МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ

ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка комплекса нормативных актов и регламентов для удостоверяющего центра»

Исполнитель Бледных Сергей Юрьевич
(фамилия, имя, отчество)

Руководитель Старший преподаватель
(ученая степень, ученое звание)

Богданов Павел Юрьевич
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____
(подпись)

доктор технических наук, профессор
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«17» февраля 2017 г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ

ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему«Разработка комплекса нормативных актов и регламентов для удостоверяющего центра»

ИсполнительБледных Сергей Юрьевич
(фамилия,имя,отчество)

РуководительСтарший преподаватель
(ученая степень, ученое звание)

Богданов Павел Юрьевич
(фамилия, имя, отчество)

«Кзащитедопускаю»

Заведующийкафедрой_____
(подпись)

доктор технических наук, профессор
(ученаястепень,ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия,имя,отчество)

«_»_20г.

Санкт–Петербург

2017

Оглавление

Введение

В век информационных технологий и глобальной компьютеризации особую важность представляют электронный документооборот и обеспечение конфиденциальности данных. Документы в электронно–цифровой форме имеют ряд неоспоримых преимуществ перед своими бумажными аналогами. Среди основных можно выделить удобство использования, экономию времени, значительное снижение затрат на хранение и снижение загрязнения экологии. В итоге, работа с электронными документами намного эффективнее и оперативнее. В большинстве значимых электронных документов зачастую применяется электронно–цифровая подпись. Электронная подпись– своеобразный аналог собственноручной подписи, защищающей электронный документ от искажения и доступа посторонних лиц. Тем не менее, защита электронных документов не ограничивается только лишь электронной подписью. Для того, чтобы сформированная электронная подпись имела юридический вес, она должна быть заверена сертификатом электронной подписи, выдаваемым удостоверяющим центром. Компания ООО “DISTATE” была образована в 2009 году. Это команда высококвалифицированных специалистов, основной целью которых является создание удобной универсальной системы электронного документооборота. На данном этапе развития, компании “DISTATE” потребовалось расширить бизнес – открыть собственный центр сертификации. Для того, чтобы удостоверяющий центр функционировал необходимо провести ряд организационных и технических мер, нацеленных на получение аккредитации в Министерстве связи и массовых коммуникаций. Именно поэтому целью в данной Выпускной Квалификационной Работе является необходимость разработать и подготовить комплект нормативной документации удостоверяющего центра. Для реализации этой цели были поставлены следующие задачи:

— Анализ руководящих документов

— Исследование специфики организации рабочего процесса, схем помещений и вида деятельности предприятия.

— Разработка комплекта нормативной документации с учетом специфики предприятия

Актуальность данной работы обуславливается тем, что разработанный комплект документации определяет условия деятельности Удостоверяющего центра, а также основные организационно–технические мероприятия, направленные на обеспечение безопасности обрабатываемой и хранящейся информации.

1Анализ руководящих документов. Основные требования и мероприятия для обеспечения Информационной Безопасности

1.1 Руководящие документы

Данная выпускная квалификационная работа опирается на следующие руководящие документы:

— Федеральный закон от 6 апреля 2011 г. N 63–ФЗ “Об электронной подписи”

— Положение “О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)”

— Инструкция “Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну”

— Федеральный закон от 27 июля 2006 г. N 149–ФЗ "Об информации, информационных технологиях и о защите информации"

Данные положения выбраны основными руководящими документами для этой дипломной работы из–за специфики предоставления услуг и рабочего процесса любого Удостоверяющего центра, которая заключается в создании и выдаче сертификатов электронной подписи, а также осуществления проверки отсутствия искажения информации в электронном документе (целостность), принадлежности подписи владельцу сертификата ключа подписи (авторство) и подтверждения факта подписания электронного документа (неотказуемость). Т.е. обработке и хранении персональных данных и конфиденциальной информации с использованием криптографических средств.Рассмотрим вышеперечисленные положения и проведём их детальный анализ.

Начнем с Федерального закона “Об электронной подписи” от 06.04.2011. Указанный закон является основополагающим и главенствующим перечнем требований и предписаний для такого типа организации не только на этапе подготовки к получению лицензий и прохождения аккредитации, но и в

процессе осуществления самой деятельности по предоставлению услуг удостоверяющим центром, поскольку регулирует отношения в области использования электронных подписей при совершении гражданско–правовых сделок и пр. Принципами использования электронной подписи, описанными в ФЗ, являются :

— право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, в случае если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами, либо соглашением между участниками электронного взаимодействия;

— возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования Федерального закона применительно к использованию конкретных видов электронных подписей;

— недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Также, закон об ЭП предоставляет классификацию видов электронных подписей, в соответствии с их признаками. Электронную подпись разделяют на простую электронную подпись и усиленную электронную подпись.

1) Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

2) Усиленная электронная подпись. Средиусиленных ЭП различают два вида – неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Неквалифицированной электронной подписью является электронная подпись, которая:

— получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

— позволяет определить лицо, подписавшее электронный документ;

— позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

— создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной ЭП и следующим дополнительным признакам:

— ключ проверки электронной подписи указан в квалифицированном сертификате;

— для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом.

Важной составляющей ФЗ №63 является статья регламентирования средств электронной подписи, обусловливающая порядок использования средств и требования для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.

Согласно данной статье, средства электронной подписи позволяют установить факт изменения подписанного электронного документа после момента его подписания и обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки. При создании электронной подписи средства электронной подписи должны:

— показывать лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

— создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

— однозначно показывать, что электронная подпись создана.

При проверке электронной подписи средства электронной подписи должны:

— показывать содержание электронного документа, подписанного электронной подписью;

— показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

— указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Не менее важной считается статья 13 ФЗ №66 “Об электронной подписи”, т.к. в ней описаны общие требования и предписания действий к удостоверяющему центру. Деятельность удостоверяющего центра включает в себя несколько основных пунктов[1]:

— создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов лицам, обратившимся за их получением, только в случае установления личности получателя сертификата, либо полномочий лица, выступающего от имени заявителя;

— установление сроков действия сертификатов ключей проверки электронных подписей;

— упразднение выданных этим удостоверяющим центром сертификатов ключей проверки электронных подписей;

— выдача по обращению заявителя средств электронной подписи, которые содержат ключи электронной подписи проверки электронной подписи (в т.ч. созданные удостоверяющим центром) или позволяют создать ключ ЭП или проверки ЭП заявителем;

— ведение реестра сертификатов – перечня выданных и аннулированных сертификатов ключей проверки электронных подписей;

— обеспечение доступа к информации, содержащейся в реестре сертификатов, в т.ч. посредством сети "Интернет";

— создание по обращениям заявителей ключей электронных подписей и ключей проверки электронных подписей;

— проверка на уникальность ключей проверки электронных подписей в реестре сертификатов;

— осуществление по обращениям участников электронного взаимодействия проверки электронных подписей;

— осуществляет иную связанную с использованием электронной подписи деятельность.

Далее рассмотрим положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005) .

Положение (ПКЗ–2005), о котором говорится в приказе №66 ФСБ России, осуществляет регулирование отношений, возникающих при разработке, производстве, реализации и эксплуатации криптографических (шифровальных) средств обеспечения безопасности информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (т.е. конфиденциальной информации).

Внесем ясность относительно средств шифрования.Таковыми могут являться аппаратные или программные, а также аппаратно–программные средства/системы/комплексы осуществляющие криптографическое преобразование информации для обеспечения защиты информации от несанкционированного доступа при обработке и хранении в ИС и передаче по каналам связи. Отсюда вытекает определение средств электронной подписи, которые эксплуатируются в процессе деятельности удостоверяющих центров – Средства электронной подписи относятся к одному из видов средств шифрования и обеспечивают создание ЭП с помощью ключа ЭП, подтверждение подлинности подписи использованием открытого ключа, создание закрытых и открытых ключей электронной подписи.

Для организации работы удостоверяющего центра необходимо руководствоваться Положением ПКЗ–2005. В случае УЦ, взятого за основу в данной ВКР, взаимодействие с СКЗИ будет заключаться только в их эксплуатации.

— СКЗИ эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

— СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России.

— СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

— контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, а также условий производства ключевых документов, осуществляется в соответствии с требованиями Федерального закона от 26 декабря 2008 г. № 294–ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

— контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется: обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ; собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ ФСБ России в рамках контроля за организацией и функционированием криптографической инженерно–

технической систем шифрованной, засекреченной и иных видов специальной связи.

— контроль за соблюдением условий производства ключевых документов, указанных в технической, конструкторско–технологической и эксплуатационной документации к внешней системе изготовления ключей, осуществляется изготовителем ключевых документов, а также ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно–технической безопасности информационно–телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

— с целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, обладатель, пользователь (потребитель) данной информации, установивший режим ее защиты с применением СКЗИ, а также собственник (владелец) информационных применяются СКЗИ, вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

Третьим значимым руководящим документом выступает Инструкцияоб организации и обеспечении безопасности хранения, обработки и передачи конфиденциальной информации.

Инструкция определяет единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Согласно пункту 20 части 2 Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, пользователи средств криптографической защиты информации обязаны[3]:

— не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

— соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

— сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

— сдать СКЗИ, эксплуатационную и техническую документацию к ним,

ключевые документы в соответствии с порядком, установленным данной Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

— немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Последним руководящим документов выступает Федеральный закон от 27 июля 2006 г. N 149–ФЗ "Об информации, информационных технологиях и о защите информации", который регулирует отношения, возникающие при [4]:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Предписывающей для данной выпускной квалификационной работы является статья, посвященная защите информации. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

— обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления,

распространения, а также от иных неправомерных действий в отношении такой информации;

— соблюдение конфиденциальности информации ограниченного доступа;

— реализацию права на доступ к информации.

— обладатель информации или оператор обработки информации, каким является удостоверяющий центр обязан обеспечить выполнение следующих установленных требований:

— предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

— своевременное обнаружение фактов несанкционированного доступа к информации;

— предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

— недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

— возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

— постоянный контроль за обеспечением уровня защищенности информации;

— нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

1.2 Требования и мероприятия

Первоначально, необходимо обеспечить получение аттестата соответствия требованиям по обеспечению безопасности конфиденциальной

информации. Для этого необходимо аттестовать защищаемое помещение и автоматизированную систему удостоверяющего центра.

1.2.1 Аттестационные испытания по требованиям безопасности информации защищаемого помещения включают в себя[5]:

— Экспертный анализ готовности ЗП к Аттестации по требования безопасности информации

— Разработка проекта организационно–распорядительных документов на объект.

— Разработка и согласование Программы и методик проведения аттестационных испытаний по требованиям безопасности информации

— Проведение инструментальных измерений, специальных исследований и оценки защищенности объекта от возможных каналов утечки речевой информации.

— Выдача рекомендаций по устранению выявленных недостатков и применению необходимых технических средств защиты (при необходимости)

— Монтаж, настройка технических средств защиты информации

— Подготовка и оформление пакета аттестационной отчетной документации

— Выдача Аттестата соответствия объекта требованиям по безопасности информации

Необходимый и достаточный пакет исходных данных документов для аттестации ЗП:

— Приказ о назначении специалиста по защите информации (п. 2.15 СТР–К).

— Положение о порядке организации и проведения работ по защите конфиденциальной информации (п. 3.5 СТР–К).

— Перечень сведений конфиденциального характера (п. 3.6 СТР–К).

— Перечень угроз безопасности информации (в соответствии с ГОСТ Р 51275–2006) и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта (п. 3.8 СТР–К).

— Приказы (п. 3.21 СТР–К):

– о назначении лиц, ответственных за эксплуатацию объекта информатизации;

– на обсуждении в ЗП конфиденциальной информации.

— Перечень ЗП и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации (п. 4.2.1 СТР–К).

— Технический паспорт на ЗП (п. 4.2.1 СТР–К).

— Схема размещения ВП внутри здания и относительно КЗ (п. 3.8 СТР–К).

— Схема охранной сигнализации (должно быть в составе ТП)

— Схема пожарной сигнализации (должно быть в составе ТП)

— Перечень мебели и предметов интерьера в ВП (должно быть в составе ТП)

— Схема размещения мебели, технических средств в ВП (должно быть в составе ТП)

— Схема электроснабжения кабинета и осветительной сети (должно быть в составе ТП)

— Перечни сведений конфиденциального характера, подлежащих защите (п. 5.2.2 СТР–К)

— Инструкции: (п. 3.18 СТР–К)

– ответственному за ЗП ;

– по эксплуатации СЗИ.

1.2.2 Аттестация автоматизированных систем

Аттестация автоматизированных систем (объектов информатизации) с последующей выдачей аттестата является необходимым условием, дающим возможность получить соответствующие лицензию в ФСБ , на основании которой компания сможет беспрепятственно заниматься разработкой, производством, распространением средств защиты информации, выдачей электронных подписей и др.

Аттестация автоматизированных систем – сложная процедура, включающая в себя комплекс мероприятий, таких как[6]:

— Экспертный анализ готовности АС к Аттестации по требованиям безопасности информации

— Разработка проекта организационно–распорядительных документов на объект

— Разработка и согласование Программы и методик проведения аттестационных испытаний по требованиям безопасности информации

— Проведение инструментальных измерений, специальных исследований и оценки защищенности объекта от утечки информации по каналам ПЭМИН

— Анализ организационной структуры объекта, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, и выдача рекомендаций по применению систем и средств защиты информации на объекте

— Установка и настройка СЗИ от НСД в соответствии с требованиями РД по защите информации от НСД, с последующими испытаниями Проверка эффективности применяемых на объектах средств и систем защиты информации

— Подготовка и оформление пакета аттестационной отчетной документации

— Выдача Аттестата соответствия объекта требованиям по безопасности информации

Необходимый и достаточный пакет исходных данных документов для аттестации АС:

— Приказ о назначении специалиста по защите информации (п. 2.15 СТР–К).

