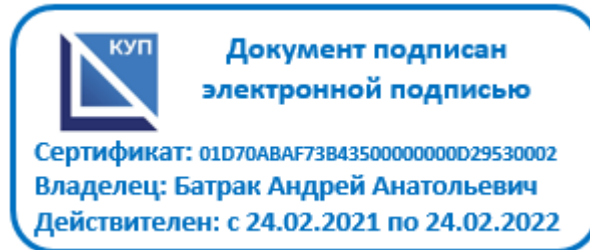




Частное профессиональное образовательное учреждение  
«КОЛЛЕДЖ УПРАВЛЕНИЯ И ПРОИЗВОДСТВА»

УТВЕРЖДАЮ  
Директор ЧПОУ «КУП»



А.А.Батрак  
« 20 » декабря 2021 г.

**Методические рекомендации по подготовке выпускной  
квалификационной работы  
для обучающихся специальности  
10.02.05 Обеспечение информационной безопасности  
автоматизированных систем**

**Год приёма на обучение: 2018**

Москва, 2021

Методические рекомендации разработаны на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО)  
10.02.05 Обеспечение информационной безопасности автоматизированных систем

**Организация разработчик:** Частное профессиональное образовательное учреждение колледж управления и производства

Рассмотрены и одобрены:

ПЦК Социально-экономического профиля и ПЦК Технического профиля  
Протокол № 2 от «19» ноября 2021 г

## Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ .....	4
2.ПОРЯДОК ВЫПОЛНЕНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ .....	5
3. СТРУКТУРА И СОДЕРЖАНИЕ ВКР .....	5
3.1. Структура дипломной работы (проекта):.....	5
4. ПЕРЕЧЕНЬ РЕЗУЛЬТАТОВ, ДЕМОНСТРИРУЕМЫХ НА ГИА .....	6
ПРИЛОЖЕНИЕ 1.....	9
ПРИЛОЖЕНИЕ 2.....	10
ПРИЛОЖЕНИЕ 3 .....	11

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Методические рекомендации по подготовке выпускной квалификационной работы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем составлены в соответствии с требованиями ФГОС СПО в части подготовки выпускной квалификационной работы.

Выпускная квалификационная работа (дипломная работа) (далее, ВКР) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем представляет собой исследование одной из актуальных тем в рамках содержания одного или нескольких профессиональных модулей, должна способствовать продолжению формирования профессиональных и общих компетенций, и направлена на демонстрацию сформированности компетенций, умений, знаний в рамках основных видов профессиональной деятельности, среди которых важнейшее значение имеют умения:

- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;
- осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;
- обеспечивать работоспособность, обнаруживать и устранять неисправности;
- устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять средства гарантированного уничтожения информации;
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.

ВКР должна:

- носить творческий характер с использованием актуальных статистических данных и действующих нормативных правовых актов;
- отвечать требованиям логичного и четкого изложения материала, доказательности и достоверности фактов;
- отражать умение обучающегося пользоваться рациональными приемами поиска, отбора, обработки и систематизации информации, способности работать с нормативно-правовыми актами;
- быть правильно оформлена (четкая структура, завершенность, правильное оформление библиографических ссылок, списка литературы и нормативных правовых актов, аккуратность исполнения).

Выпускная квалификационная работа может быть логическим продолжением курсовой работы, идеи и выводы которой реализуются на более высоком теоретическом и практическом

уровне. *Курсовая работа может быть использована в качестве раздела выпускной квалификационной работы.*

Данные методические рекомендации помогут обучающемуся избежать характерных ошибок в процессе написания ВКР. Если при выполнении работы возникают не учтенные в рекомендациях нюансы, они должны решаться обучающимся и руководителем ВКР в индивидуальном порядке.

## 2. ПОРЯДОК ВЫПОЛНЕНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Выпускная квалификационная работа выполняется на заключительном этапе обучения в виде дипломной работы. Это самостоятельное исследование по одной из актуальных тем сферы эксплуатации и обслуживания электрического и электромеханического оборудования.

Весь период подготовки и оформления ВКР делится на этапы:

1. Получение задания на выполнение дипломной работы с указанием календарного графика работы над ВКР.
2. Составление и согласование рабочего плана к выполнению ВКР.
3. Поиск и изучение источников литературы, а также выполнение исследований по теме.
4. Написание разделов дипломной работы.
5. Оформление дополнительных материалов по ВКР.
6. Подготовка презентационного материала.
7. Подготовка к защите ВКР.
8. Защита ВКР.

