации, хранимой на компьютере, используемом несколькими лицами; – защиту информации на мобильных и карманных компьютерах, дискетах и любых других носителях; подготовку конфиденциальных материалов на любых носителях информации для пересылки в зашифрованном виде с использованием традиционной и электронной почты. 	ФСТЭК России №3285 Срок действия до 01.07.2018г.

Рынок средств криптографической защиты информации (СКЗИ) подразумевает те решения, в которых применяются криптографические технологии, средства и алгоритмы — шифрование информации, ее хэширование, а также электронная цифровая подпись данных.

В таблице 25 приведены примеры некоторых продуктов СКЗИ с описанием их функциональных возможностей.

Таблица 25 - Примеры продуктов СКЗИ

Название технического средства	Возможности технического средства	Наличие сертификата соответствия
DioNIS Security Server v.6.0	<ul style="list-style-type: none"> – маршрутизация на любой тип интерфейса. – инкапсуляция IP в X.25. – управление доступом для абонентов ПАК Дионис, по расписанию. – контроль целостности файлов при старте системы. – максимум 4000 абонентов. – неограниченное число TCP-сессий через маршрутизатор. 	ФСТЭК России № 359/5 Срок действия до 03.05.2018г
АПКШ «Континент» 3.6	<ul style="list-style-type: none"> – межсетевое экранирование; – безопасный доступ пользователей VPN к ресурсам сетей общего пользования; – криптографическая защита передаваемых данных в соответствии с ГОСТ 28147–89; – межсетевое экранирование – защита внутренних сегментов сети от несанкционированного доступа; – безопасный доступ удаленных пользователей к ресурсам VPN-сети; – создание информационных подсистем с разделением доступа на физическом уровне. 	ФСТЭК России №2648 Срок действия до 31.05.2018г
КРИПТОПРО CSP 3.6	<ul style="list-style-type: none"> – формирование секретных ключей на различные типы носителей; – возможность генерации ключей с различными параметрами; – криптографическая защита информации. – формирование электронной цифровой подписи; – опциональное использование пароля (PIN-кода) для дополнительной защиты ключевой информации; – реализация мер защиты информации пользователя от НСД. 	ФСБ России № СФ/124-2917 Срок действия до 31.10.2018г

Продолжение таблицы 25

Название технического средства	Возможности технического средства	Наличие сертификата соответствия
Удостоверяющий Центр ViPNet	<ul style="list-style-type: none"> – информационный обмен, связанный с обеспечением работы инфраструктуры ЭЦП, производится в зашифрованном виде; – служебный информационный обмен по ЭЦП программное обеспечение ViPNet на клиентских станциях обеспечивает криптографический контроль целостности справочников сертификатов Главных абонентов УКЦ; – межсетевой экран ViPNet, защищающий УКЦ, совмещен с сервером; – центр управления и УКЦ ViPNet могут обеспечить автоматическое защищенное взаимодействие более чем с 65 000 сетевыми узлами. 	ФСБ России № СФ/128-2932 Срок действия до 10.08.2019г

Для защиты информационной системы предприятия от вредоносного ПО требуется наличие антивирусной защиты. В таблице 26 приведены некоторые из таких программ, с описанием их функциональных возможностей.

Таблица 26 – Примеры средств антивирусной защиты

Название ПО	Возможности ПО	Наличие сертификата соответствия
Kaspersky Endpoint Security 8	<ul style="list-style-type: none"> – защита файловой системы компьютера от проникновения вредоносных программ; – проверка входящих и исходящих почтовые сообщения на наличие в них вирусов и других вредоносных программ; – защита информации при использовании программ для мгновенного обмена сообщениями; – фильтрация и контроль входящего на компьютер трафика в соответствии с заданными сетевыми правилами; – отслеживание во входящем сетевом трафике активности, характерной для сетевых атак; – предоставление информации о текущей сетевой активности компьютера; – сбор данных о действиях программ на компьютере и предоставление этой информации другим компонентам для более эффективной защиты компьютера; 	ФСТЭК России №2682 Срок действия до 26.07.2018г