— Положение о порядке организации и проведения работ по защите конфиденциальной информации (п. 3.5 СТР–К).

— Перечень сведений конфиденциального характера (п. 3.6 СТР–К). Перечень угроз безопасности информации (в соответствии с ГОСТ Р 51275–99) и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта (п. 3.8 СТР–К).

— Приказы (п. 3.21 СТР–К): – на проведение работ по защите конфиденциальной информации;

– о назначении лиц, ответственных за эксплуатацию объекта информатизации;

– на обработку вАС конфиденциальной информации.

— Перечень АС и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации (п. 4.2.1 СТР–К).

— Технический паспорт на АС (п. 4.2.1 СТР–К).

— Состав технических и программных средств АС (должно быть в составе ТП)

— Схема размещения ОТСС, ВТСС и средств защиты информации (должно быть в составе ТП)

— Схема размещения объекта относительно границ контролируемой зоны(должно быть в составе ТП) (п. 3.8 СТР–К)

— Описание технологического процесса обработки закрытой информации на АС

— Схема информационных потоков (при необходимости в больших распределенных ЛВС)

— Акт классификации АС (п. 5.1.4 СТР–К).Перечни сведений конфиденциального характера, подлежащих защите (п. 5.2.2 СТР–К).

— Технический паспорт на АС (п. 3.18 СТР–К)

— Описания технологического процесса обработки информации (п. 3.18 СТР–К)

— Разрешительная система допуска пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации (п. 5.3.1 СТР–К)

— Инструкции: (п. 3.18 СТР–К)

– администратору защиты информации;

– пользователям АС;

– по организации антивирусной защите в АС;

– по эксплуатации СЗИ.

1.2.4 Вторым этапом является получение лицензии ФСБ

Основные требования и мероприятия для получения лицензии ФСБ Для получения данной лицензии заявитель направляет в ЦЛСЗ ФСБ России (или свой территориальный орган, если организация не из Москвы или Московской области)[7]:

1) Заявление о предоставлении лицензии с указанием:Полного, фирменного и сокращенного наименования юридического лица;

- Организационно–правовой формы;

- Должности и Ф.И.О. руководителя юридического лица;

- Номеров и наименования работ в соответствии с перечнем работ и услуг;

- Местонахождение заявителя;

- Адреса мест осуществления лицензируемой деятельности;

- Телефона/факса с указанием кода города;

- ИНН и данных документа о постановке соискателя лицензии (лицензиата) на учет в налоговом органе;

- ОГРН и данных документа, подтверждающего факт внесения сведений о юридическом лице в Единый государственный реестр юридических лиц.

2) Копии учредительных документов юридического лица, засвидетельствованные в нотариальном порядке;

3) Копии правоустанавливающих документов на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

4) Копии внутренних распорядительных документов, подтверждающих наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, определенных Положением, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации";

5) Копии документов, подтверждающих нахождение в штате соискателя лицензии на основной работе сотрудников;

6) Копии документов государственного образца (дипломы, аттестаты, свидетельства) об образовании, переподготовке, повышении квалификации по направлению "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей сотрудников;

7) Копии трудовых книжек сотрудников;

8) Копии должностных инструкций сотрудников;

9) Копии документов, подтверждающих наличие у соискателя лицензии приборов и оборудования, прошедших поверку и калибровку в соответствии с Федеральным законом "Об обеспечении единства измерений", принадлежащих ему на праве собственности или ином законном основании и необходимых для выполнения работ и оказания услуг, указанных в пунктах 1 – 11, 16 – 19 перечня работ и услуг;

10) Оригинал документов, подтверждающих оплату лицензионного сбора;

11) Опись прилагаемых документов.

Конечными являются требования Минкомсвязи к удостоверяющим центрам, претендующим на получение статуса аккредитованного удостоверяющего центра, которая осуществляется при условии выполнения им следующих требований [8]:

— стоимость чистых активов УЦ составляет не менее чем один миллион рублей;

— наличие финансового обеспечения ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в

сертификате ключа проверки электронной подписи, выданном таким УЦ, или информации, содержащейся в реестре сертификатов, который ведет такой УЦ, в сумме не менее чем полтора миллиона рублей;

— наличие средств электронной подписи и средств УЦ, получивших подтверждение соответствия требованиям федеральных законов в области обеспечения безопасности;

— наличие в штате УЦ не менее двух работников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей, которые имеют высшее профессиональное образование в области ИТ или ИБ либо высшее или среднее профессиональное образование с последующим прохождением переподготовки или повышения квалификации по вопросам использования электронной подписи.

Изучив требования и проведя анализ руководящих документов, необходимо исследовать специфику предприятия для разработки перечня рекомендаций по обеспечению защиты от утечки конфиденциальной информации и устранения всех несоответствий требованиям, предъявляемым к удостоверяющему центру.

2 Исследование и анализ схем помещений и специфики рабочего процесса

В данной главе представлено описание выбранного Удостоверяющего центра – схема помещения, схема размещения мебели, технических средств в ЗП, схема электроснабжения и осветительной сети, технический паспорт на защищаемое помещение, схема размещения ОТСС, ВТСС и средств защиты информации и технический паспорт на АС. А также обозначен перечень потенциальных угроз информационной безопасности и перечень конфиденциальной информации, во взаимодействии (хранение, обработка и пр.) с которой будет заключаться деятельность удостоверяющего центра. Введем понятия ОТСС и ВТСС, а также перечень ТС, которые к ним относятся.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной (секретной) информации.

К ОТСС могут относиться средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно–вычислительные комплексы, сети и системы, средства и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической видео–, смысловой и буквенно–цифровой информации) используемые для обработки конфиденциальной (секретной) информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в выделенных помещениях [9].

К ним относятся:

— различного рода телефонные средства и системы;

— средства и системы передачи данных в системе радиосвязи;

— средства и системы охранной и пожарной сигнализации;

— средства и системы оповещения и сигнализации;

— контрольно–измерительная аппаратура;

— средства и системы кондиционирования;

— средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);

— средства электронной оргтехники.

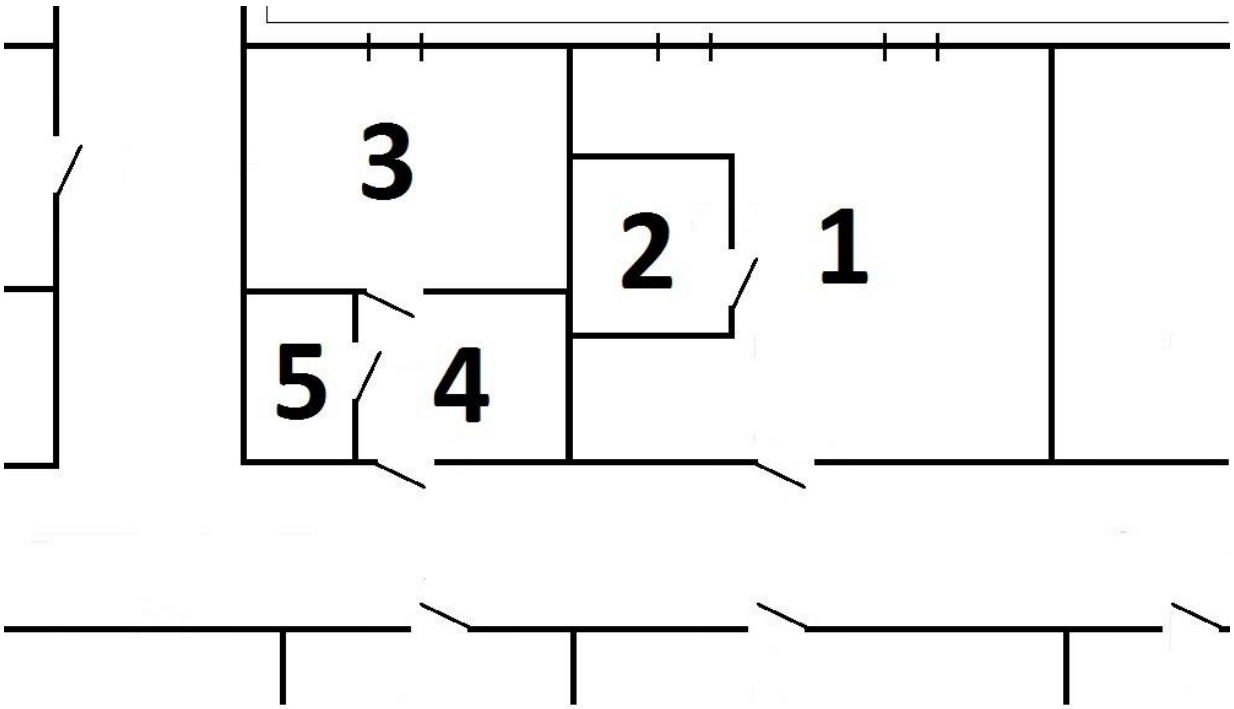
2.1 Схемы помещений

Первостепенно, необходимо провести анализ схемы защищаемого помещения. Поскольку, в необходимый пакет документов для аттестации требуется включить схемы ОТСС, ВТСС, пожарной и охранной сигнализации и т.д., то целесообразнее разделить схему помещения на две идентичные по строению схемы с различными элементами. Это позволит улучшить читаемость схемы.

На основе анализа представленных ниже схем разработан индивидуальный перечень угроз информационной безопасности для выбранного удостоверяющего центра.

Для начала следует ознакомиться с исходным планом помещений, представленным на рисунке 1. Под удостоверяющий центр арендуется два помещения, в свою очередь, разделенных на доп. помещения. В данном случае на помещение персонала обеспечения безопасности и технической поддержки,

внутри которого отдельным помещением расположена серверная, и на помещение административного персонала, помещение персонала по обеспечению регистрации и приемную, которые разделены ненесущими стенами.

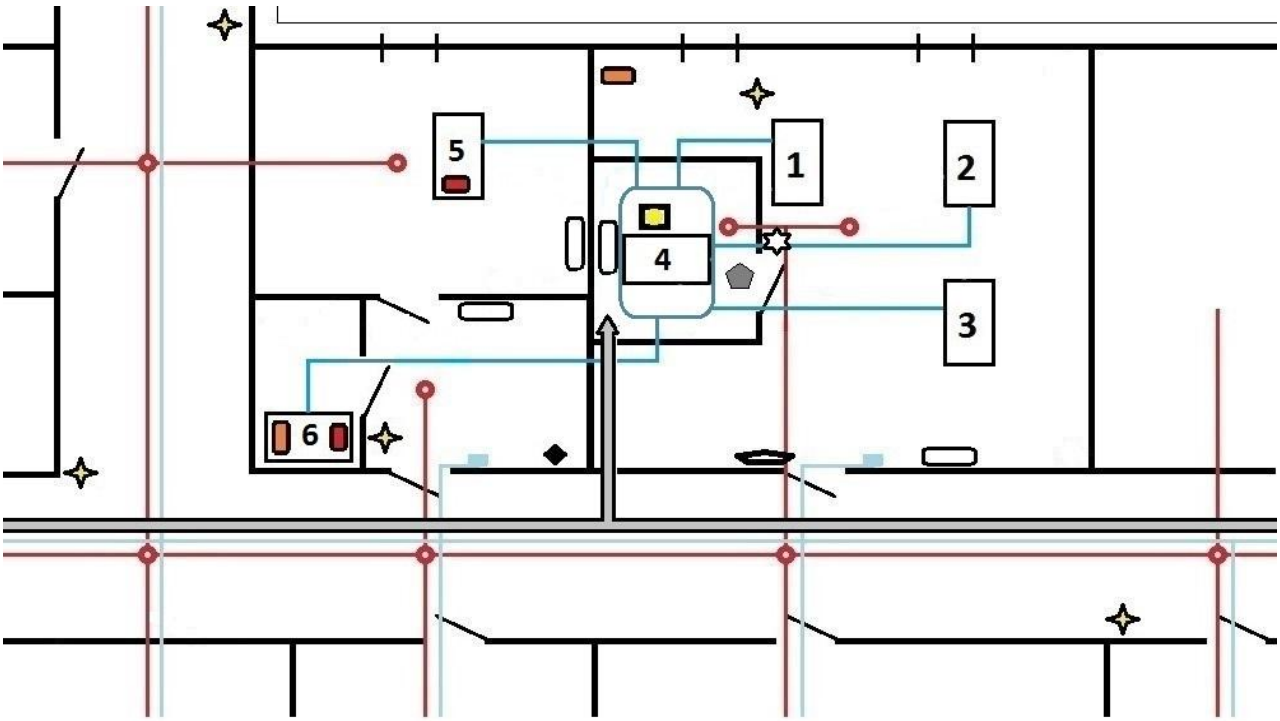


1 - Помещение персонала по обеспечению безопасности
2 - Серверная
3 - Помещение административного персонала
4 - Приемная комната
5 - Помещение персонала по обеспечению регистрации

Рисунок 1 – Исходный план помещений

Защищаемым помещением в данном УЦ является только помещение персонала обеспечения безопасности и тех. поддержки, т.к. основные технические средства и системы находятся именно в нем, а область их действия не выходит за границы ЗП. Граница контролируемой зоны условно определена внешними несущими стенами арендуемых помещений бизнес центра.

Рассмотрим расположение элементов пожарной безопасности, охранной сигнализации, ОТСС и ВТСС в защищаемом помещении (Рисунок 2).