Последовательное описание основных этапов выполнения ВКР указано в «Общих методических рекомендациях по выполнению дипломной работы (проекта) по специальностям среднего профессионального образования» <https://cmp2014.ru/wp-content/uploads/2021/10/Obshhie-metodicheskie-ukazaniya-po-VKR-SPO-PPSSZ.pdf>.

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ВКР

### 3.1. Структура дипломной работы (проекта):

- титульный лист;
- задание;
- содержание;
- введение;
- глава 1 Теоретическая часть (10-20 с.);
- глава 2 Экономическая часть (10-15 с.);
- заключение (3-5 с.)
- список использованных источников;
- приложения.

Образцы написания введения, заключения и главы 1 Теоретическая часть - размещены в Приложениях № 1, № 2, № 3 настоящих методических рекомендаций.

Последовательное описание структуры ВКР и макеты оформления: календарного плана выполнения дипломной работы (проекта), задания на дипломную работу (проект), отзыва на дипломную работу (проект), рецензии указаны в «Общих методических рекомендациях по выполнению дипломной работы (проекта) по специальностям среднего профессионального образования» <https://cmp2014.ru/wp-content/uploads/2021/10/Obshhie-metodicheskie-ukazaniya-po-VKR-SPO-PPSSZ.pdf>

#### 4. ПЕРЕЧЕНЬ РЕЗУЛЬТАТОВ, ДЕМОНИСТРИРУЕМЫХ НА ГИА

**Перечень результатов, демонстрируемых на ГИА (защита выпускной квалификационной работы) для специальности 13.02.11. Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям):**

Оцениваемые основные виды деятельности и компетенции по ним	Описание выполняемых в ходе процедур ГИА на защите ВКР (примерная тематика дипломных работ)
<b>Защита дипломной работы</b>	
<p>ВД 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении:</p> <p>ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.</p> <p>ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.</p>	<p><b>Примерная тематика дипломной работы:</b></p> <p>Разработка политики информационной безопасности компании</p> <p>Обеспечение информационной безопасности в коммерческой организации</p> <p>Модернизация существующей системы с целью повышения информационной безопасности</p> <p>Автоматизация и обеспечение информационной безопасности рабочего места менеджера по работе с клиентами фирмы</p> <p>Разработка и обеспечение информационной безопасности автоматизированного рабочего места секретаря</p> <p>Организация защиты персональных данных в условиях реализации вирусных атак</p> <p>Комплексная автоматизированная система учета конфиденциальных документов на предприятии</p> <p>Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux</p> <p>Обеспечение безопасности баз данных информационно-аналитических подразделений организации</p> <p>Методы защиты информационных ресурсов,</p>

<p>ВД 2. Защита информации в автоматизированных системах программными и программно-аппаратными средствами:</p> <p>ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.</p> <p>ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.</p> <p>ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.</p> <p>ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.</p> <p>ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.</p> <p>ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</p>	<p>реализуемые при проведении дистанционного образования</p> <p>Организация защиты персональных данных в организации</p> <p>Проектирование и внедрение системы контроля и управления доступом в компании</p> <p>Обеспечение целостности и сохранности базы данных корпоративной сети</p> <p>Методика обеспечения информационной безопасности при использовании облачных сервисов</p> <p>Защита от DDOS-атак</p> <p>Защита информации предприятия на уровне электронной почты</p> <p>Обеспечение информационной безопасности мобильных автоматизированных рабочих мест</p> <p>Внедрение комплексной системы информационной безопасности в компании</p> <p>Информационная безопасность компьютерной системы при реализации угроз несанкционированного доступа</p> <p>Модернизация системы защиты информационно-телекоммуникационных сетей</p> <p>Исследование не криптографического метода сокрытия потоковой видеоинформации</p> <p>Разработка комплекса мероприятий информационной безопасности и защиты информации в подразделениях государственного учреждения</p> <p>Комплексная система организации безопасного удаленного доступа к ЛВС предприятия</p> <p>Разработка предложений по применению криптографических методов защиты информации в системах электронного документооборота</p> <p>Разработка защищенного интернет-сайта организации</p> <p>Разработка предложений по проведению аудита информационной безопасности образовательного учреждения</p> <p>Разработка проекта по созданию защищенной корпоративной сети с применением технологий VPN</p> <p>Разработка типового проекта защиты локальной вычислительной сети предприятия</p> <p>Разработка системы защиты интеллектуальной собственности, записанной на отчуждаемых электронных носителях</p> <p>Исследование тенденций развития межсетевых экранов нового поколения</p> <p>Разработка телевизионной системы наблюдения охраны объектов</p> <p>Разработка проекта инженерно-технической защиты информации</p> <p>Разработка комплекса рекомендаций по технической защите конфиденциальной информации на автоматизированных рабочих местах</p> <p>Оценка защищенности помещения хозяйствующего субъекта от утечки речевой конфиденциальной информации по акустическому и</p>
<p>ВД 3. Защита информации техническими средствами:</p> <p>ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.</p> <p>ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.</p> <p>ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.</p>	

