|  |  |
| --- | --- |
| C:\Users\T'rain\Desktop\логотип 2016 УКРТБдля документов.jpg | МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БАШКОРТОСТАНГосударственное бюджетное профессиональное образовательное учреждениеУфимский колледж радиоэлектроники, телекоммуникаций и безопасности |

|  |  |
| --- | --- |
| СОГЛАСОВАНОПредседатель ГАК\_\_\_\_\_\_\_\_\_\_\_\_ Р.А.Валеев«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. | УТВЕРЖДАЮ Директор ГБПОУ УКРТБ\_\_\_\_\_\_\_\_\_\_\_\_ И.В. Нуйкин«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

**ПРОГРАММА ГОСУДАРСТВЕННОЙ (ИТОГОВОЙ) АТТЕСТАЦИИ ВЫПУСКНИКОВ УКРТБ
ПО СПЕЦИАЛЬНОСТИ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

|  |  |  |
| --- | --- | --- |
| 10.02.02 |  | Информационная безопасность телекоммуникационных систем |
| *код* |  | *наименование специальности* |

**Уровень подготовки:** базовой

|  |  |
| --- | --- |
|  | СОГЛАСОВАНОЗам.директора ГБПОУ УКРТБ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л.Р. ТуктароваЗав. кафедрой компьютерных систем и комплексов и информационной безопасности\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.Г. Хакимова |

Уфа

2019 год

**Содержание**

|  |  |
| --- | --- |
| 1. Паспорт программы государственной итоговой аттестации………… | 3 |
| 2. Структура и содержание государственной итоговой аттестации……. | 8 |
| 3. Условия реализации государственной итоговой аттестации………… | 9 |
| 4. Контроль и оценка результатов государственной итоговой аттестации…………………………………………………………………… | 10 |
| Приложение 1……………………………………………………………….. | 13 |

**1. ПАСПОРТ ПРОГРАММЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**1.1. Область применения программы ГИА**

Программа государственной итоговой аттестации (далее – ГИА) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности:

|  |  |  |
| --- | --- | --- |
| 10.02.02 |  | Информационная безопасность телекоммуникационных систем (базовой подготовки) |
| *код* |  | *наименование специальности* |

в части освоения видов профессиональной деятельности:

ВПД 1. Техническое обслуживание оборудования защищенных телекоммуникационных систем.

ВПД 2. Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем.

ВПД 3. Участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем

ВПД 4 Выполнение работ по профессии "Оператор электронных вычислительных машин"

**1.2. Цели и задачи государственной итоговой аттестации**

Целью государственной итоговой аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, Федеральному государственному образовательному стандарту среднего профессионального образования. ГИА призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определить уровень подготовки выпускника к самостоятельной работе.

**1.3. Количество часов, отводимое на государственную итоговую аттестацию**

Всего –6 недель, в том числе:

выполнение выпускной квалификации работы –4 недели,

защита выпускной квалификационной работы – 2 недели.

**1.4 Требования к уровню подготовки выпускника по профессиональной образовательной программе базовой подготовки**

1.4.1 Иметь практический опыт

- эксплуатации оборудования защищенных телекоммуникационных систем;

- диагностики составных частей защищенных телекоммуникационных систем;

- работы с технической документацией;

- применения инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;

- применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;

- организационного и правового обеспечения информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;

-выполнение требований техники безопасности при работе с вычислительной техникой;

организация рабочего места оператора электронно-вычислительных и вычислительных машин;

- подготовка оборудования компьютерной системы к работе;

-инсталляция, настройка и обслуживание программного обеспечения компьютерной системы;

-управление файлами;

-применение офисного программного обеспечения в соответствии с прикладной задачей;

-использование ресурсов локальной вычислительной сети;

-использование ресурсов, технологий и сервисов Интернет;

-применение средств защиты информации в компьютерной системе.

1.4.2 Уметь

- осуществлять техническую эксплуатацию линейных сооружений связи;

- производить монтаж кабельных линий и оконечных кабельных устройств;

- настраивать, эксплуатировать и обслуживать локальные вычислительные сети;

- сопрягать между собой различные телекоммуникационные устройства;

- производить настройку программного обеспечения коммутационного оборудования защищенных телекоммуникационных систем;

- осуществлять настройку модемов, использующихся в защищенных телекоммуникационных системах;

- производить испытания, проверку и приемку оборудования защищенных телекоммуникационных систем;

- проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры;

- оформлять эксплуатационную и ремонтную документацию;

- выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;

- определять рациональные методы и средства защиты на объектах и оценивать их эффективность;