	Камера наблюдения		Кофемашина
	Телефон		Кондиционер
	Принтер		Граница КЗ
№	ЭВМ		Средства защиты информации
	Пожарная сигнализация		Маршрутизатор
	Охранная сигнализация		Локальная сеть
	Система дымоудаления		Система контроля доступа
	Система порошкового пожаротушения		Вентиляционная шахта

Рисунок 2 – Расположение элементов пожарной безопасности, охранной сигнализации, ОТСС и ВТСС на территории УЦ и в коридоре

Разделим обозначения на ОТСС и ВТСС. Основными техническими средствами, находящимися в отделе в отделе службы безопасности, являются:

— ЭВМ в количестве 3 штук, образующих АС класса 1Г (многопользовательская с разными правами)

— Сервер

— Принтер

— Маршрутизатор

— ЭВМ в помещениях административного персонала и персонала по обеспечению регистрации

Вспомогательными техническими средствами в данном случае следует считать:

— Телефоны, расположенные в помещениях административного персонала и персонала по обеспечению регистрации
— Принтер в помещении персонала по обеспечению регистрации
— Датчики пожарной сигнализации
— Датчики охранной сигнализации
— Система порошкового пожаротушения
— Система контроля доступа в серверную
— Кондиционеры
— Средство защиты информации Соната РК–1
— Широкоугольные камеры видеонаблюдения

Рисунок 2 наглядно отображает специфику построения сети пожарной и охранной сигнализации. Пожарная безопасность обеспечивается датчиками дыма, расположенными в количестве по 2 штуки на каждое помещение и подключенными к единой сети пожарной сигнализации бизнес центра. Также датчики дыма расположены в коридоре здания, таким образом охватывая всю его площадь. В серверной установлены система дымоудаления и система порошкового пожаротушения, в случае возгорания, минимизирующая угрозу техническому оборудованию сервера и данным, которые на нем хранятся. Чтобы избежать перегревания аппаратных средств сервера, в серверной установлен кондиционер.

Охранная сигнализация и механические замки на дверях офисов, в совокупности с контрольно–пропускным пунктом на входе в БЦ, обеспечивают невозможность несанкционированного проникновения посторонних лиц на территории контролируемой зоны, в частности несанкционированного проникновения в помещения удостоверяющего центра и доступа к автоматизированной системе и ПЭВМ.

Для контроля действий посторонних лиц, которым предоставлен доступ на территорию БЦ, установлены широкоугольные камеры видеонаблюдения. Специфика их расположения позволяет охватывать все пространство коридорных проемов. В том числе, локальные камеры видеонаблюдения были установлены непосредственно на территории удостоверяющего центра с целью отслеживания возможных несанкционированных действий сотрудников обеспечения безопасности и технической поддержки, а также клиентов УЦ. Локальные камеры наблюдения не относятся к общей системе наблюдения бизнес центра, запись с них записывается и хранится на сервере УЦ.

В УЦ имеется локальная вычислительная сеть топологии “звезда”, объединяющая ЭВМ помещения персонала обеспечения безопасности, сервер и ЭВМ помещений административного персонала и персонала по обеспечению регистрации в единую систему. Разграничение доступа к серверу и КИ, хранящейся на нем, осуществляется при помощи СЗИ SecretNet, что обеспечивает защиту от НСД через ЛВС.

Не менее важным является анализ цепи электроснабжения, осветительной сети и мебели (Рисунок 3).

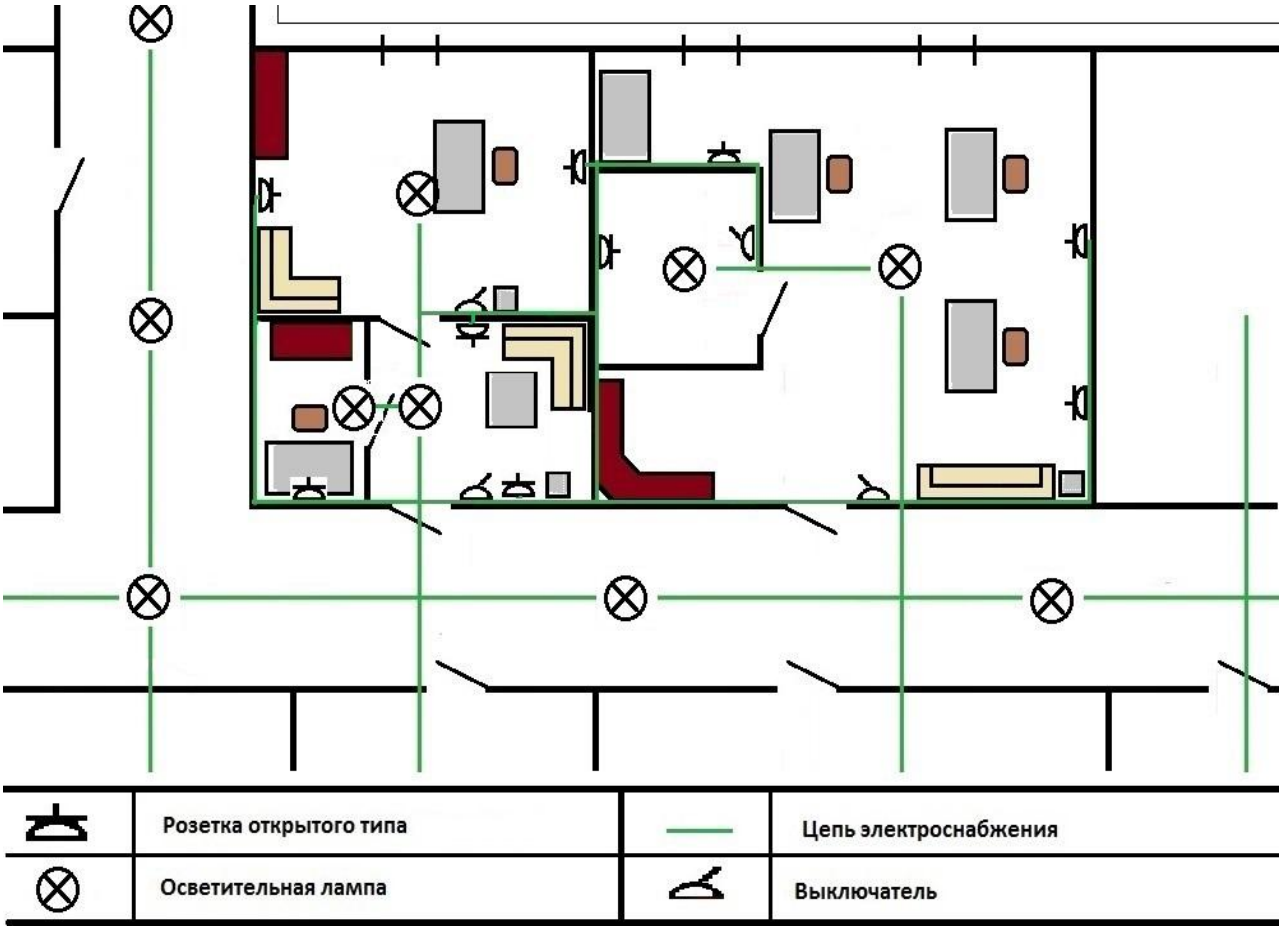


Рисунок 3 – Построение цепи электроснабжения, осветительной сети и расположение предметов интерьера.

Электрические сети и электрооборудование, а также осветительная сеть к общегородской сети электроснабжения. Это соответствует требованию к организации рабочего помещения удостоверяющего центра и обеспечивает бесперебойное снабжение здания электричеством. Однако, есть нюанс относительно использования общегородской сети электроснабжения. Поскольку, данная сеть электропитания выходит за границы контролируемой зоны, возникает опасность утечки конфиденциальной информации по цепям заземления и электропитания из–за побочных электромагнитных излучений от ОТСС. Для предотвращения подобного рода утечки, как было указано выше, используется средство защиты информации Соната РК–1 и маскираторы электромагнитных излучений и наводок (генераторы электромагнитного шума) Маис–М.

Для осветительной сети помещений удостоверяющего центра и коридора БЦ используются люминесцентные лампы и настенные выключатели. Для

обеспечения питания электричеством электрооборудования установлены розетки открытого типа с заземлением.

Предметы интерьера установлены в помещениях удобным образом для рабочего процесса сотрудников. В приемной и помещении административного персонала установлены угловые диваны для клиентов УЦ. Помимо удобства также предусмотрены противопожарные требования к расположению предметов мебели на случай эвакуации – оптимальная расстановка, не препятствующая передвижению в экстренных случаях.

2.2 Специфика рабочего процесса

Следующим этапом был проведен анализ специфики рабочего процесса удостоверяющего центра. Рабочий процесс обуславливает порядок и последовательность выполнения действий по предоставлению услуг.

Для начала стоит ознакомиться с перечнем информации, обрабатываемой техническими средствами удостоверяющего центра:

— Персональные данные – разновидность информации, которая напрямую или косвенно относится к какому либо физическому лицу и подлежит защите от НСД. Таковыми являются данные о клиентах удостоверяющего центра.

— Коммерческая тайна – вид конфиденциальной информации, составляющей сведения об экономических, технических, финансовых управленческий и других аспектах деятельности организации.

— Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока

Для изучения специфики необходимо представить УЦ более структурировано. Для этого предприятие условно делится на организационные службы. Каждое из подразделений выполняет различного рода обязанности, в совокупности образующие общий рабочий процесс предприятия.

2.2.1 Административный отдел

Сотрудники этого отдела внутри организации осуществляют управление деятельностью УЦ и координируют деятельность сотрудников других отделов. Помимо управленческой составляющей, сотрудники административной службы также взаимодействуют с пользователями (зарегистрированными клиентами), обеспечивая поддержку в решении вопросов, связанных с применением продуктов, изготавливаемых удостоверяющим центром, а также в вопросах подтверждения электронной подписи.

2.2.2 Отдел регистрации

В этом отделе проводится регистрация лиц, подавших заявление на предоставление услуг, как пользователей услуг удостоверяющего центра.

Также сотрудники отдела регистрации обеспечивают ведение реестра зарегистрированных Пользователей УЦ, предоставляют служебные ключи ЭП и сертификаты служебных ключей проверки пользователям УЦ.
В обязанности персонала также входит распространение средств электронной подписи и криптографического преобразования информации заявителям.

2.2.3 Служба безопасности и технической поддержки

В контексте данной дипломной работы, службу безопасности и технической поддержки составляют сотрудники отдела обеспечения безопасности. В обязанности данной службы входит проведение организационных и технических мероприятий по предоставлению услуг и обеспечению безопасности. Таким образом, в компетенцию данного отдела входят организация и выполнение мероприятий по защите обрабатываемой информации, техническому сопровождению распространяемых средств электронной подписи и эксплуатации программных и технических средств. Также отдел занимается изготовлением и предоставлением ключей, сертификатов ключей проверки ЭП на электронном носителе, копий сертификатов ключей проверки на бумажном носителе. В том числе осуществляется, по обращениям пользователей услуг, аннулирование, приостановление и возобновление действия сертификатов ключей проверки ЭП, предоставление копий сертификатов ключей проверки и сведений об аннулированных и приостановленных сертификатах, подтверждение

электронной подписи в документах, представленных в электронной форме и подтверждение подлинности электронных подписей.

Обобщенно, рабочий процесс удостоверяющего центра заключается в непосредственной обработке персональных данных и использовании средств криптографической защиты информации, т.е. средств электронной подписи. При этом, все данные о заказах, заказчиках, списке выданных сертификатов электронной подписи и ключей электронной подписи, а также сведения, составляющие коммерческую тайну хранятся на сервере УЦ. Права доступа, как было сказано выше, ограничены для всех. Это означает отсутствие суперпользователей, которые обладают доступом ко всей обрабатываемой информации. Таким образом обеспечивается защита от утечки информации по сети ЛВС.

Персональные данные предоставляются заявителями на получение услуг удостоверяющего центра и хранятся на сервере. Персонал по обеспечению регистрации обрабатывает персональные данные с целью занесения их в клиентскую базу. Также персоналом по обеспечению регистрации осуществляется выдача выполненного заказа.

Сам процесс выполнения заказа проходит в помещении службы безопасности и технической поддержки. В данном отделе находятся основные технические средства и системы, осуществляющие обработку и криптографическое преобразование КИ. Криптографическое преобразование информации – формирование ключей электронной подписи осуществляется в автоматизированной системе. В качестве СКЗИ используются ключевые носители типа USB–токенРутокен ЭЦП 2.0, поставляемые отечественной компанией.

Автоматизированная система состоит из трех электронно–вычислительных машин. Конфиденциальную информацию, обрабатываемую вАС, составляют только коммерческая тайна, ключевая информация и персональные данные. Исходя из этого аспекта, автоматизированной системе присвоен класс 1–Г, т.е. многопользовательская автоматизированная система

для обработки персональных данных и коммерческой тайны с различными правами доступа пользователей.

В соответствии с требованиями ФЗ № 63 Об ЭП, удостоверяющий центр обязан предоставить доступ к реестру выданных, аннулированных и замороженных сертификатов электронной подписи. Такой доступ предоставляется посредством размещения ссылки скачивания реестра на сайте удостоверяющего центра в сети Интернет. За актуальностью информации в реестре выданных сертификатов обязаны следить персонал обеспечения регистрации и административный персонал удостоверяющего центра.

Специфику рабочего процесса также обуславливают технические средства защиты информации. Для данного удостоверяющего центра были разработаны индивидуальные рекомендации.

Доступ в серверную осуществляется, в соответствии требованию к УЦ, посредством системы контроля доступа с идентификацией по карте. Такие идентификационные карты выдаются персоналу по приказу руководителя Удостоверяющего Центра. Стоит упомянуть, что таковыми являются сотрудники отдела безопасности.