	<p>виброакустическому каналам</p> <p>Оценка защищенности помещения хозяйствующего субъекта от утечки речевой информации по каналам электроакустических преобразований</p> <p>Оценка защищенности технических средств и систем хозяйствующего субъекта, предназначенных для обработки конфиденциальной информации от утечки по линиям связи</p> <p>Оценка защищенности конфиденциальной информации хозяйствующего субъекта от утечки за счет наводок на технические средства, системы и их коммуникации линиям связи</p> <p>Комплексная оценка защищенности помещения хозяйствующего субъекта от утечки конфиденциальной информации по техническим каналам</p> <p>Оценка защищенности конфиденциальной информации хозяйствующего субъекта от утечки за счет побочных электромагнитных излучений и наводок при использовании электронно-вычислительной техники</p> <p>Разработка комплекса мероприятий по обнаружению и поиску устройств для несанкционированного съема информации по радиоканалу в защищаемом помещении хозяйствующего субъекта</p> <p>Разработка комплекса мероприятий по обнаружению и поиску временно отключенных устройств несанкционированного съема информации в защищаемом помещении хозяйствующего субъекта</p> <p>Разработка комплекса мероприятий по обнаружению и поиску устройств несанкционированного съема информации в защищаемом помещении хозяйствующего субъекта</p> <p>Организация и методика проведения радиомониторинга защищаемого помещения</p>
--	---



**ОБРАЗЕЦ НАПИСАНИЯ ВВЕДЕНИЯ**

Потребность в защите информации в современном Российском обществе существует не только у предприятий крупного и среднего бизнеса, но и у малого бизнеса. Регулярное появление новых угроз требует постоянного совершенствования защищённости любой организации, ведь в противном случае при реализации угрозы предприятию может быть нанесён непоправимый ущерб. Возможности малого бизнеса зачастую не позволяют организовать работу специальных служб, обеспечивающих информационную безопасность организации, осуществляющих выявление, предупреждение и устранение возникающих в ней угроз.

Малый бизнес является одним из наименее защищенных от угроз информационной безопасности в силу ряда причин:

1. Высокая стоимость средств защиты информации;
2. Потребность в привлечении сторонних квалифицированных специалистов в области ЗИ;
3. Недостаточное методическое обеспечение деятельности по разработке КСЗИ.

Актуальность данной работы заключается в создании комплексной системы защиты информации в ООО “....”.

Объектом выпускной квалификационной работы является компьютерная фирма ООО “...”, занимающаяся продажей компьютеров и оргтехники для корпоративных клиентов и государственных структур.

Предметом выпускной квалификационной работы является КСЗИ.

Целью ВКР является создание комплексной системы мер по защите информации, составляющей коммерческую тайну ООО “...”.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Проанализировать информационную систему ООО “...” с точки зрения информационной безопасности;
2. Определить объекты защиты и привести теоретическое обоснование рекомендуемых средств защиты информации;
3. Разработать проект комплексной системы защиты информации ООО “...”;
4. Дать оценку экономической целесообразности реализации проекта КСЗИ в ООО “...”.

**ОБРАЗЕЦ НАПИСАНИЯ ЗАКЛЮЧЕНИЯ**

В ходе выполнения ВКР был произведен анализ существующих мер по защите информации на предприятии ООО "...". В результате этого были выявлены угрозы, которые требуют устранения. На основании этого была разработана работа КСЗИ ООО "...". Данная работа, включает в себя мероприятия, благодаря которым возможно устранение угроз и уязвимостей в данной организации. В процессе выполнения данной ВКР, было произведено обследование, которое включает в себя:

1. Разработку паспорта предприятия с точки зрения информационной безопасности – выявлена общая структура организации, информационная среда предприятия, программно - аппаратные средства, виды деятельности, виды защищаемой информации, конкуренты, описана строительная инфраструктура здания, определена контролируемая зона защищаемого помещения и объектов защиты информации, на которых обрабатывается информация ограниченного доступа.
2. Разработку модели деятельности предприятия – выявлены базовые бизнес – процессы, определены информационные потоки и информация ограниченного доступа циркулирующая на предприятии.
3. Описание информационной системы предприятия – выявлены характеристики АРМ, сервера и программное обеспечение, установленное на них, а также периферийные устройства.
4. Выявление объектов защиты – были выявлены объекты защиты, в которых обрабатывается и циркулирует информация ограниченного доступа.
5. Разработку модели угроз и уязвимостей для важных объектов защиты и расчет рисков для них – установлены угрозы и уязвимости для важных объектов защиты и вероятность их реализации, а также рассчитаны риски по выбранной методике ФСТЭК.