Продолжение таблицы 26

Название ПО	Возможности ПО	Наличие сертификата соответствия
ESET NOD32 Smart Security Business Edition 5	<ul style="list-style-type: none"> — защита от вредоносных программ; — защита сети; — контроль устройств; — web-антивирус; — web-фильтрация; — защита электронной почты; — централизованное управление антивирусной защитой; — управление удаленной установкой ESET Endpoint Security 5.0 на защищаемые компьютеры; — удаленное управление конфигурацией и функциями клиентов на защищаемых компьютерах. 	Отсутствует
Dr.Web Enterprise Security Suite	<ul style="list-style-type: none"> — централизованная защита всех узлов сети; — комплексная защита рабочих станций от угроз; — возможность установки агентской части на уже зараженную машину и высокая доля вероятности излечения; — управление всей инфраструктурой защиты сети с одного рабочего; — реализация необходимых для конкретного предприятия и отдельных групп сотрудников политик безопасности; — назначение отдельных администраторов для различных групп; — настройка политик безопасности для любых типов пользователей; — защита любых сетей, в том числе не имеющих доступа в Интернет; — возможность использования большинства существующих баз данных; 	ФСТЭК России №3509 Срок действия до 27.01.2019 г

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС- линейное зашумление. В таблице 27 представлены средства защиты от утечек побочных электромагнитных излучений.

Таблица 27 - Средства защиты от утечек побочных электромагнитных излучений

Название устройства	Описание	Характеристики
Генератор шума ГШ-2500М	<p>Стационарный генератор шума ГШ-2500М предназначен для маскировки информативных побочных электромагнитных излучений и наводок (ПЭМИН) персональных компьютеров, рабочих станций на объектах вычислительной техники 1, 2, и 3 категорий путем формирования и излучения в окружающее пространство электромагнитного поля шума и наведения шумового сигнала в отходящие цепи и инженерные коммуникации в широком диапазоне частот [12].</p> <p>Один генератор обеспечивает маскировку (защиту) информации устройств вычислительной техники, размещенной в помещении площадью примерно 40 м².</p> <p>Отличительной особенностью генератора является использование рамочной антенны для создания пространственного зашумления. Генератор шума формирует сигнал с помощью специальных индукторов ИС11-01 и ИС11-02 в токопроводящие коммуникационные линии (например, электропитания и заземления) с заданными параметрами мощности.</p> <p>Генератор шума «Старкад-11» может устанавливаться в выделенных помещениях до второй категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты.</p>	<p>– диапазон частот шумового сигнала - от 100 кГц до 2 ГГц;</p> <p>– спектральная плотность шума от 45 до 75 дБ;</p> <p>– индикация работы - световая и звуковая;</p> <p>– питание - 220 В, 50 Гц;</p> <p>– длина - 700 мм (с антенной);</p> <p>– ширина - 600 мм (с антенной);</p> <p>– высота - 35 мм;</p>
ЛГШ-513	<p>Генератор шума по цепям электропитания, заземления и ПЭМИН «ЛГШ-513» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем</p>	<p>– диапазон частот шумового сигнала - от 10 кГц до 30 МГц;</p> <p>– спектральная плотность шума от 25 до 50 дБ;</p> <p>– индикация работы - световая и звуковая;</p> <p>– питание - 187 В-242 В, 50 Гц; длина - 230 мм (с антенной);</p> <p>– ширина - 110 мм (с антенной);</p>