- проводить типовые операции настройки средств защиты операционных систем;

- применять технические методы и средства защиты информации на выделенных объектах;

- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов;

- организовывать безопасный доступ к информационным ресурсам информационно-телекоммуникационной системы;

- производить установку и настройку типовых программно-аппаратных средств защиты информации;

- пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;

- осуществлять установку, настройку и обслуживание технических средств защиты информации и средств охраны объектов;

- решать частные технические задачи при аттестации объектов, помещений, технических средств;

- обнаруживать и обезвреживать разрушающие программные воздействия с использованием программных средств;

- осуществлять настройку, регулировку и ремонт оборудования средств защиты;

- применять нормативные правовые акты и нормативные методические документы в области защиты информации;

- выявлять каналы утечки информации на объекте защиты;

- контролировать соблюдение персоналом требований режима защиты информации;

- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

- защищать свои права в соответствии с трудовым законодательством;

- выполнять требования техники безопасности при работе с вычислительной техникой;

- производить подключение блоков персонального компьютера и периферийных устройств;

- производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники;

- диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;

- выполнять инсталляцию системного и прикладного программного обеспечения;

- создавать и управлять содержимым документов с помощью текстовых процессоров;

- создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;

- создавать и управлять содержимым презентаций с помощью редакторов презентаций;

- использовать мультимедиа проектор для демонстрации презентаций;

- вводить, редактировать и удалять записи в базе данных;

- эффективно пользоваться запросами базы данных;

 - создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;

- производить сканирование документов и их распознавание;

- производить распечатку, копирование и тиражирование документов на принтере и других устройствах;

- управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;

- осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера;

- осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;

- осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;

- осуществлять резервное копирование и восстановление данных.

1.4.3 Знать

- принципы передачи информации в системах электросвязи;

- принцип модуляции;

- временные и спектральные характеристики модулированных сигналов и периодической последовательности импульсов; принципы аналого-цифрового преобразования, работы компандера, кодера и декодера;

- свойства электромагнитных волн;

- принципы факсимильной передачи сообщений;

-виды помех, методы их подавления;

- разновидности проводных линий передачи;

- конструкцию и характеристики электрических и оптических кабелей связи;

- способы коммутации в сетях связи; принципы построения многоканальных систем передачи;

- принципы помехоустойчивого кодирования;

- основные принципы синхронизации цифровых потоков;

- основы маршрутизации в сетях передачи данных;

- особенности построения и составные элементы сетей передачи данных;

- принципы построения сетей радиосвязи с подвижными элементами и их классификацию;

- типовые услуги цифровых систем связи, информационного обслуживания, предоставляемые пользователям;

- принципы построения и технические средства локальных сетей;

- принципы функционирования маршрутизаторов;

- модемы, использующиеся в защищенных телекоммуникационных системах, принципы функционирования и подключения;

- спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения;

- принципы организации технической эксплуатации защищенных телекоммуникационных систем;

- методы организации и технологию ремонта оборудования защищенных телекоммуникационных систем;

- периодичность поверок контрольно-измерительной аппаратуры;

- принцип действия выпрямителей переменного тока;

- принципы работы стабилизаторов напряжения и тока, импульсных источников питания;

- принципы защиты электронных устройств от недопустимых режимов работы;

- основные положения системного подхода к технической защите информации;

-основные технические каналы утечки защищаемой информации в автоматизированных и телекоммуникационных системах, физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности;

- порядок проведения работ по технической защите информации объекта;

- типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;

- основные протоколы идентификации и аутентификации в телекоммуникационных системах;

- состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;

- особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;

- основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;

- основные понятия криптографии и типовые криптографические методы защиты информации;

- основные технические методы и средства защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам, средства охраны и безопасности объектов;

- назначение, принципы работы и правила эксплуатации технических средств и систем, аппаратуры контроля, защиты и другого оборудования, используемого при проведении работ по защите информации;

- правила применения, эксплуатации и обслуживания технических средств защиты информации;

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

- правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;

- организацию ремонтного обслуживания аппаратуры и средств защиты информации;

- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организациях;

- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность).

- требования техники безопасности при работе с вычислительной техникой;

-основные принципы устройства и работы компьютерных систем и периферийных устройств;

- классификацию и назначение компьютерных сетей;

- виды носителей информации;

- программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета;

- основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

1.4.4 В результате освоения основной образовательной программы техник по защите информации должен обладать общими компетенциями, включающими в себя способность:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Формулировать задачи логического характера и применять средства математической логики для их решения.