В результате установленной информации было разработано техническое задание на создание КСЗИ ООО "...".

Были выявлены угрозы и уязвимости, с помощью которых может быть разглашена информация ограниченного доступа. В связи с этим, разработаны мероприятия затрудняющие или полностью исключающие реализацию угроз через уязвимости.

Была рассчитана экономическая целесообразность внедрения данной работы, по итогу которой было установлено, что создание КСЗИ в ООО "... " экономически целесообразно.

**ОБРАЗЕЦ НАПИСАНИЯ: глава 1 Теоретическая часть**

**ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

**2.1. Обзор возможных методов устранения уязвимостей**

Важным этапом работы по созданию комплексной системы защиты информации является определение и анализ имеющихся мер, методов и средств, направленных на устранение выявленных у объектов защиты угроз и уязвимостей. На данном этапе работы необходимо определить наиболее эффективные пути решения поставленных задач.

**2.2. Угрозы связанные с нарушением свойства информации**

**2.2.1. Разглашение, копирование, хищение информации ограниченного доступа.** Данный тип угрозы реализуется посредством акустического, оптического и материального каналов утечки информации. Уязвимости, приводящие к возможной реализации данной угрозы:

1. Нарушение соглашения о неразглашении коммерческой тайны;
2. Несанкционированное проникновение в помещение;
3. Отсутствие режима коммерческой тайны.

Установленные уязвимости возможно устранить благодаря разработке организационно-распорядительной документации, включающей в себя: положение о режиме коммерческой тайны, перечень сведений составляющих коммерческую тайну, приказы об их утверждении. Для наилучшей эффективности устранения данных уязвимостей, необходимо провести беседу с сотрудниками организации, работающими с информацией ограниченного доступа с целью доведения требований по работе с ней и ответственности за её разглашение.

**2.2.2. Уничтожение, модификация, блокировка носителей информации, АРМ сотрудников, серверного оборудования**

К данному типу угроз относятся следующие уязвимости:

1. Несанкционированное проникновение в помещение;
2. Отсутствие мероприятий по повышению информационной грамотности;
3. Отсутствие инструкции по работе с АРМ и серверным оборудованием обрабатывающим коммерческую тайну;
4. Отсутствие учета носителей содержащих коммерческую тайну;
5. Отсутствие пломбирования корпуса АРМ.

В качестве решения по устранению данных уязвимостей, необходимо выполнение ряда мероприятий. Во первых, необходимо установить средство контроля и управления доступом. Данное средство позволит организовать пропускной режим, благодаря которому ограничим доступ сотрудникам не имеющим доступ к защищаемой информации. Во вторых, необходимо через определённый промежуток времени проводить мероприятия по повышению информационной грамотности. Проводимые мероприятия позволят улучшить владение приемами поиска, сбора, обработки, анализа и синтеза необходимой информации. В третьих, необходима инструкция по работе с АРМ и серверным оборудованием. В рамках данной дипломной работы, разработка данной инструкции не требуется. В четвёртых, нанести на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя такой информации. Учет носителей позволит в любое время определить, у кого находится тот или иной документ, содержащий информацию ограниченного доступа. В пятых, произвести опломбировку системных блоков АРМ сотрудников и сервера, а так же назначение ответственного за сохранность пломб. Данный способ позволит исключить физическое несанкционированное взаимодействие с носителями, содержащими коммерческую тайну.

**2.3. Угрозы, связанные с НСД**

В связи со стремительным развитием информационных технологий, большое количество организаций занимается обработкой информации ограниченного доступа в рамках своей информационной системы. В результате, в условиях высокой конкурентности, возрастает интерес сторонних компаний к информации ограниченного доступа своих конкурентов.

Несанкционированный доступ, служит одним из методов для получения сторонними организациями информации ограниченного доступа.