Для предотвращения утечки информации по речевому каналу и техническому каналу ПЭМИН установлено устройство комбинированной защиты Соната РК–1, сочетающее в себе возможность создания маскирующих помех, пространственного зашумления и частичного поглощения информативных сигналов распространяющихся по линиям электропитания и заземления и генерации шумов, препятствующих утечке по акустическому каналу. Также удостоверяющим центром используются средства типа “пилот” – маскираторы электромагнитных излучений и наводок (генераторы электромагнитного шума) Маис–М.

2.3 Угрозы безопасности информации и мероприятия защите

Из–за конкуренции на рынке предоставления услуг в сфере информационных технологий, безопасность информации играет ключевую роль

в жизнедеятельности любой подобной организации. Наличие мер по обеспечению защиты является обязательным требованием уполномоченных органов исполнительной власти, проводящих аттестацию, аккредитацию и выдачу лицензий.

На основе проведенного анализа схем помещений и специфики рабочего процесса и взаимодействия с пользователями УЦ был разработан индивидуальный перечень угроз безопасности информации для данной организации.

Перечень угроз защищаемой информации:

— Видовой канал утечки информации. Реализуется посредством наблюдения нарушителем информации конфиденциального характера. В случае выбранного удостоверяющего центра, с учетом расположения в здании бизнес–центра, наиболее вероятным является осуществление наблюдения в пределах границ контролируемой зоны, т.е на территории здания бизнес–центра или удостоверяющего центра, через дверные проемы. В качестве защиты необходимо организовать меры по контролю за лицами, допущенными в помещения УЦ. Реализация наблюдения через окна помещений менее вероятна, так как помещения УЦ расположены на восьмом этаже бизнес–центра. Тем не менее, следует пресечь данную возможность путем установки окон с зеркальной внешней поверхностью, штор из плотного материала и жалюзи.

— Акустический и вибрационный каналы утечки могут возникнуть в вентиляционных шахтах, трубах теплоснабжения и окнах. Вопрос решается с помощью установления активного генератора пространственного шума Соната РК–1.

— Акустоэлектрический каналы утечки информации могут быть сформированы в электросети и низковольтных линиях, таких как линия охранной сигнализации, системы пожарной сигнализации и интернета, которые расположены в помещениях удостоверяющего центра. Предотвращение утечки – трансформаторная развязка. Это препятствует передаче информации по сети питания.

— Побочные электромагнитные излучения и наводки образуются путем излучения основными техническими средствами и системами электромагнитных полей, воздействующих на сети электропитания и заземления. Для предотвращения утечки информации по такому каналу используются активные методы защиты информации – пространственное зашумление и маскирующие помехи, купирующие возможность выделить информационный сигнал, делая его нечитаемым. В качестве используемых ТСЗИ следует выделить устройство комбинированной защиты Соната РК–1 и устройство маскирования э/м излучений Майс–М.

Проведения подобных исследований, представленных в данной главе, значительно облегчает понимание аспектов деятельности предприятия, особенно при выявлении угроз, условий и факторов угрожающих безопасности защищаемых данных. Также подобные исследования являются основой для реализации организационных и технических мер, направленных на обеспечение соответствия требованиям руководящих документов.

3 Разработка комплекта нормативных актов и регламентов

После изучения и анализа руководящих документов, специфики работы и обустройства помещений предприятия, проведения всех необходимых организационных и технических мероприятий, наступает этап формирования самого комплекта нормативных актов и регламентов, поставляемого в уполномоченный орган удостоверяющим центром.

Данная глава содержит основные выдержки из документов, входящих в состав разработанного пакета – технические паспорта на защищаемые помещения и автоматизированные системы на объекте информатизации с

приведенными схемами размещения ТС, сетей снабжения и пр., перечни конфиденциальной информации и угроз ее безопасности, модель нарушителя, а также инструкции по эксплуатации и пр. Следует заранее отметить, что приказы входящие в комплект, могут быть оформлены только уполномоченным на то лицом. Такими приказами являются:

— о назначении лиц, ответственных за эксплуатацию объекта информатизации;

— на обсуждении в ЗП конфиденциальной информации;

— на проведение работ по защите конфиденциальной информации;

— на обработку вАС конфиденциальной информации

Формирование комплекта документов осуществлялось в соответствии специальным требованиям и рекомендациям по защите конфиденциальной информации. Поскольку, в составе технических паспортов на защищаемые помещения и АС имеется достаточно большой объем требуемых сведений, то разработка комплекта была начата именно с них.

3.1Технический паспорт на ЗП

Технический паспорт – один из важнейших, требуемых для прохождения аттестации, документов. Как правило, он содержит в себе техническую характеристику, эксплуатационные условия, предписания действий касательно помещения, оборудования и пр. В случае защищаемого помещения, технический паспорт обязан содержать сведения об установленном оборудовании, схемы пожарной и охранной сигнализаций, схемы осветительной сети, а также перечень предметов интерьера. Ниже представлен технический паспорт на защищаемое помещение удостоверяющего центра компании ООО "DISTATE".

Технический паспорт на защищаемое помещение №33

3.1.1 Памятка по обеспечению режима безопасности и эксплуатацииоборудования, установленного в защищаемом помещении.

— Лица, на постоянной основе работающие на территории защищаемого помещения, или специально уполномоченное лицо несет ответственность за соблюдение режима безопасности и выполнение требований по эксплуатации технических средств, расположенных в защищаемом помещении

— Все манипуляции с предметами интерьера и оборудования, такие как установка или замена, а также проведение ремонтных работ в защищаемом помещении должны проводиться только после согласования со специалистом по защите информации.

— В нерабочее время помещение должно закрываться наключ.

— В рабочее время, в случае ухода руководителя,помещение должно быть закрыто на ключ или оставлено подответственность лиц, назначенных руководителем подразделения.

— При проведении конфиденциальных мероприятийвспомогательные технические средства и системы, установленные в помещении, должны быть отключены от сети электропитания.

— Для исключения утечки по видовому каналу конфиденциальной информации через окна помещения рекомендуется установить жалюзи.

— Должны выполняться предписания на эксплуатациюсредств связи, вычислительной техники, оргтехники, бытовыхприборов и другого оборудования, установленного в помещении.

— Запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой и тому подобных видов связи.

— Служба безопасности организации обязана проводить ежедневный контроль за выполнением требований по защите помещения

— Специалистами по защите информации должен осуществляться периодический контроль эффективности мер защиты помещения

— Запрещается отключать технические средства защиты информации во при работающих средствах вычислительной техники

3.1.2Перечень оборудования, установленного в защищаемом помещениипредставлен в таблице 1.

Таблица 1

Вид (Тип)оборудования	Класс ТС (ОТСС или ВТСС)	Дата установки (ДД/ММ/ГГ)	Учетный (зав.) номер	Сведения по сертификации, спец исследованиям и спецпроверкам
ЭВМ Asus 1	ОТСС	15.07.16	1641	Программных и аппаратных закладок не обнаружено.
ЭВМ Asus 2	ОТСС	15.07.16	1642	
ЭВМ Asus 3	ОТСС	15.07.16	1643	
Сервер Asus	ОТСС	15.07.16	1644	
Принтер HP	ОТСС	15.07.16	1645	Color LaserJet Professional CP5225dn (CE712A)
Маршрутизатор Cisco	ОТСС	15.07.16	1646	Модель маршрутизатора Cisco 1751 сертифицированная ФСТЭК Росси
Датчик пожарной сигнализации	ВТСС	15.07.16	1647	ИП 212–45
Датчик пожарной сигнализации	ВТСС	15.07.16	1648	ИП 212–45
Датчик	ВТСС	15.07.16	1649	ИП 212–45

охранной сигнализации				
Средство защиты информации	ВТСС	15.07.16	1650	Соната РК–1
Генератор э/м шума	ВТСС	15.07.16	1651	Маис–М
Система контроля доступа	ВТСС	15.07.16	1652	Matrix–II K
Камера видеонаблюдения	ВТСС	15.07.16	1653	OrientAHD–950–OT10B
Система порошкового пожаротушения	ВТСС	15.07.16	1654	Буран 15–КД–В
Кондиционер Toshiba	ВТСС	15.07.16	1655	RAS–10N3AVR–E
Кондиционер Toshiba	ВТСС	15.07.16	1666	RAS–10N3AVR–E

3.1.3 Схемы размещения мебели, электроснабжения и пр.

1) Схема пожарной и охранной сигнализации размещена на рисунке 1

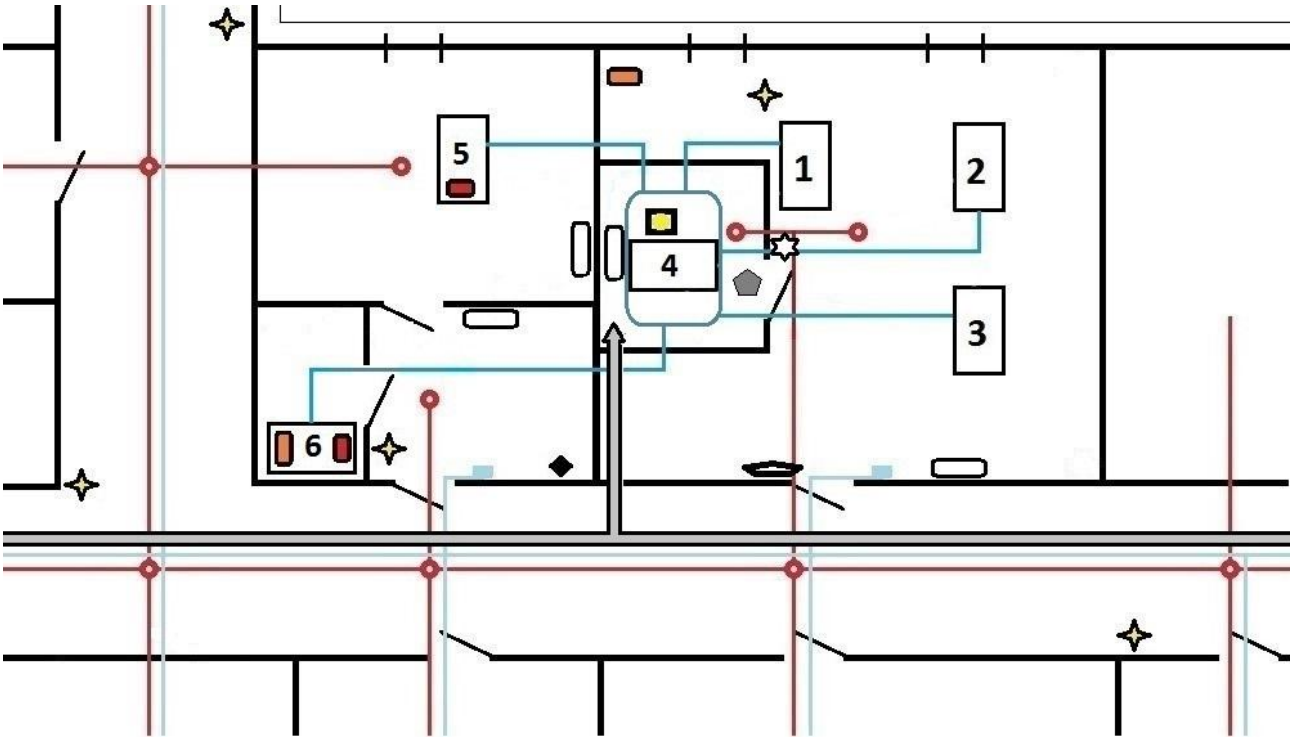


Рисунок 1 – Схема пожарной и охранной сигнализации

2) Схема размещения электроснабжения кабинета,осветительной сети,мебели и предметов интерьера расположена на рисунке 2

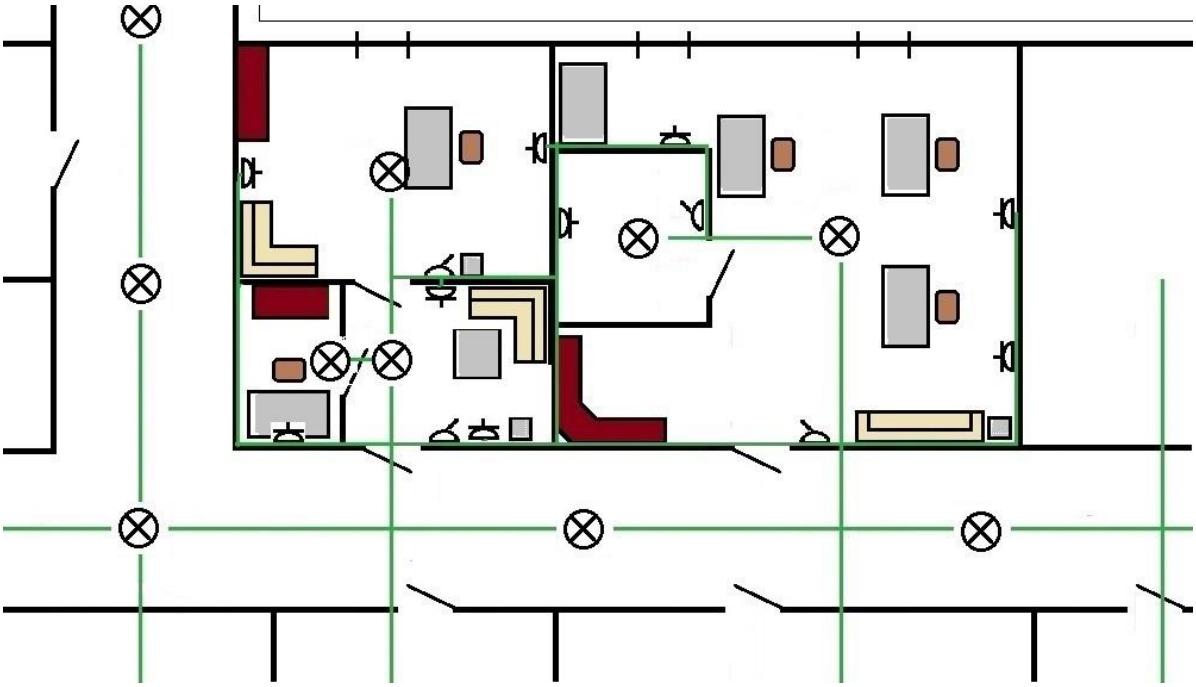


Рисунок 2 – Схема размещения электроснабжения кабинетов,осветительной сети,мебели и предметов интерьера

3.1.4 Перечень мебели и предметов интерьера в защищаемом помещении представлен в таблице 2.