ОК 11. Понимать физическую сущность задач, возникающих в ходе профессиональной деятельности, и применять соответствующий физический аппарат для их решения.

ОК 12. Использовать вычислительную технику и прикладные программные пакеты для решения профессиональных задач.

ОК 13. Ориентироваться в элементной базе устройств телекоммуникационных систем и обеспечения их информационной безопасности.

1.4.5 Техник по защите информации должен обладать профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

ПК 1.1. Устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем.

ПК 1.2. Эксплуатировать оборудование защищенных телекоммуникационных систем.

ПК 1.3. Осуществлять техническое обслуживание, диагностирование, устранение отказов, настройку и ремонт оборудования, проводить его аттестацию.

ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации телекоммуникационных систем и средств защиты информации в них.

ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.

ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению.

ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.

ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей.

ПК 3.1. Руководствоваться законодательными и иными нормативными правовыми актами в области обеспечения информационной безопасности телекоммуникационных систем, защиты государственной тайны и конфиденциальной информации.

ПК 3.2. Участвовать в подготовке и проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации.

ПК 3.3. Участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств.

ПК 4.1 Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения.

ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах.

ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета.

ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе.

**2. СТРУКТУРА И СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**2.1. Форма и сроки проведения государственной итоговой аттестации**

Форма проведения ГИА: защита выпускной квалификационной работы (ВКР).

Объем времени и сроки, отводимые на выполнение выпускной квалификационной работы: 4 недели, май, июнь.

Сроки защиты выпускной квалификационной работы: 2 недели, июнь.

**2.2. Содержание государственной итоговой аттестации**

Темы ВКР должны иметь практико-ориентированный характер и должны соответствовать содержанию одного или нескольких профессиональных модулей ПМ.01. «Техническое обслуживание оборудования защищенных телекоммуникационных систем», ПМ.02. «Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем», ПМ.03. «Участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем», ПМ. 04 «Выполнение работ по профессии «Оператор электронных вычислительных машин»» специальности 10.02.02 «Информационная безопасность телекоммуникационных систем».

Темы выпускных квалификационных работ с указанием руководителя закрепляются за студентом приказом директора колледжа.

Примерная тематика выпускных квалификационных работ представлена в приложении 1.

**2.3 Требования к выпускной квалификационной работе.**

Структура ВКР:

- титульный лист;

- индивидуальный график выполнения ВКР;

- задание на ВКР;

- отзыв руководителя ВКР;

- внешняя рецензия;

- пояснительная записка:

- введение с обоснованием актуальности и практической значимости выбранной темы;

- общая часть;

- специальная часть;

- заключение;

- список литературы;

- приложения;

- графическая часть;

- изготовление макета, стенда, разработанный программный продукт и т.п.

Объем ВКР должен быть не меньше 40 страниц машинописного текста.

Требования к содержанию разделов выпускной квалификационной работы описаны в Методических указаниях по выполнению выпускной квалификационной работы.

Требования по оформлению выпускной квалификационной работы описаны в методических рекомендациях по оформлению выпускных квалификационных работ.

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**3.1.Требования к информационно-методическому обеспечению**

- Федеральный Государственный образовательный стандарт специальности;

- программа Государственной (итоговой) аттестации;

- приказ директора о создании Государственной аттестационной комиссии для проведения ГИА;

- приказ директора о допуске студентов к Государственной (итоговой) аттестации;

- сведения об успеваемости студентов за весь период обучения;

- зачетные книжки студентов;

- книга протоколов заседаний ГАК;

- приказ о закреплении за выпускниками тем выпускных квалификационных работ;

- литература по специальности, ГОСТ, справочники.

**3.2 Условия подготовки и процедура проведения защиты выпускной квалификационной работы**

3.2.1 Условия подготовки выпускной квалификационной работы:

К Государственной (итоговой) аттестации допускается студент, не имеющий академической задолженности и в полном объеме выполнивший учебный план по осваиваемой образовательной программе среднего профессионального образования.

После утверждения темы руководителями ВКР разрабатываются индивидуальные задания (к каждому из руководителей прикрепляется не более 8 студентов). Индивидуальные задания рассматриваются кафедрами и утверждаются заместителем директора УКРТБ.

Индивидуальные задания на ВКР выдаются студентам за 2 недели до начала преддипломной практики.

Общее руководство и контроль за ходом выполнения ВКР осуществляется заместителем директора УКРТБ, заведующими отделениями, заведующим кафедрой в соответствии с должностными обязанностями.

3.2.2 Защита ВКР

Допуск к защите ВКР оформляется приказом директора колледжа.