Продолжение таблицы 27

Название устройства	Описание	Характеристики
	<p>формирования маскирующих шумоподобных помех.</p> <p>Изделие «ЛГШ-513» соответствует:</p> <p>типу «А» - средства активной защиты информации от утечки за счет побочных электромагнитных излучений;</p> <p>типу «Б» - средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.</p>	<p>антенной);</p> <p>– высота - 50 мм;</p>
Соната-РЗ.1	<p>Средство активной защиты информации "Соната-РЗ.1" предназначено для защиты информации от утечки за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие проводные коммуникации [13]. "Соната РЗ.1" обеспечивает защиту путем излучения в окружающее пространство электромагнитное поля шума, а также инъекции шумовых токов в линии сети электропитания и заземления.</p> <p>"Соната-РЗ.1" является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа "А" и "Б", соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 2 классу защиты, может применяться в выделенных помещениях до 2 категории включительно.</p>	<p>– диапазон частот шумового сигнала - от 10 кГц до 2</p> <p>– спектральная плотность шума от 50 до 90 дБ;</p> <p>– индикация работы - световая и звуковая; питание - 220 В, 50 Гц;</p> <p>– диаметр - 65 мм;</p> <p>– высота - 325 мм;</p>

12 Выбор и обоснование технических и программных средств защиты информации для информационной системы

На основании требований защитных мер разработанных в параграфе 9.2 для информационной системы АО «ПО «Электроприбор» наиболее предпочтительным вариантом является использование СКЗИ от НСД Secret Net 7.0, т.к. его можно использовать для защиты конфиденциальной информации и государственной тайны в автоматизированных системах до класса 1 Б включительно, информационных систем персональных данных до класса К1 включительно [14]. Кроме того, помимо возможностей защиты от несанкционированного доступа, он может выполнять возможности межсетевого экрана, системы обнаружения вторжений и антивируса. Функционал данного ПО наиболее полно удовлетворяет требованиям системы.

Использование АПКШ «Континент» 3.6 обусловлено тем, что его использование для разграничения прав доступа к информации передаваемой внутри подсистемы, а так же служит для криптографической защиты информации передаваемой между сегментами сети и отдельными компьютерами.

Использование программного комплекса Удостоверяющий Центр ViPNet обусловлено тем, что он наиболее полно удовлетворяет требованиям системы для работы с электронно-цифровой подписью.

Все основные и вспомогательные технические средства и системы, а также специальные технические средства, на которых обрабатывается информация ограниченного доступа, не составляющая государственную тайну, прошли спецпроверку и специсследование.

Линии связи, электропитания и заземления, находится на территории 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. Линейное зашумление на

предприятию не требуется, поскольку отсутствуют выходящие за пределы контролируемой зоны линии. Соната-Р2 по сравнению с другими средствами обладает более широким диапазоном шумового сигнала и более высокой плотностью шума. Поэтому для использования в информационной системе генератор шума Соната-Р2.

Двери всех помещений оборудованы кодовыми замками. Все окна оборудованы жалюзи.

Само предприятие огорожено забором из металла и кирпича высотой 2м. периметр предприятия оборудован камерами видеонаблюдения, с выводом изображения установленном в караульном помещении.

Допуск сотрудников и посетителей осуществляется через пост охраны по пропускам.

13 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Специалисты по защите информации во время выполнения своих профессиональных обязанностей подвержены воздействию опасных и вредных производственных факторов. Каждый работник должен быть проинструктирован о возможном негативном воздействии тех или иных производственных факторов[15].

Опасные и вредные производственные факторы делятся на физические, химические, биологические и психофизиологические. Последние в свою очередь делятся на физические и нервно-психические перегрузки.

К психофизиологическим опасным воздействиям относятся: чрезмерное умственное напряжение, чрезмерные физические нагрузки, монотонность труда.