Таблица 2

Учетный (зав.) номер	Вид
9342	Стол 1
9343	Стол 2
9344	Стол 3
9345	Стол 4
9346	Диван
9347	Стул 1
9348	Стул 2
9349	Стул 3

9350	Шкаф угловой

3.1.5 Меры защиты информации

— В защищаемом помещении установлено средство защиты информации Соната РК–1 №7257.

— Выполнены требования предписания на эксплуатацию (Перечень предусмотренных мер защиты согласно предписанию).

— К ЭВМ подключены генераторы электромагнитного шума Маис–М №8125.

— Права доступа к лвс и серверу разграничиваются при помощи сзиSecretNet.

— Доступ в серверную осуществляется через систему контроля доступа с помощью бесконтактных карт.

— Доступ в помещение и нахождение посторонних лиц без присутствия специалиста по безопасности исключен.

— Доступ к вентиляционным каналам, выходящим на чердак здания, посторонних лиц исключен (приводятся предусмотренные для этого меры).

3.2 Технический паспорт на АС

Технический паспорт на автоматизированную систему также является очень важным документом в разрабатываемом комплекте. Он в полной мере отображает структуру, топологию и размещение ОТСС в помещении, в которым размещена АС. В том числе, техпаспорт содержит в себе состав автоматизированной системы – основные и вспомогательные технические средства, установленные на АС. Ниже представлен технический паспорт наАС "КриптоАРМ Стандарт".

3.2.1 Общие сведения об АС

Наименование АС: «КриптоАРМ Стандарт».

Расположение АС: г. Санкт–Петербург, ул. Новорощинская, дом 4, 8 этаж, помещение 33(адрес, здание, строение, этаж, комнаты)

Класс АС: 1Г

(номер и дата акта классификации АС, класс АС)

3.2.2 Состав оборудования АС

1) Состав ОТСС:

Перечень основных технических средств и систем, входящих в состав АС «КриптоАРМ Стандарт» представлен в таблице 1.

Таблица 1

№ п/п	Тип ОТСС	Заводской №	Сведения по сертификации, Специсследованиям и спецпроверкам
1	Монитор	23514563	Программных и аппаратных закладок выявлено не было. Недекларированных возможностей не выявлено
2	Системный блок	45225232	
3	Клавиатура	45673466	
4	Мышь	34562674	

2) Состав ВТСС объекта:

Перечень вспомогательных технических средств, входящих в состав АС «КриптоАРМ Стандарт» (средств вычислительной техники, не участвующих в обработке конфиденциальной информации) представлен на таблице 2.

Таблица 2

№ п/п	Тип ВТСС	Заводской №	Примечание
1	Сетевой фильтр	1534563	Аппаратных закладок выявлено не было. Недекларированных возможностей выявлено не было.
2	Источник бесперебойного питания	7646245	

3) Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта отображены на рисунке 1

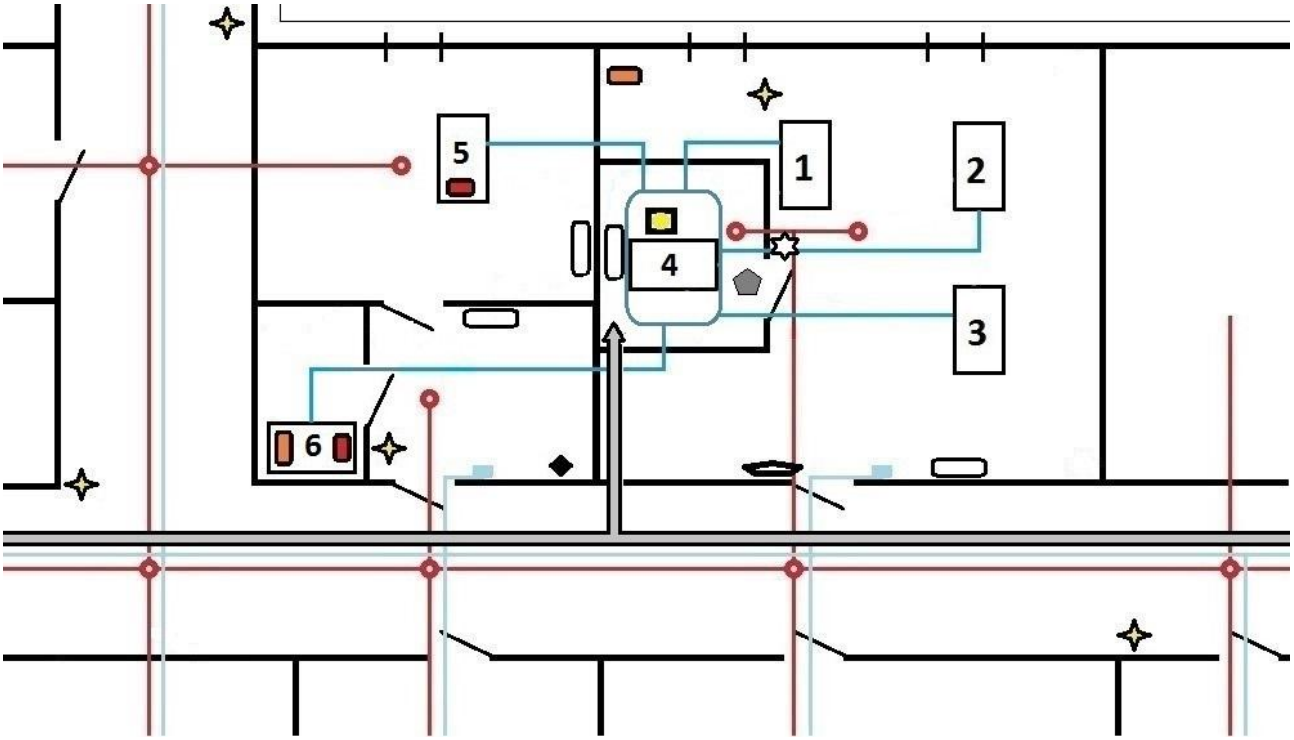


Рисунок 1 – Структура, топология и размещение ОТСС относительно границ контролируемой зоны

4) Система электропитания отображена на рисунке 2

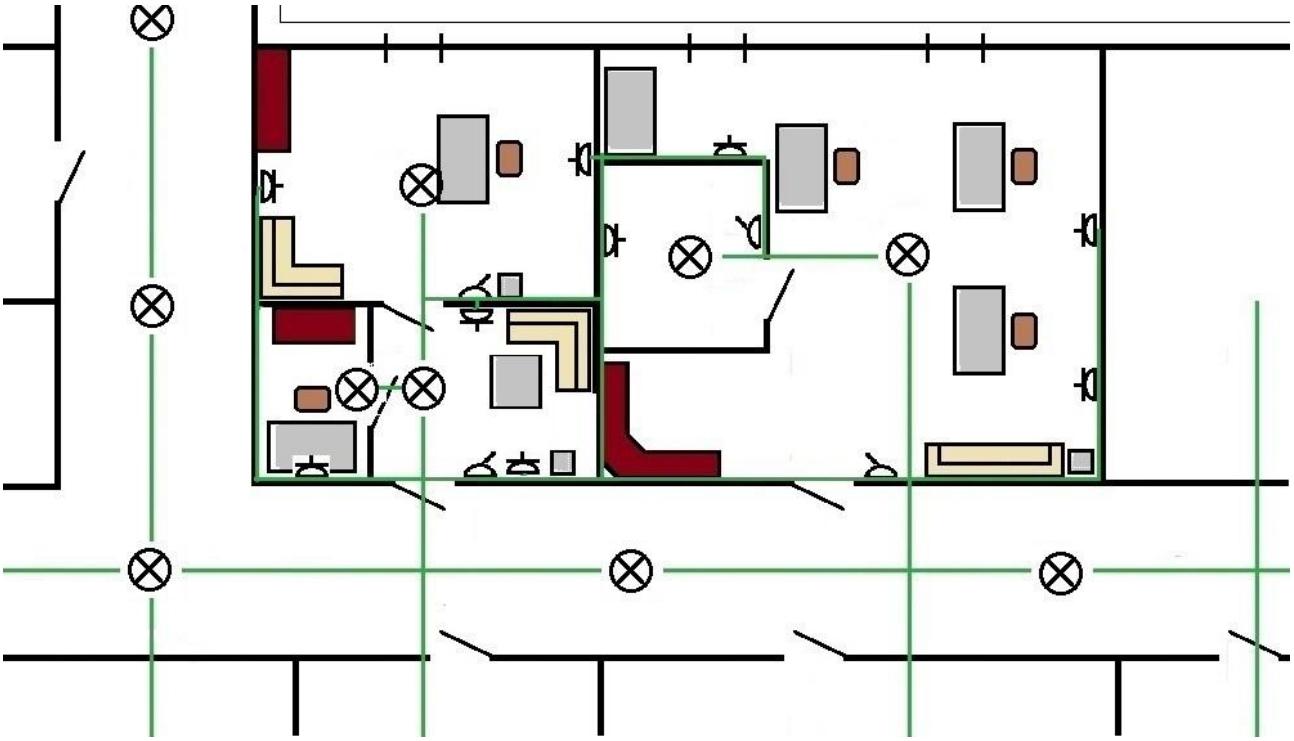


Рисунок 2 – Цепи электропитания

5) Состав средств защиты информации:

Перечень средств защиты информации, установленных наАС «КриптоАРМ Стандарт» представлен на таблице 3

Таблица 3

№ п/п	Наименование и тип Технического средства	Заводской №	Место и дата Установки	Сведения о сертификате
1.	Программно–аппаратный комплекс СЗИ НСД «Соболь»	5657845	АС«КриптоАРМ Стандарт» 10.09.16	№ 907

6) Перечень оборудования, установленного в помещении

Перечень оборудования, установленного в помещении отображен на таблице 4.

Таблица 4

Вид (Тип)оборудования	Класс ТС (ОТСС или ВТСС)	Дата установки (ДД/ММ/ГГ)	Учетный (зав.) номер	Сведения по сертификации, спец исследованиям и спецпроверкам
ЭВМ Asus 1	ОТСС	15.07.16	1641	Программных и аппаратных закладок выявлено не было. Недекларированных возможностей выявлено не было
ЭВМ Asus 2	ОТСС	15.07.16	1642	
ЭВМ Asus 3	ОТСС	15.07.16	1643	
Сервер Asus	ОТСС	15.07.16	1644	
Принтер HP	ОТСС	15.07.16	1645	Color LaserJet Professional CP5225dn (CE712A)
Маршрутизатор Cisco	ОТСС	15.07.16	1646	Модель маршрутизатора Cisco 1751 сертифицированная ФСТЭК России
Датчик пожарной сигнализации	ВТСС	15.07.16	1647	ИП 212–45
Датчик пожарной сигнализации	ВТСС	15.07.16	1648	ИП 212–45

Датчик охранной сигнализации	ВТСС	15.07.16	1649	ИП 212–45
Средство защиты информации	ВТСС	15.07.16	1650	Соната РК–1
Генератор э/м шума	ВТСС	15.07.16	1651	Маис–М
Система контроля доступа	ВТСС	15.07.16	1652	Matrix–II K
Камера видеонаблюдения	ВТСС	15.07.16	1653	OrientAHD–950–OT10B
Система порошкового пожаротушения	ВТСС	15.07.16	1654	Буран 15–КД–В
Кондиционер Toshiba	ВТСС	15.07.16	1655	RAS–10N3AVR–E
Кондиционер Toshiba	ВТСС	15.07.16	1666	RAS–10N3AVR–E

7) Меры защиты информации:

— В защищаемом помещении установлено средство защиты информации Соната РК–1 №7257.

— Выполнены требования предписания на эксплуатацию (Перечень предусмотренных мер защиты согласно предписанию).

— К ЭВМ подключены генераторы электромагнитного шума Маис–М №8125.

— Права доступа к ЛВС и серверу разграничиваются при помощи СЗИSecretNet.

— Доступ в серверную осуществляется через систему контроля доступа с помощью бесконтактных карт.

— Доступ в помещение и нахождение посторонних лиц без присутствия специалиста по безопасности исключен.

— Доступ к вентиляционным каналам, выходящим на чердак здания, посторонних лиц исключен (приводятся предусмотренные для этого меры).

Перечень сведений конфиденциального характера виден в таблице 5

Таблица 5

Наименование сведений	Типы документов, где возможно появление сведений конфиденциального характера
Персональные данные	Анкеты заявителя; данные на сервере; документы,хранимые в сейфе
Коммерческая тайна	
Ключевая информация	

3.3 Акт классификации АС

Разумеется, любая АС должна пройти процесс классификации, присваивающий ей соответствующий класс функционирования с точки зрения информационной безопасности. Классификация должна проводится специальной комиссией. Присваиваемый класс напрямую зависит от типа обрабатываемой АС конфиденциальной информации и матрицы доступа пользователей (многопользовательская с одинаковыми или разными правами,

однопользовательская). Так, например для обработки сведений, составляющих государственную тайну, автоматизированная система должна иметь класс 1А, 2А, 3А, 1Б или 1В, в зависимости от степени секретности сведений и матрицы доступа. Для АС, обрабатывающих конфиденциальную информацию предусматриваются класс 1Г, 1Д, 2Б и 2В. Поскольку, в ас данного удостоверяющего центра будет обрабатываться коммерческая тайна и персональные данные, а доступ к АС – многопользовательский с разными правами, то она относится к классу 1Г. Ниже приведен акт классификации АС "КриптоАРМ Стандарт".