Защита ВКР проводится на открытом заседании Государственной экзаменационной комиссии

На защиту ВКР отводится 45 минут. Процедура защиты:

- доклад студента 10-15 минут;

- чтение отзыва и рецензии (не более 5 минут);

- вопросы членов ГАК и ответы студента (не более 15 минут);

- по желанию (необходимости) выступление руководителя ВКР и рецензента (если они присутствуют на заседании ГАК) с целью защиты, согласия или несогласия с оценкой конкретной ВКР (не более 15 минут).

Заседание ГАК протоколируется. В протоколе записываются:

- итоговая оценка ВКР;

- присуждение квалификации;

- особое мнение членов комиссии.

**4. ОЦЕНКА РЕЗУЛЬТАТОВ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**4.1 Критерии оценки выпускной квалификационной работы**

- соответствие названия работы ее содержанию, четкая целевая направленность;

- логическая последовательность изложения материала;

- необходимая глубина исследования и убедительность аргументации;

- конкретность представления практических результатов работы;

- соответствие оформления выпускной квалификационной работы требованиям ГОСТ Р 705 -2008 и методическим рекомендациям по оформлению выпускных квалификационных работ.

**4.2 Критерии оценки защиты выпускной квалификационной работы**

- четкость и грамотность доклада;

- четкость, внятность, глубина ответов на вопросы присутствующих на заседании ГАК;

- использование технических средств для сопровождения доклада.

**4.3 Определение окончательной оценки**

При определении окончательной оценки за защиту дипломного проекта (работы) учитываются:

- доклад выпускника по каждому разделу выпускной работы;

- ответы на вопросы;

- оценка рецензента;

- отзыв руководителя.

«Отлично» выставляется за следующую выпускную квалификационную работу:

- работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, глубокий анализ проблемы, характеризуется логичным, последовательным изложением материала с соответствующими выводами и обоснованными предложениями;

- имеет положительные отзывы руководителя и рецензента;

- при защите работы студент показывает глубокие знания вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, во время доклада использует презентацию и наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, легко отвечает на поставленные вопросы.

«Хорошо» выставляется за следующую выпускную квалификационную работу:

- работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, достаточно подробный анализ проблемы, характеризуется последовательным изложением материала с соответствующими выводами, однако с не вполне обоснованными предложениями;

- имеет положительный отзыв руководителя и рецензента;

- при защите студент показывает знания вопросов темы, оперирует данными исследования, вносит предложения, во время доклада использует презентацию и наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, без особых затруднений отвечает на поставленные вопросы.

«Удовлетворительно» выставляется за следующую выпускную квалификационную работу:

- носит исследовательский характер, содержит теоретическую главу, базируется на практическом материале, но отличается поверхностным анализом проблемы, в ней просматривается непоследовательность изложения материала, представлены необоснованные предложения;

- в отзывах руководителя и рецензента имеются замечания по содержанию работы и методике анализа;

- при защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полного, аргументированного ответа на заданные вопросы.

«Неудовлетворительно» выставляется за следующую выпускную квалификационную работу:

- не носит исследовательского характера, не содержит анализа проблемы, не отвечает требованиям, изложенным в методических указаниях;

- не имеет выводов либо они носят декларативный характер;

- в отзывах руководителя и рецензента имеются существенные критические замечания;

- при защите студент затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки, к защите не подготовлены презентация, наглядные пособия или раздаточный материал.

Общая оценка защиты выставляется на закрытом заседании ГАК простым большинством голосов членов ГАК. При равенстве голосов, решение принимает председатель ГАК.

Студенты, выполнившие выпускную квалификационную работу, но получившие при защите оценку «неудовлетворительно», имеют право на повторную защиту (не ранее, чем через 6 месяцев после прохождения ГИА впервые).

По результатам защиты составляется отчет о защите выпускных квалификационных работ за подписью председателя ГАК.

Приложение 1

**Примерная тематика выпускных квалификационных работ**

1. Разработка списков контроля доступа к внешним и внутренним ресурсам организации.

2. Разработка системы контроля и управления доступом.

3. Разработка и построение системы безопасности сети.

4. Разработка корпоративной сети с применением различных технологий.

5. Разработка процессов оптимизации и обеспечение безопасности компьютерной сети организации.

6. Проектирование систем видеонаблюдения.

7. Разработка защищенной локальной вычислительной сети предприятия.

8. Разработка комплексной защиты предприятия.

9. Построение защиты информационных систем персональных данных предприятия.

10. Проектирование систем ОПС.

11. Разработка системы защиты персональных данных на предприятии

12. Модернизация и построение защиты локальной вычислительной сети предприятия.

13 Разработка системы защиты информации от спама.