Несанкционированный доступ представляет собой противоправное действие, в результате которого злоумышленник получает доступ к защищаемой информации для сторонних лиц. На основании обследования, в рамках данной ВКР были установлены следующие угрозы, связанные с несанкционированным доступом:

1. Несанкционированный доступ к АРМ сотрудников;
2. Угрозы несанкционированного доступа по каналам связи.
- 2.3.1. Несанкционированный доступ к АРМ сотрудников

Угроза несанкционированного доступа к АРМ сотрудников может быть реализована посредством следующих уязвимостей:

1. Отсутствие пломбирования корпуса АРМ;
2. Отсутствие регламента доступа к АРМ;
3. Отсутствие видеонаблюдения;
4. Отсутствие средств защиты от НСД.

Способ устранения первой уязвимости представлен в пункте 2.3. В качестве решения второй проблемы можно разработать матрицу доступа, в которой будет содержаться список лиц, допущенных к АРМ на которых обрабатывается информация ограниченного доступа. В рамках данной ВКР, разработка матрицы доступа не требуется. Третью уязвимость можно устранить посредством внедрения на объекте видеонаблюдения. Видеонаблюдение предназначено для контроля сотрудников, имеющих доступ к информации ограниченного доступа, а также для выявления несанкционированного проникновения в помещение с конфиденциальной информацией. Для устранения четвертой проблемы необходимо установить специальное программно-аппаратное средство защиты информации. Для этого необходимо сравнить сертифицированные СЗИ от НСД.

Таблица № – Сравнение средств защиты от НСД

Критерии сравнения	Secret Net 7	Dallas Lock 8.0 – К	Страж NT 4.0	СЗИ Аура 1.2.4
--------------------	--------------	---------------------	--------------	----------------

Таким образом, на основании данного анализа СЗИ от НСД было выбрано СЗИ "Аура 1.2.4". Данный выбор был связан с низкой стоимостью продукта и удовлетворением функциональными возможностями продукта. СЗИ "Аура 1.2.4" позволяет обеспечить идентификацию и аутентификацию автоматизированных рабочих мест сотрудников, а также разграничить доступ к устройствам и защищаемой информации, путем применения политики доступа. Скриншоты настроек представлены в приложении №.

### 2.3.2. Угрозы несанкционированного доступа по каналам связи.

У данного вида угрозы выявлены следующие уязвимости:

1. Анализ сетевого трафика;
2. Сканирование сети;
3. Выявление паролей;
4. Получение НСД путем подмены доверенного объекта;
5. Отказ в обслуживании.

Первые две проблемы связанными с анализом сетевого трафика и сканированием сети имеют малую вероятность реализации. Это связано с тем что в организации установлен

антивирус включающий в себя защиту от данных уязвимостей. Таким образом, в рамках ВКР устранение данных уязвимостей не требуется. Проблему связанной с выявлением паролей можно устранить путем реализации одноразовых паролей. Данный способ является эффективным от подсматривания паролей другими сотрудниками. Четвёртая уязвимость может быть ликвидирована путём грамотной настройки управлением доступа. Уязвимость типа отказа в обслуживании могут сделать сеть организации недоступной. Таким образом во избежание этого необходимо настроить виртуальную внутреннюю сеть, позволяющей ликвидировать выявленную уязвимость.

#### Выводы по второй главе

На основании выявленных угроз информационной безопасности в организации ООО "...", в рамках ВКР, был разработан комплекс мероприятий, направленных на минимизацию вероятности реализации выявленных угроз:

1. От угрозы, связанной с разглашением, копированием, хищением информации ограниченного доступа: разработка организационно-распорядительной документации по защите информации, составляющей коммерческую тайну в организации; проведение беседы с сотрудниками организации для ознакомления под расписку с требованиями по работе с защищаемой информацией.

2. От угрозы, связанной с уничтожением, модификацией, блокировкой, хищением носителей информации, АРМ сотрудников, серверного оборудования: установка средства контроля управлением доступа; проведение мероприятий по повышению информационной грамотности персонала; разработка инструкции по работе с АРМ и серверным оборудованием; нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна"; опломбировка системных блоков автоматизированных рабочих мест сотрудников и сервера, а так же назначение ответственного за их сохранность.

3. От угрозы, связанной с несанкционированным доступом к АРМ сотрудников: разработка матрицы доступа; внедрение в организации видеонаблюдения; установка СЗИ от НСД " Аура 1.2.4";

4. От угрозы, связанной с несанкционированным доступом по каналам связи: использование одноразовых паролей; настройка управления доступом; настройка виртуальной внутренней сети организации.

Результаты теоретического обоснования выбора средств защиты для реализации КСЗИ ООО "...", легли в основу разработки ВКР.