Комиссия, назначенная приказом в составе Председателя комиссии: руководитель отдела криптографической защиты информации Михайлова Е.В., членов комиссии: специалист по защите информации Ёлкина Ксения Валерьевна, ведущий системный администратор Никулин Сергей Сергеевич, провела классификацию автоматизированной системы «АС УЦ» и установила:

3.3.1 Состав автоматизированной системы объекта информатизации «КриптоАРМ Стандарт»

Перечень технических средств автоматизированной системы «КриптоАРМ Стандарт» ООО «ДиСтэйт», расположенной по адресу:г. Санкт–Петербург, ул. Новорощинская, дом 4, помещение 33 представлен в таблице 1.

Таблица 1

№	Название	Уч. (зав.) номер	Модель
1	ЭВМ Asus 1	1641	M32CD–RU029T
2	ЭВМ Asus 2	1642	M32CD–RU029T
3	ЭВМ Asus 3	1643	M32CD–RU029T
4	Сервер Asus	1644	RS500–E6/PS4

5	Монитор	2767	AOC I2775PQU
6	Системный блок	2768	90PD01J8–M12190
7	Клавиатура	2769	K120
8	Мышь	2770	M175

3.3.2 Выявленные определяющие признаки классификации автоматизированной системы:

— Указанная АС входит в состав локальной сети, имеет выход в открытые международные телекоммуникационные сети;

— Наивысший уровень обрабатываемой информации – Конфиденциальная информация (ПДн, Ключевая информация СКЗИ);

— Наличие в рассматриваемой автоматизированной системе (АС) информации различного уровня конфиденциальности: «Конфиденциально», «Строго конфиденциально», «не секретно»;

— Различный уровень полномочий субъектов (пользователей АС) по доступу к защищаемым информационным ресурсам АС;

— Коллективный, последовательный по времени режим работы пользователей АС.

3.3.3 Заключение.

Комиссия, учитывая вышеизложенное и рассмотрев следующие утвержденные документы:

— «Перечень защищаемых ресурсов автоматизированной системы «АС УЦ» ООО «ДиСтэйт» и уровень их конфиденциальности»;

— «Перечень лиц, имеющих право самостоятельного доступа к штатным средствам автоматизированной системы «АС УЦ» ООО «ДиСтэйт» и уровень их полномочий»;

— «Матрица доступа субъектов автоматизированной системы «АС УЦ» ООО «ДиСтэйт» к ее защищаемым информационным ресурсам» .

На основании определяющих признаков классификации и в соответствии с п.п. 1.7., 1.9. руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и руководящим документом Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К)», установила для автоматизированной системы «АС УЦ» ООО «ДиСтэйт» класс защищенности 1Г.

3.4 Инструкция ответственного за защиту конфиденциальной информации

Помимо технических средств обеспечения защиты информации, огромным значением обладают организационные меры. К таким относятся и инструкции лицам, несущим ответственность. Как правило, при разработке, такие инструкции состоят из общих положений, функций и обязательств ответственного лица, а также его прав. Соблюдение всех инструкций и предписаний имеет огромное значение в жизнедеятельности предприятия. Так, бездолжным образом реализованных организационных мер, невозможно представить успешную деятельность предприятия. Ниже приведена инструкция ответственного за защиту конфиденциальной информации на объекте информатизации ООО «ДиСтэйт».

3.4.1 Общие положения

— Ответственный за защиту информации назначается приказом Генерального Директора ООО «ДиСтэйт» (далее Общество)и отвечает за организацию и проведение (внедрение и эксплуатацию) мероприятий по защите информации на объекте информатизации в ходе выполнения работ по обработке защищаемой информации на объекте информатизации.

— Ответственный за защиту информации в своей работе руководствуется положениями руководящих и нормативных документов ФСТЭК России в области защиты информации от утечки по техническим

каналам и регламентирующими документами на объекте информатизации Общества.

— Система защиты конфиденциальной информации (СЗКИ) включает комплекс организационных, технических и программных средств и мероприятий по защите информации.

— Ответственный за защиту информации несет ответственность за функционирование созданной в организации СЗКИ.

— 3.4.2 Функции ответственного за защиту информации.

— Разработка и внедрение системы защиты конфиденциальной информации на объекте информатизации организации.

— Выбор и представление руководителю организации кандидатур на должности в разработанной СЗКИ.

— Методическое руководство специалистами, эксплуатирующими объекты информатизации организации.

— Аналитическое обоснование разработанной СЗКИ, согласование выбора средств вычислительной техники, технических и программных средств защиты.

— Организация работ по выявлению возможностей и предупреждению утечки защищаемой информации.

— Участие в аттестации объекта информатизации организации.

3.4.3 Ответственный за защиту информации обязан:

— Четко знать и выполнять требования руководящих и нормативных документов ФСТЭК России в области защиты информации от утечки по техническим каналам.

— Знать перечень задач, решаемых на объектах информатизации организации.

— Организовать обследование объектов информатизации с целью выявления состава объектов информатизации, опасных факторов и возможных угроз, критических мест циркулирования защищаемой информации,

снижающих уровень защиты, для выработки и определения необходимых мер и средств защиты информации.

— Осуществлять методическое и организационное руководство в части защиты информации персоналом, работающим на объектах информатизации организации.

— Разработать инструкции администратору информационной безопасности, ответственному за эксплуатацию АС и пользователям.

— В случае отказа работоспособности технических средств объектов и средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу их работоспособности.

— Обеспечить постоянный контроль за выполнением специалистами установленного комплекса мероприятий по обеспечению безопасности информации и своих функциональных обязанностей, изложенных в технологических инструкциях.

— Периодически проводить работы и мероприятия по выявлению возможностей и предупреждению утечки защищаемой информации.

— Контролировать выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств АС и отправке их в ремонт.

— Принимать участие в организации и проведении работ по аттестации объектов информатизации.

— Информировать руководителя Общества о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к программным и информационным ресурсам АС.

3.4.4 Ответственный за защиту информации имеет право:

— Контролировать работу эксплуатационного персонала в части использования ими технических средств объекта и средств защиты информации.

— Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования объектов.

— Обращаться за методической помощью к должностным лицам организации.

4 Безопасность жизнедеятельности

Важным моментом в комплексе мероприятий направленных на совершенствование условий труда являются мероприятия по охране труда. Вопрос обеспечения здравоохранения стал одним из элементов конкуренции работодателей в вопросе привлечения кадров. Для реализации в жизнь всех мероприятий по охране труда необходимо обладать знаниями в области физиологии труда, позволяющими оптимально организовать процесс трудовой деятельности человека. В данном разделе дипломного проекта освещаются основные вопросы техники безопасности и экологии труда в отделе информационных технологий.

4.1 Потенциально опасные и вредные производственные факторы

Доступные в настоящее время разработанные комплексы организационных мероприятий и технических средств защиты, накопленный опыт целого ряда центров обработки данных показывает, что можно добиться значительно большего успеха при детальном рассмотрении воздействия на работников опасных и вредных производственных факторов.

Опасным называется производственный фактор, воздействие которого на работающего человека при определенных обстоятельствах может привести к травме или другому внезапному резкому ухудшению здоровья. Если фактор производства приводит к болезни или инвалидности, то он считается вредным. В зависимости от уровня и продолжительности воздействия вредным факторам может быть разный уровень опасности. Опасные и вредные производственные факторы подразделяются на четыре группы: физические, химические, биологические и психофизические.

Рабочие условия и безопасность работников, на сегодняшний день, до сих пор не отвечают современным требованиям. Сотрудники сталкиваются с воздействием физически опасных и вредных производственных факторов, таких как повышенный шум, повышенная температура окружающей среды, отсутствие или недостаток освещения рабочей зоны, электрический ток, статическое электричество и другие.

Многие вредные факторы, связанны с последствиями психических и физических факторов, таких как психическое напряжение, перенапряжение зрительных и слуховых анализаторов, монотонность труда, эмоциональные перегрузки. Воздействие этих негативных факторов приводит к снижению работоспособности, вызванное развивающейся усталости. Также имеет место возникновение и развитие усталости из–за изменений, которые происходят во время работы в центральной нервной системе и с процессами в коре головного мозга.

Медицинские осмотры работников показали, что в дополнение к снижению высоких уровней производительности шумовые воздействия

могутпривести к потере слуха. Долгосрочное присутствие человека в зоне комбинированного воздействия различных неблагоприятных факторов может привести к профессиональному заболеванию. Анализ травматизма среди работников сферы ИТпоказывает, что большинство несчастных случаев происходит в результате воздействия физических угроз безопасности при выполнении не основных работ сотрудников, а также факторов, в которых участвуют влияние электрического тока и халатное отношение к правилам безопасности.

4.1.1 Санитарно–гигиенические требования

Помещения , их размер (площадь, объем) в первую очередь должны соответствовать количеству работников и размещать их наборы технических средств. Они обеспечивают соответствующие параметры температуры, освещения, чистоты воздуха, обеспечивают изоляцию от неблагоприятных воздействий, от производственных шумов и т.д. Для обеспечения нормальных условий труда должны соблюдаться санитарные нормы СН 245–71– набор на одного работника, размеры производственных помещений не менее 15 м3 пола, площадь закрытых стен или перегородок не менее 4,5 м3.

Чтобы обеспечить функционирование компьютера работодатель должен предоставить следующие условия:

— компьютерный зал, комната для размещения службы и периферийного оборудования, помещение для хранения запасных частей, инструментов, устройств (АРР);

— помещения для приточных и вытяжных;

— комната для персонала;

— помещение для приема и выдачи информации.

В случае если, основные объекты расположены в непосредственной близости друг от друга, они должны быть оснащены общей системой вентиляции для разбавления циркулирующего воздуха и системой искусственного освещения. Для комнатных условий машинного зала и хранения магнитных носителей предъявляются особые требования. Площадь

машинного зала должна соответствовать требуемой площади для заводских спецификаций данного типа компьютера.

Высота зала от пола до потолка, с учетом технологического регламента, должна быть 33,5 м. Расстояние между подвесным потолком и основнымдолжно быть в то же время 0,50 м. Обычно применяется боковое естественное освещение. Мастеровые классы и офисы должны иметь естественное освещение. При этом, искусственное освещение допускается в других областях. В тех случаях, когда естественное освещение поступает в недостаточном количестве, необходимо установить комбинированное освещение. Это дополнительное искусственное освещение применяется не только в темноте, но и в дневное время. Искусственное освещение делится в соответствии выполняемой задаче– операционной, чрезвычайные ситуации, эвакуации. Эффективная схема освещения помещения и его цвета направлена на улучшение санитарно–гигиенических условий труда, повышение производительности и безопасности.

Цветовое покрытие пространства влияет на нервную систему человека, его настроение и в конечном счете на производительность труда. Основные производственные площади желательно красить в соответствии с технологией цветопередачи. Освещение номера и установленного оборудования должно быть мягким, без блеска. Снижение шума, создаваемого на рабочем месте от внутренних источников, а также шума проникающего извне, является очень важной задачей. Снижение шума в источнике излучения может быть достигнуто с помощью эластичных прокладок между машинным базовым блоком и опорной поверхностью. В качестве прокладок используются резина, войлок, пробка, различные конструкции–амортизаторы. Под шумные технические средства рабочего стола следует прокладывать грунтовочные мягкие коврики из синтетических материалов, а под ножки столов, на которых они установлены – мягкие резиновые прокладки, войлок, толщиной 68 мм. Крепление прокладок возможно путем склеивания их поддерживающих частей. Также может быть использована прокладка звукоизолирующими кожухами, которые не мешают процессу. Не менее важным способом, чтобы уменьшить

шум во время работы, является вопрос правильной и своевременной регулировки, смазывания и замены механических узлов шумного оборудования. Рациональное расположение предметов интерьера помещения и размещение оборудования являются важными факторами, которые позволят техническим средствам уменьшить шум. При планировании компьютерный зал и оборудование обслуживания должны быть размещены вдали от шумного и вибрационного оборудования.

Снижение шума, проникающего в помещение извне может быть достигнуто за счет увеличения акустической ограждающие конструкции – уплотнение по периметру окна, крыльца и двери. Таким образом, для уменьшения шума, создаваемого на рабочих местах внутренними источниками, а также шума, проникающего снаружи следует:

— уменьшить мощности (использование экранов, звук корпус) источников шума;

— уменьшить эффект кумулятивного воздействия отраженных звуковых волн (звукопоглощающие поверхности конструкций);

— применять рациональное расположение оборудования;

4.2 Безопасность при обращений с электрооборудованием

Электрический ток представляет собой скрытый тип опасности, так как трудно определить качество материалов в токопроводящем оборудовании, которые могут являться хорошими проводниками электричества. Смертельная опасность – ток, величина которого превышает 0,05А, ток меньше 0,05А для человеческой жизни – безопасен. Для предотвращения поражения электрическим током, обеспечения безопасности работы эксплуатация технических средств и проведение работ должно быть разрешено только тем сотрудникам, которые хорошо изучили и сдали требования и основные правила безопасности.