Трудовая деятельность специалистов в сфере защиты информации заключается в работе с большим объёмом сведений, использовании автоматизированных рабочих мест, СВТ, реализации необходимых решений в короткие сроки, работе с людьми, обладающими различными характерами и т.п. Наличие нагрузки на нервную систему человека и его психику способствует снижению его функциональной активности, развитию болезней нервной системы, расстройствам, утомлению, переутомлению, стрессу. И, наконец, продолжительная работа на автоматизированном рабочем месте (работа за монитором) организует чрезмерную нагрузку на все компоненты зрительного аппарата человека, способствует появлению усталости и переутомлению глазного анализатора. Такая работа, вызывающая напряжение зрительного аппарата, может вызывать заболевания глаз (боль в глазах, резь в глазах, покраснения глаз и век, возникновение пелены, раздвоение предметов, неприятное мерцание, чрезмерная утомляемость при напряжённой зрительной работе и т.д.), способствовать нарушению зрительных органов, и результатом

этого, в свою очередь, будет являться появление головной боли, возникновение напряжения, усиливающего нервно-психическое расстройство и снижающего работоспособность специалиста.

На основе выявленных опасных факторов осуществляется выбор методов и средств обеспечения безопасности, негативно влияющих на органы зрения и присущих тому или иному производственному оборудованию или технологическому процессу.

Для нормального функционирования зрительной системы важно соблюдать правила безопасности при работе с ПЭВМ. Большое количество людей не имеют проблем со зрением, но в то же время их зрительные привычки не соответствуют физиологическим правилам и нормам. Таким образом рано или поздно это приводит к ухудшению работы зрительного аппарата. Для сидения рисков возникновения возможных проблем, необходима постоянная профилактика зрения, включающая в себя комплекс мероприятий, направленных на поддержание и улучшение здоровья глаз.

Перенапряжение глазодвигательных мышц является причиной большинства болезней органов зрения. Данное состояние приводит к ослаблению местного кровообращения и ухудшению трофики тканей (клеточного питания). Для защиты глаз от излишнего напряжения не рекомендуется длительное время фокусировка зрения на одном и том же предмете. В целях профилактики необходимо выработать полезную привычку: периодически отрывать глаза от работы и переводить взгляд на отдаленный предмет. Это действие способствует поддержанию упругости глазных мышц и получению постоянно четкого изображения предметов на сетчатке.

Существует большое количество методов для достижения расслабления глазного аппарата, в последнее время успешно зарекомендовал себя метод пальминга. Это упражнение, заключающееся в накладывании на закрытые глаза ладоней обеих рук (без давления). В таком положении следует находиться 4-5 минут. Данную процедуру, направленную на естественное восстановление зрения, рекомендуется выполнять ежедневно.

Не менее эффективная профилактика для глаз - распределения слезной жидкости, обладающей увлажняющими и дезинфицирующими свойствами, по поверхности глазного яблока необходимо часто моргать. Моргание дает кратковременный отдых, укрепляет нервные волокна сетчатки, обеспечивает расслабление глазных мышц, улучшает центровку и способность глаза фокусировать изображение.

Для предотвращения ухудшения зрения необходимо регулярно укреплять сетчатку при помощи солнечного света. Глаза, созданные для восприятия световых лучей, нуждаются в естественном освещении не меньше, чем в периодическом отдыхе и расслаблении. Каждый день следует начинать с принятия световых ванн (соляризации). Закрытые глаза на несколько минут подставляют солнцу или, при его отсутствии, другому источнику яркого света. Данная процедура способствует усилению кровообращения, нормализации обменных процессов в тканях глазного яблока и сохранению зрения.

Так же немаловажный фактор, повышающий остроту и предотвращающий ухудшение зрения, подходящие условия для работы глаз. Главное их них – правильная освещенность. Искусственный свет должен быть достаточно ярким, но не резать глаза. Специалисты рекомендуют использовать с целью сохранения зрения при работе за письменным столом настольные лампы мощностью 60 Вт с плафонами. Источник света должен располагаться слева (у правшей), в 50 см от документов.

Заключение

В ходе выполнения выпускной квалификационной работы были проанализированы нормативно-правовые акты в области защиты информации ограниченного доступа, не составляющей государственную тайну, изучены технические каналы утечки информации и источники угроз безопасности информации, разработана модель угроз организации.