Электроустановки, которые включают в себя практически все компьютерное оборудование, полны большой потенциальной опасности для

человека, так как в процессе эксплуатации или проведения работ по техническому обслуживанию, любой из людей может коснуться какого–либо элемента электропитания, находящегося под напряжением. Специальную опасность поражения электрическим током могут содержать в себе самые различные системы и их элементы – токоведущие провода, составляющие элементы стойки компьютеров и другого оборудования, которые находятся под напряжением и в результате повреждения (пробоя) изоляции, не подают каких–либо сигналов, которые предупреждают об опасности человека. Решающее значение для предотвращения фактора поражения электрическим током заключается в правильной организации обслуживания существующих электрических трансформаторов напряжения, ремонта, монтажа и технического обслуживания.В зависимости откатегории помещения, необходимо принять определенные меры для обеспечения надлежащей электрической безопасности при эксплуатации и ремонте электрооборудования. Возникновение разряда статического электричества часто происходит при прикосновении к любому из компонентов компьютера. Такой уровень опасности для человека незначителен, но, кроме дискомфорта, они могут привести к повреждению компьютера. Для того, чтобы уменьшить величину поломок электрооборудования, возникающего из–за статического электричества, в процессе покрытия полов следует использовать однослойный ПВХ линолеум с антистатическим покрытием. Другим методом защиты является нейтрализация статического электричества под воздействием ионизированного газа. Общие меры защиты от статического электричества также включают в себя общее и местное увлажнение воздуха.

4.3 Организация и оборудование рабочих мест с ПЭМВ

Требования к организации и оборудованию рабочего места персонала, работающего с ПЭМВ приведены в ГОСТ 12.2.03278. Высота рабочей поверхности стола для пользователя должна регулироваться в пределах 680–800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм. Следует учитывать модульные размеры рабочей

поверхности стола для ПК, на основании которых должны рассчитываться конструктивные размеры: ширина 800, 1200, 1400 мм, глубина 800 и 1000 мм с неправильной высотой, равной 725 мм. Стол должен быть с высотой пространства для ног 600 мм, шириной– не менее 500 мм, глубиной на уровне колен – не менее 450 мм, на уровне вытянутых ног – не менее 650 мм. Рабочий стул (кресло) должен быть подъемно–поворотным и регулируемым по высоте и углу наклона, угла сиденья и спинки, а также расстояние спинки до переднего края сиденья.

Рабочее место должно быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубиной не менее 400 мм, для регулировки высоты до 150 мм и наклонаопорный поверхности 20 градусов. Поверхность подставки должна быть рифленой и иметь по переднему краю обода высотой 10 мм. Клавиатура должна располагаться на поверхности стола на расстоянии 100–300 мм от края и обращена к пользователю, или на регулируемой по высоте рабочей поверхности отделена от основной рабочей поверхности.

Таким образом, выполняя все вышеуказанные меры по безопасности при обращении с электрическими приборами и организации рабочего места сотрудника отдела информационных технологий, можно повысить не только уровень работоспособности сотрудников предприятия, но и значительно снизить риски, связанные с работой в помещении, содержащим электрическое оборудование, электронно–вычислительные машины и прочие потенциально опасные инструменты, используемые в процессе работы.

Экономическое обоснование ВКР

Многим предприятиям, для обеспечения жизнедеятельности и функционирования, требуется квалифицированная поддержка и помощь компетентных специалистов, так как зачастую выполнить какие–либо работы самостоятельно по разным причинам нет возможности. В связи с этим, очень часто руководители предприятий обращаются за помощью в специальные организации, предоставляющие такие услуги на платной основе. Не являются исключением и работы, связанные с подготовкой к прохождению аккредитации или получению лицензии в уполномоченных государственных органах. Разумеется, на рынке имеются услуги и в такой сфере. К примеру, средняя стоимость услуг по составлению пакета документов, необходимых для прохождения аттестации, по разным данным, составляет около 80 000 тысяч рублей.

Данная работа выполнялась на безвозмездной основе, с целью получения практического опыта подготовки предприятия к получению лицензии.

Заключение

Подводя итоги проделанной работы, хотелось бы отметить, что прохождение аккредитации имеет огромное значения для удостоверяющих центров. Однако, подготовка к этому – долгий и кропотливый процесс, подразумевающий как организационные, так и технические мероприятия, направленные на устранение несоответствий требованиям аккредитующего органа. В частности, большое значение играет составление пакета необходимых документов. Исходя из этой информации, в данной выпускной квалификационной работе было решено разработать комплект нормативных актов и регламентов для удостоверяющего центра. В ходе выполнения дипломной работы были выполнены поставленные задачи. Первая глава раскрывает основные аспекты, актуальных на первых этапах подготовки удостоверяющего центра – анализ руководящих документов и выполнение требуемых мероприятий. В данном случае руководящими документами выступают федеральные законы и приказы уполномоченных органов. В том числе был выполнен ряд мероприятий таких как:

- Подготовка исходных данных для прохождения аттестации защищаемого помещения;
- Подготовка исходных данных для прохождения аттестации автоматизированной системы в защищаемом помещении;
- Подготовка исходных данных для получения удостоверяющим центром лицензии ФСБ на средства защиты криптографической информации.

Во второй главе показан анализ специфики рабочего процесса, а также составлены схемы помещений и размещенного в них оборудования и предметов интерьера.

Третья глава представляет выдержки из комплекта нормативных документов, разработанного на основании изученных требований и проанализированной специфики работы и обустройства удостоверяющего центра.

Список использованной литературы

1. Федеральный закон РФ от 06 апреля 2011 г.№ 63–ФЗ "Об электронной подписи"
2. Приказ ФСБ России от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)»
3. Приказ ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну"
4. Федеральный закон от 27 июля 2006 г. № 149–ФЗ "Об информации, информационных технологиях и о защите информации"
5. Аттестационные испытания по требованиям безопасности информации защищаемого помещения[Электронный ресурс]URL:http://edinstvo–spb.ru/zashchishchaemye–pomeshcheniya (Дата обращения: 08.01.2017)
6. Аттестационные испытания по требованиям безопасности автоматизированной системы [Электронный ресурс]URL:http://edinstvo–spb.ru/avtomatizirovannye–sistemy (Дата обращения: 15.01.2017)
7. Практика получения лицензий ФСТЭК и ФСБ[Электронный ресурс]URL:http://bis-

expert.ru/sites/default/files/miscellaneous/practic_licenc_fstec(Дата обращения: 20.01.2017)

8. Об аккредитации удостоверяющих центров Министерство связи и массовых коммуникацийй[Электронный ресурс]URL:http://minsvyaz.ru/ru/documents/3713/ (Дата обращения: 13.01.17)
9. ВТСС. ОТСС. Функциональное назначение. Характеристики образования технических каналов утечки информации. Критерии защищенности [Электронный ресурс]URL:http://studopedia.ru/4_29945_vtss–otss–funktsionalnoe–naznachenie–harakteristiki–obrazovaniya–tehnicheskih–kanalov–utechki–informatsii–kriterii–zashchishchennosti.html (Дата обращения: 20.01.2017)
10. Требования к помещению удостоверяющего центра[Электронный ресурс]URL:ttps://www.cryptopro.ru/forum2/default.aspx?g=posts&m=9889 (Дата обращения: 24.01.2017)
11. Руководящий документ ФСТЭК от 30 марта 1992 г. “Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации”
12. "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных." ФСТЭК России от 15 февраля 2008 г.
13. Специальные требования и рекомендации по защите информации (СТР–К)№ 7.2 от 02 марта 2001 г.
14. Доктрина информационной безопасности Российской Федерациот 09.09.2000 № ПР. 1895. 2004г.– 48 стр.
15. Садердинов А. А., Трайнѐв В. А., Федулов А. А.Информационная безопасность предприятия: Учебное пособие. Москва:2005 – 336 с.
16. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. Брянск:2007 – 223 с.

17. Гришина Н.В.Организация комплексной системы защиты информации. Москва:2007– 256 с
18. В.А.Кулишкин. Организационно–правовое обеспечение информационной безопасности : Краткий курс лекций. Санкт–Петербург: 2007 –149 с.
19. Е.А. Степанов., И.К. Корнеев.Информационная безопасность и защита данных: Учебное пособие. Москва: 2001– 304 с.
20. Ю.А. Родичев.Информационная безопасность: нормативно–правовые аспекты: Учебное пособие.Санкт–Петербург: 2010 –272с.
21. Д.А. Скрипник. Общие вопросы технической защиты информации. Москва: 2012–264 с.
22. Ю.Н. Загинайлов.Правовые основы защиты информации: Учебное пособие. Алтай: 2000 – 130 с.
23. А.А. Парошин.Нормативно–правовые аспекты защиты информации: Учебное пособие. Владивосток: 2010 – 116с.
24. С.Я. Казанцев Белов Е.Б., Згадзай О.Э.Правовое обеспечение информационной безопасности: Учебное пособие. Москва: 2005 – 240 с.
25. А.В. Терехов, Е.В. Бурцева. Правовое обеспечение информационной безопасности : методические указания. Тамбов: 2010 – 160 с.
26. Ю.А. Родичев. Информационная безопасность: нормативно–правовые аспекты: Учебное пособие. Санкт–Петербург: 2010 – 272 с.
27. Гайкович В.Ю., Ершов Д.В. Основные стандарты и руководящие документы в области защиты информации. Москва, 1994 – 24 с.
28. Шрамкова И.Г., Крат Ю.Г.Защита и обработка конфиденциальных документов. Хабаровск: 2008 – 140 с.
29. Федеральный закон РФ от 27 июля 2006 г. №152–ФЗ «О персональных данных»
30. Федеральный закон РФ от 08 августа 2001г. №128–ФЗ «О лицензировании отдельных видов деятельности»

Приложение

ИНСТРУКЦИЯ Администратора информационной безопасности

1. Общие положения.

1.1 Администратор информационной безопасности назначается приказом Генерального Директора ООО «ДиСтэйт» (далее Общество)и отвечает за обеспечение устойчивой работоспособности и информационной безопасности объекта информатизации.

1.2Администратор информационной безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в автоматизированной системе, а также правильность использования и нормального функционирования средств защиты информации (СЗИ), подготовку пользователей по вопросам безопасной обработки информации на СВТ.

1.3 Система защиты информации (СЗИ) в АС от несанкционированного доступа (НСД) построена на основе функционирования программно–аппаратного средства и организационно–технических мер защиты информации.

1.4 Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от НСД. При организации парольной защиты необходимо руководствоваться требованиями соответствующих пунктов данной инструкции.

1.5 Администратор информационной безопасности в своей работе руководствуется положениями федеральных законов, руководящими и нормативными документами ФСТЭК России и регламентирующими

документами на данном объекте информатизации, руководством администратора информационной безопасности, комплектом документации СЗИ от НСД.

2 Функции Администратора информационной безопасности.

2.1 Осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

2.2 Осуществляет настройку и сопровождение подсистемы управления доступом, при этом:

— реализует полномочия доступа для каждого пользователя к элементам защищаемых информационных ресурсов АС на основе утвержденной разрешительной системы доступа к АС;

— проводит периодическую проверку работоспособности системы защиты от НСД, а также при изменении программной среды и полномочий пользователей АС;

— один раз в месяц, а также в случае необходимости (при компрометации пароля) производит смену паролей пользователей для доступа в систему.

Периодически, по указанию Генерального Директора Общества уточняет список прав доступа и полномочия сотрудников по доступу к средствам ВТ, которые используются для обработки защищаемых сведений.

3 Администратор информационной безопасности обязан:

3.1 Обеспечивать функционирование и поддерживать работоспособность средств защиты автоматизированного рабочего места в пределах возложенных на него функций.

3.2В случае отказа работоспособности технических средств и программного обеспечения СВТ, в том числе средств защиты АС, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.3 Информировать Генерального Директора Общества о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам АС.

3.4 Знать перечень АС, предназначенных для обработки защищаемой

информации, и перечень задач, решаемых с их использованием.
3.5 Немедленно сообщать ответственному по защите информации об имевших место попытках несанкционированного доступа к информации и техническим средствам АС, а также принимать необходимые меры по устранению нарушений.
3.6 В случае выявления каких–либо неквалифицированных действий пользователей, несущих в себе угрозы для безопасности информации, поставить в известность об этом ответственного по защите информации, временно заблокировать возможность работы этого пользователя и организовать дополнительные занятия с ним.
3.7Не реже 1 раза в неделю выполнять работу по администрированию АС, проверять данные в системном журнале и в случае необходимости распечатывать системные журналы СЗИ. В случае выявления попыток НСД к защищаемой информации представлять данный журнал ответственному по защите информации.
3.8 Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств АС и отправке их в ремонт.
3.9 Присутствовать (участвовать) в работах по внесению изменений в аппаратно–программную конфигурацию АС.
3.10 Контролировать соответствие состава АС техническому паспорту.
3.11 Хранить, осуществлять прием и выдачу персональных идентификаторов пользователей, производить выработку и выдачу пользователям паролей, осуществлять контроль за правильностью использования персональных идентификаторов и паролей пользователями АС.
3.12 Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам АС. При выявлении таковых сообщать о них ответственному за защиту информации.
3.13 Проводить инструктаж пользователей АС по правилам работы с используемой СЗИ НСД.

3.14 Не реже одного раза в год проводить тестирование всех функций СЗИ НСД с помощью специальных программных средств.

4 Администратор информационной безопасности имеет право:

4.1 Контролировать работу пользователей в автоматизированной системе.

4.2 Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АС.

5 Организация парольной защиты при работе на объекте информатизации:

5.1 Личные пароли доступа пользователей к системе защиты от НСД объекта информатизации, выбираются Администратором информационной безопасности при соблюдении следующих требований:

—длина пароля должна быть не менее 8–ми буквенно–цифровых символов;

—пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АС, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

—не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

—не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

—при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

—в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

—не использовать ранее использованные пароли.