В рамках разработки подсистемы обеспечивающей информационную безопасность средствами криптографической защиты в АО «ПО «Электроприбор» в соответствии с действующим законодательством Российской Федерации по защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке, хранении и передаче по каналам связи, проведена классификация информационной системы по требованиям защиты информации, определены актуальные угрозы безопасности информации, обрабатываемой в информационной системе, определен потенциал возможного нарушителя и определены защитные меры, которые необходимо использовать. Все действия выполнялись в соответствии с требованиями и методиками ФСТЭК.

Для информационной системы были определены средства, которыми должны быть реализованы защитные меры. Были определены организационно-технические меры защиты информации, выбраны программные и технические средства, которые должны использоваться при эксплуатации информационной системы.

Результаты выпускной квалификационной работы, использованы в создании информационной системы по обработке информации конфиденциального характера. Акт о внедрении результатов ВКР приведен в приложении Б.

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 Федеральный закон "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" ОТ 20.08.2004 № 119-ФЗ // " Консультант Плюс" - Законодательство РФ. с изм. и допол. в ред. ОТ 29.12.2004.

4 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). "Стандарт", 1993.

5 Лунегов А.Н., Рыжов А.Л. Технические средства и способы добывания и защиты информации. М.: ВНИИ "Стандарт", 1993.

6 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.

7 Методический документ "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 14.02.2008 ФСТЭК России.

8 Методический документ "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15.02.2008 ФСТЭК России.

9 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).

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

11 СЗИ Dallas Lock 8.0-К // 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).

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

12 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).

13 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).

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

ПРИЛОЖЕНИЕ А

(обязательное)

Модель угроз безопасности информации

А.1 Общие положения

Информационная система (ИС), для которой была сформирована модель угроз и модель нарушителя (далее – модель угроз), находится на территории предприятия АО «ПО «Электроприбор».

При разработке модели угроз были использованы следующие источники информации:

- федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- «Банк данных угроз безопасности информации» ФСТЭК России;
- положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;
- «Методика определения угроз безопасности информации в информационных системах», методический документ ФСТЭК.

А.2 Описание информационной системы и особенностей ее функционирования

В АО «ПО «Электроприбор» телекоммуникационная сеть состоит из 7 серверов и 797 автоматизированных рабочих мест (АРМ). Все оборудование находится в пределах контролируемой зоны.

На сервере 1 установлен первичный контроллер домена, который используется для создания, настройки и управления учетными записями пользователей и компьютеров телекоммуникационной сети. Для избежание выхода из строя первичного контроллера домена, был создан резервный контроллер. Он носит имя вторичного контроллера домена и установлен на

сервере 2. Периодически происходит синхронизация данных учетных записей и прав доступа, поэтому в случае выхода из строя первичного контроллера. Программное обеспечение обоих серверов представлено Microsoft Windows Server 2008.

Сервер 3 выполняет функции почтового и прокси-сервера. Для работы сервера используется ОС Microsoft Windows Server 2008 и Microsoft Windows Server 2010. Также для работы почтового сервера установлено ПО Courier Mail Server 1.56. Выполнение функций прокси-сервера осуществляется при помощи универсального шлюза безопасности Traffic Inspector. Traffic Inspector осуществляет фильтрацию спама, баннеров, графики и другого нежелательного медиа-контента, запрещает доступ к нежелательным веб-сайтам, фильтрует нежелательную почту перед тем как она попадет на почтовый сервер организации.

На сервере 4 установлено программное обеспечение «1С:Предприятие 8.2», предназначенное для автоматизации бухгалтерского и управленческого учётов. Так же на сервере находятся «Комплекс решений Аскон 2011». Данное ПО используется для управления инженерными и проектными данными, циркулирующими в единой информационной системе предприятия.

На сервере 5 находится программное обеспечение «1С:Предприятие 8.2» для резервирования сервера 4. Для работы сервера 4 и 5 используется ОС Microsoft Windows Server 2008.

Сервер 6 представляет собой систему управления базы данных (СУБД) Microsoft SQL Server 2008. СУБД представляет собой реляционную архитектуру, т.е. данные выражены в виде таблиц. Сервер не имеет доступа к внешним сетям. Сервер 6 резервирован на сервере 7.

Сервер 8 осуществляет работу с ЭЦП, антивирусную защиты, контроль входящего трафика, централизованное управление системой защиты, мониторинг и аудит безопасности, на сервере установлено следующее ПО:

- Kaspersky Endpoint Security 8;
- Secret Net 7.0;

– Удостоверяющий Центр ViPNet.

На предприятии имеется 797 АРМ. АРМ сотрудников состоят из ПК, представленных в виде стационарных компьютеров, на которых обрабатываются данные бухгалтерского и финансового учета, данные персонала и конструкторско-технологическая информация, необходимые для осуществления деятельности предприятия.

На ПК сотрудников установлены операционные системы Windows XP и Windows 7 с установленным ПО для работы с базами данных «1С:Предприятие 8.2», системой автоматизированного проектирования радиоэлектронных средств Altium Designer, графическим редактором CorelDRAW Graphics Suite X5, текстовыми процессорами LibreOffice и Microsoft Office 2007 и почтовым клиентом Microsoft Office Outlook 2010. Для защиты обрабатываемых данных установлено СЗИ Secret Net 7.0, межсетевой экран и антивирус «Kaspersky Anti-Virus».

Для разграничения прав доступа к информации передаваемой внутри подсистемы был установлен АПКШ «Континент» 3.6. Комплекс так же служит для криптографической защиты информации передаваемой между сегментами сети и отдельными компьютерами.

Для объединения АРМ и серверов в локальную сеть используются 4 коммутатора Cisco WS-C3550-12T и маршрутизатор Cisco RVS4000.

На предприятии используются волоконно-оптические линии и кабели UTP категории 5. Все кабели находятся в пределах контролируемой зоны. Единственным передающим каналом во вне является подключение провайдера ПАО «Ростелеком» к сетевому оборудованию внутренней сети Интернет. Скорость канала 100 Мб/с.

АО «ПО «Электроприбор» имеет официальный сайт, находящимся на оборудовании сторонней организации по договору хостинга.

А.3 Возможности нарушителей

Характеристики нарушителей представлены в таблице А.1.

Таблица А.1 - Характеристики нарушителей

Угроза	Возможность реализации угрозы	Последствия реализации угрозы	Нарушитель	Степень возможного ущерба	Актуальность угрозы
УБИ.008 Угроза восстановления аутентификационной информации	Низкая	Нарушение конфиденциальности	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Низкая	Актуальная
УБИ.031 Угроза использования механизмов авторизации для повышения привилегий	Средняя	Нарушение конфиденциальности	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Средняя	Актуальная
УБИ.038 Угроза исчерпания вычислительных ресурсов хранилища больших данных	Низкая	Нарушение доступности	Внутренний нарушитель с низким потенциалом	Низкая	Актуальная
УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией	Средняя	Нарушение конфиденциальности	Внутренний нарушитель с низким потенциалом	Средняя	Актуальная
УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	Низкая	Нарушение конфиденциальности	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Средняя	Актуальная
УБИ.091 Угроза несанкционированного удаления	Средняя	Нарушение доступности	Внутренний нарушитель с низким	Средняя	Актуальная

Продолжение таблицы А.1

Угроза	Возможность реализации угрозы	Последствия реализации угрозы	Нарушитель	Степень возможного ущерба	Актуальность угрозы
защищаемой информации			потенциалом Внешний нарушитель с низким потенциалом		
УБИ.162: Угроза эксплуатации цифровой подписи программного кода	Средняя	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Средняя	Актуальная
УБИ.187: Угроза несанкционированного воздействия на средство защиты информации	Средняя	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Средняя	Актуальная

ПРИЛОЖЕНИЕ Б
(обязательное)
Акт о внедрении

ПРИЛОЖЕНИЕ В

(обязательное)

Протокол проверки ВКР в системе Антиплагиат