5.2 Лица, использующие паролирование, обязаны:

—четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

—своевременно сообщать Администратору информационной безопасности о

всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

5.3 При организации парольной защиты запрещается:

—записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

—хранить персональные идентификаторы в общедоступных местах;

—сообщать посторонним лицам свой пароль, а также сведения о применяемой системе защиты от НСД.

Описание технологического процесса обработки конфиденциальной информации в автоматизированной системе

Обработку информации в автоматизированной системе «КриптоАРМ Стандарт» ООО«ДиСтэйт» имеют право пользователи имеющие доступ к объекту информатизации в соответствии с разрешительной системой доступа утвержденной приказом Генерального Директора Общества

Перечень объектов и субъектов доступа указаны в «Разрешительной системе допуска к конфиденциальной информации…» Все пользователи допущенные к обработке конфиденциальной информации (далее информации) зарегистрированы в установленной системе защиты информации от несанкционированного доступа

Перечень штатных средств доступа к информации автоматизированных систем:

–MicrosoftWindows 7 Professional

– Средство для обеспечения работы с криптографическими средствами «КриптоАРМ Стандарт»

–Средство криптографической защиты информации «КриптоПро»

Перечень средств защиты информации установленных в АС:

–Программно–аппаратный комплекс СЗИ НСД «Соболь»

На объекте информатизации разрешается обработка конфиденциальной информации Ключевая информация СКЗИ персональные данные

Описание правил работы.

Обработка и запись информации осуществляется только на предварительно учтенных носителях информации прошедших антивирусный контроль

При необходимости разрешается передача носителей с содержащейся на них защищаемой информацией между пользователями под роспись в соответствующем журнале

Обращение с носителями содержащими защищаемую информацию организуется порядком принятым в организации по работе с конфиденциальной информацией

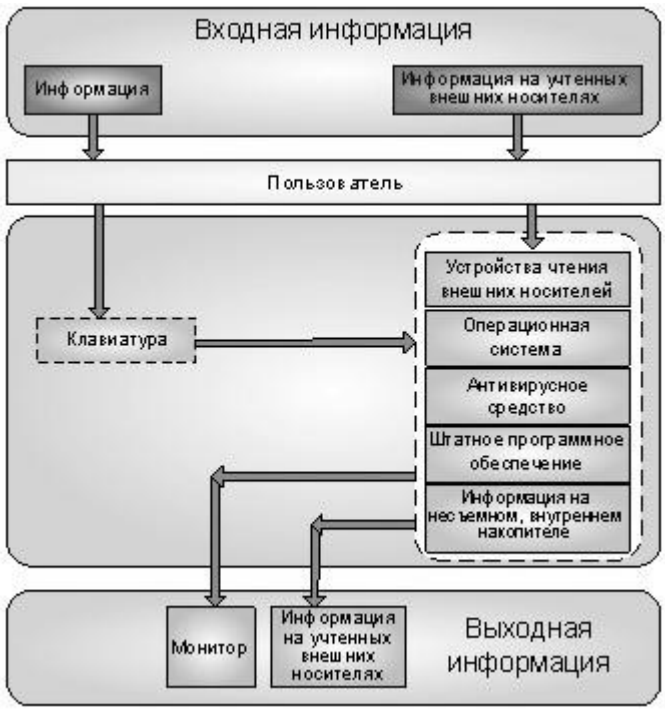
Доступ пользователя к АС осуществляется идентификатором и вводом пароля Персональный пароль выдается пользователю Администратором информационной безопасности с последующей его периодической заменой на новый

Администратор информационной безопасности организует контролирует и несет ответственность за доступ к защищаемым ресурсам АС

По окончании рабочего дня все внешние носители с защищаемой информацией убираются и закрываются установленным порядком

Пользователь используя штатные средства доступа выполняет обработку и вывод защищаемой информации на учтенные носителю

7. Схема информационных потоков обработки информации:



Инструкция по организации антивирусной защиты

1.Настоящая Инструкция предназначена для Администратора информационной безопасности и пользователей, обрабатывающих информацию на объекте информатизации ООО «ДиСтэйт».

2.В целях обеспечения антивирусной защиты на автоматизированной системе«АС УЦ» производится антивирусная защита. Обязательному антивирусному контролю подлежат вся информация, получаемая на внешних носителях из сторонних организаций.

3.Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Администратора информационной безопасности,ответственного за эксплуатацию автоматизированной системы.

4.К применению наАС допускаются лицензионные антивирусные средства.

5.Пользователи объекта при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

6.Ярлык для запуска антивирусной программы должен быть легко доступен(вынесен в окно "Рабочий стол" операционной системы).

7.Администратор информационной безопасности осуществляет периодическое обновление антивирусных пакетов (не реже одного раза в месяц). Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

8.Администратор информационной безопасности, пользователь проводят периодическое тестирование всего установленного программного обеспечения, записанных на хранение защищаемых ресурсов на предмет отсутствия компьютерных вирусов. Результаты проверки фиксируются в «Журнале проверок АС» по каждому объекту отдельно (ведется по произвольной форме).

9.При обнаружении компьютерного вируса пользователь обязан немедленно установленным порядком его уничтожить, поставить в известность

Администратора информационной безопасности об обнаружении компьютерного вируса.

Инструкция ответственного за эксплуатацию автоматизированной системы

1 Общие положения.

1.1 Ответственный за эксплуатацию автоматизированной системы «АС УЦ» – назначается приказом Генерального Директора ООО «ДиСтэйт»и отвечает за обеспечение работоспособности и информационной безопасности автоматизированной системы при обработке защищаемой информации.

2 Методическое руководство работой ответственного за эксплуатацию АС осуществляется ответственным за защиту информации.

3 Ответственный за эксплуатацию АС в своей работе руководствуется положениями руководящих и нормативных документов ФСТЭК России и регламентирующими документами на данном объекте информатизации.

2 Функции ответственного за эксплуатацию АС.

2.1Осуществляет контроль за целевым использованием автоматизированной системы, а также всех его внешних устройств.

2.2Осуществляет контроль за техническим обслуживанием АС, тестированием программных и аппаратных средств, обновлением необходимого программного продукта.

2.3Проводит периодический контроль принятых мер по защите.

2.4Обеспечивает работоспособность и информационную безопасность АС.

2.5Осуществляет координацию действиями персонала автоматизированной системы при возникновении нештатных ситуаций.

3 Обязанности ответственного за эксплуатацию АС.

3.1Четко знать и выполнять требования действующих нормативных и руководящих документов ФСТЭК России, а также внутренних инструкций по вопросам защиты.

3.2Обеспечивать надежное функционирование и поддержание работоспособности средств защиты информации, установленных в АС.

3.3 В случае отказа работоспособности технических средств и программного обеспечения, в том числе средств защиты информации, сообщить ответственному за защиту информации или администратору информационной безопасности и принять меры к выявлению причин, приведших к отказу работоспособности.

3.4Обеспечивать постоянный контроль за правильной эксплуатацией пользователями, установленных правил работы на АС.

3.5Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.6 Знать перечень задач, решаемых с использованием АС.

3.7 Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств АС.

3.8 Присутствовать при выполнении технического обслуживания АС, при установке (модификации) программного обеспечения.

3.9 Информировать ответственного за защиту информации или администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам АС.

3.10 Контролировать соответствие состава АС техническому паспорту на АС (в т.ч. реальной конфигурации информационных связей).

3.11 В случае обнаружения факта несанкционированного проникновения в помещение объекта информатизации, использования АС объекта лицами, не допущенными к этой работе незамедлительно сообщить ответственному за защиту информации.

4 Ответственный за эксплуатацию АС имеет право:

4.1Контролировать работу пользователя в части использования ими средств защиты информации.

4.2 Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного

порядка работ или нарушения функционирования АС.
4.3 Обращаться за методической помощью к ответственному за защиту информации на объекте информатизации.

Инструкция пользователя средств криптографической защиты информации (СКЗИ) общества с ограниченной ответственностью «ДиСтэйт»
1. ОБЩИЕ ПОЛОЖЕНИЯ
1.1 Настоящая инструкция определяет:
• порядок обращения со средствами криптографической защиты информации (далее – СКЗИ) и криптографическими ключами;
• основные обязанности, права и ответственность Пользователя СКЗИ (далее – Пользователя);
• действия при компрометации ключей и восстановлении конфиденциальной связи;
• специальные требования по обработке информации с использованием СКЗИ;
1.2 Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.
1.3 Деятельность Пользователя контролируется его непосредственным руководителем.
2.ОСНОВНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ
Пользователь обязан:
2.1 Соблюдать требования по обеспечению безопасности функционирования СКЗИ.
2.2 Обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.
2.3 Сдать в ООО «ДиСтэйт» носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.
2.4 Сдать в ООО «ДиСтэйт» носители ключевой информации по окончании

срока действия сертификата ключа. В случае компрометации ключа сообщить об этом руководителю Общества и сдать носители ключевой информации.
2.5 Немедленно уведомлять как руководителя так и организацию выдавшую электронную подпись о компрометации криптографических ключей.
2.6 Немедленно уведомлять как руководителя так и организацию выдавшую электронную подпись фактах утраты или недостачи СКЗИ, НКИ.
2.7 В пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.
3. ПРАВА ПОЛЬЗОВАТЕЛЯ
Пользователь имеет право:
3.1 Вносить предложения Руководству по совершенствованию СКЗИ.
3.2 Повышать уровень квалификации по использованию СКЗИ.
4. ПОРЯДОК ОБРАЩЕНИЯ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
4.1 Монтаж и установка СКЗИ осуществляются уполномоченным лицом (Администратором безопасности).
4.2 Служебные помещения, в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и поубытии сотрудников закрываются, опечатываются личными печатями ответственных лиц (либо закрываются кодовым замком) и сдаются под охрану.
4.3 Необходимо использовать такие системы охранной сигнализации, которые позволяют контролировать доступ в помещение с СКЗИ. Исправность сигнализации должна проверяться при каждой сдаче помещений с отметкой в журнале приема–сдачи служебных помещений под охрану.
4.4 Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей должны храниться в сейфе руководителя

подразделения в упаковках, опечатанных личными печатями пользователей. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменен.

4.5 К эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным СКЗИ.

4.6 Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

5. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

5.1 Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

5.2 Сертификат ключа подписи – документ на бумажном носителе или электронный документ сэлектронной цифровой подписью Удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются Удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

5.3 Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющимс помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

5.4 Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки

соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

5.5 Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи владельца ключа в документе на бумажном носителе при одновременном соблюдении следующих условий:

• Сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

• подтверждена подлинность электронной цифровой подписи в электронном документе;

• электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

6. ПОРЯДОК ОБРАЩЕНИЯ С КЛЮЧАМИ ЭЦП

6.1 Криптографический ключ владельца ключа применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптоключей.

Владелец ЭЦП – пользователь СКЗИ, получивший установленным порядком право использовать персональный ключ ЭЦП для удостоверения содержания электронных документов и своего авторства.

Доверенное лицо Владельца ЭЦП – пользователь СКЗИ, получивший установленным порядком право использовать ключ Владельца ЭЦП для удостоверения содержания электронных документов и авторства Владельца. Назначение владельцев ЭЦП и доверенных лиц осуществляется на основании приказа о назначении пользователей СКЗИ.

6.2 Изготовление и выдача ключей ЭЦП осуществляется отделом криптографической защиты Общества на основании предоставленного

Заявления на изготовление ключа ЭЦП (Приложение 1) и, в случае, если интересы Владельца представляет доверенное лицо, Доверенности на изготовление и получение ключа ЭЦП (Приложение 2).В случае, выдачи ключей ЭЦП сторонним Удостоверяющим центром, документы, регламентирующие выдачу ЭЦП устанавливаются этим Удостоверяющим центром.

6.3 Выработанные секретные криптоключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

6.4 НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации Владельца ключа, защиты электронного документа от подделки, компрометации.

6.5 Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

6.6 Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня Пользователь обязан сдавать НКИ лицу, ответственному за хранение.

6.7 Не позднее 10 дней до окончания срока действия сертификата криптоключей Пользователь предоставляет в ООО «ДиСтэйт» заявление на изготовление нового ключа (Приложение 1).

6.8 Использование криптоключей, выведенных из действия, запрещается.

6.9 Категорически запрещается:

• осуществлять несанкционированное и безучетное копирование ключевых данных;

• хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

• передавать НКИ каким бы то ни было лицам, кроме Владельца ключа;

• во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

• хранить на НКИ какую–либо информацию, кроме ключевой;

• использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации.

7. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ И ВОССТАНОВЛЕНИИ КОНФИДЕНЦИАЛЬНОЙ СВЯЗИ

7.1 Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

7.1.1 Утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

7.1.2 Увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

7.1.3 Передача секретных ключей по линии связи в открытом виде;

7.1.4 Нарушение правил хранения криптоключей;

7.1.5 Вскрытие фактов утечки передаваемой информации или ее искажения (подмены, подделки);

7.1.6 Отрицательный результат при проверке наложенной ЭЦП;

7.1.7 Несанкционированное или безучетное копирование ключевой информации;

7.1.8 Все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

События 7.1.1 – 7.1.5 должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

7.2 При наступлении любого из перечисленных выше событий владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в отдел криптографической защиты ООО «ДиСтэйт» либо сторонний Удостоверяющий

Центр, выпустивший ключ, лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа обязан убедиться, что его сообщение получено и прочтено адресатом.

7.3 При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

7.4 Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь повторно заказывает в ООО «ДиСтэйт» новые ключи ЭЦП на основании предоставленного Заявления (Приложение 1).

8. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

8.1 Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

8.2 В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим Законодательством Российской Федерации.