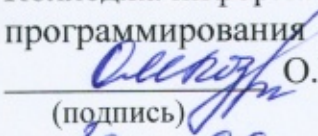


Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Колледж информатики и программирования

УТВЕРЖДАЮ

Заместитель директора
по учебно-практической работе и
стратегическому развитию
Колледжа информатики и
программирования


(подпись) О.М. Козлова
« 30 » 06 20 25 г.

РАБОЧАЯ ПРОГРАММА

производственной практики (преддипломной)
по специальности среднего профессионального образования

**10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем**

ПМ.01 Эксплуатация информационно-телекоммуникационных
систем и сетей

ПМ.02 Защита информации в информационно-
телекоммуникационных системах и сетях с использованием
программных и программно-аппаратных (в том числе,
криптографических) средств защиты

ПМ.03 Защита информации в информационно-
телекоммуникационных системах и сетях с использованием
технических и физических средств защиты

ПМ.04 Выполнение работ по одной или нескольким
профессиям рабочих, должностям служащих

Москва 2025 г.

Рабочая программа производственной практики (преддипломной) разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 Обеспечение информационной безопасности

Организации – партнеры:

ПАО «Ростелеком»; АО «Особое Конструкторское Бюро Систем автоматизированного Проектирования» (АО «ОКБ «САПР»), ООО «РусБИТех-Астра», АО «ИнфоВотч», АО «ИнфоТеКС», АО «Научно-производственное предприятие «САПФИР» (АО «НПП «САПФИР»), АО «НПП «Пульсар», Инспекция ФНС России по г. Москве, МРУ Росфинмониторинга по ЦФО, ПАО "Сбербанк России", Консорциум "Интегра-С".

Разработчики:

Мирецкая Екатерина Алексеевна, старший методист ВКК Колледжа информатики и программирования

Маринич А.Л., преподаватель высшей квалификационной категории Колледжа информатики и программирования.

Рабочая программа производственной практики (преддипломной) рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии информационных систем и программирования
Протокол от «15» мая 2025 г. №9

Председатель предметной
(цикловой)
комиссии

А.Л. Маринич

1. Паспорт рабочей программы производственной практики (преддипломной)

1.1. Область применения рабочей программы

Рабочая программа производственной практики (преддипломной) – является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности в части освоения основных видов деятельности:

- ~ Эксплуатация информационно-телекоммуникационных систем и сетей
- ~ Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты
- ~ Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
- ~ Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

1.2. Цели и задачи производственной практики (преддипломной)

- формирование у студентов практических умений (приобретение практического опыта) в рамках освоения профессиональных модулей по основным видам профессиональной деятельности;

1.3. Требования к результатам освоения производственной практики

В результате прохождения производственной практики по видам профессиональной деятельности студент должен уметь:

Эксплуатация информационно-телекоммуникационных систем и сетей
- осуществлять техническую эксплуатацию линейных сооружений связи; - производить монтаж кабельных линий и оконечных кабельных устройств; - настраивать, эксплуатировать и обслуживать оборудование ИТКС; - осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; - производить испытания, проверку и приемку оборудования телекоммуникационных систем; - проводить работы по техническому обслуживанию, диагностики технического состояния и ремонту оборудования ИТКС; - измерять основные качественные показатели и характеристики при выполнении профилактических и ремонтных работ приемно-передающих устройств (ППУ); - читать принципиальные схемы блоков ППУ; - выполнять расчеты, связанные с определением значений параметров режима и элементов ППУ; - контролировать работу и осуществлять техническую эксплуатацию ППУ; - настраивать, эксплуатировать и обслуживать локальные вычислительные сети; - сопрягать между собой различные телекоммуникационные устройства; - производить настройку программного обеспечения коммутационного оборудования телекоммуникационных систем; - осуществлять настройку модемов, используемых в защищенных телекоммуникационных системах; - проверять функционирование, производить регулировку и контроль основных

параметров источников питания радиоаппаратуры;
проводить типовые измерения;
пользоваться стандартными средствами электрорадиоизмерений;
оценивать точность проводимых измерений;
- оформлять эксплуатационную и ремонтную документацию;

Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

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;
производить установку и настройку типовых программно-аппаратных средств защиты информации;
пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
применять нормативные правовые акты, определяющие требования к обеспечению информационной безопасности объекта критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры, подлежащие защите;
классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте);
определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ;
определять требования к параметрам настройки программных и программно-аппаратных средств, наличия средств защиты информации, обеспечивающих реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации;
оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
участвовать в выборе мер защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры;
принимать участие в выборе программно-аппаратных средств защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов;
участвовать в определении комплекса мер для обеспечения безопасности информационной безопасности в значимых объектах критической информационной инфраструктуры;
выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации
применять нормативные документы по противодействию технической разведке;
планировать политику безопасности программных компонентов значимых объектах критической информационной инфраструктуры

участвовать в разработке политики безопасности информации значимых объектов критической информационной инфраструктуры;
 конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры
 определять параметры настройки программного обеспечения системы защиты информации значимых объектов критической информационной инфраструктуры;
 использовать криптографические методы и средства защиты информации в значимых объектах критической информационной инфраструктуры;
 регистрировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры
 анализировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры;
 использовать программные средства для архивирования информации;
 использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации;
 применять типовые программные средства резервирования и восстановления информации в значимых объектах критической информационной инфраструктуры;
 применять средства обеспечения отказоустойчивости значимых объектов критической информационной инфраструктуры
 определять источники и причины возникновения инцидентов
 оценивать последствия выявленных инцидентов
 обнаруживать нарушения правил разграничения доступа
 устранять нарушения правил разграничения доступа*

Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты

применять технические средства для криптографической защиты информации конфиденциального характера;
 применять технические средства для уничтожения информации и носителей информации;
 применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
 применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
 применять инженерно-технические средства физической защиты объектов информатизации

Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

-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. Количество часов, отводимое на освоение рабочей программы производственной практики (преддипломной):

Всего – 144 часа

2. Результаты освоения производственной практики (преддипломной):

Результатом освоения производственной практики (преддипломной) является сформированность у студентов практических умений в рамках профессиональных модулей по основным видам профессиональной деятельности.

Код	Общие компетенции
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.2. Перечень профессиональных компетенций

Обучающийся должен обладать профессиональными компетенциями, соответствующими основным видам деятельности:

Код	Профессиональные компетенции
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3.	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим

	каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, 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

3. Тематический план и содержание производственной практики (преддипломной)

3.1. Структура производственной практики (преддипломной)

Код и наименование профессиональных модулей	Количество часов по профессиональному модулю	Виды работ	Наименование тем производственной практики (преддипломной)	Количество часов по темам
ПМ.01 ПМ.02 ПМ.03 ПМ.04	144	Ознакомление с целями и задачами практики. Инструктаж по технике безопасности и пожарной безопасности. Составление плана и графика работы на период практики, опираясь на индивидуальное задание производственной практики и учитывая специфику и режим работы организации – места прохождения практики. Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации), вводный инструктаж по технике безопасности и охране труда. Анализ вида, структуры, функций организации. Ознакомление с кабельными цехами и участками. Работа с технической документацией. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий. Ознакомление с оборудованием ИТКС. Изучение и работа с контрольно-измерительным оборудованием. Выполнение обязанностей стажера на закрепленном рабочем месте. Выполнение индивидуального задания по практике: производить монтаж кабельных линий и окончных кабельных устройств ИТКС; Выполнение определенных видов работ и заданий в	Раздел 1 Тема 1. Цели и задачи практики Тема 2. Знакомство с рабочим местом Тема 3. Практическое изучение предмета проектирования Тема 4. Сбор информации для введения дипломной работы (проекта).	144

		соответствии с темой дипломной работы (далее – ДР). Проведение анализа и обобщения научно-технической информации по теме дипломной работы. Описание технико-экономической характеристики предметной области и объекта исследования. Анализ видов и категорий обрабатываемой в информационной (автоматизированной) системе информации. Определение требований по информационной безопасности. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием		
		Участие в организации работ по защите персональных компьютеров на предприятии Участие в организации работ по защите локальных сетей на предприятии Участие в организации работ по защите работ в глобальной сети интернет на предприятии Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных	Раздел 2 Тема 1. Анализ и обобщения научно-технической информации по теме дипломного проекта (работы) Тема 2. Подбор и изучение фактического материала Тема 3. Подготовка плана дипломного проекта (работы). Тема 4. Описание предметной области и объекта исследования и входных параметров задачи Тема 5. Сбор информации для теоретической части дипломного проекта (работы);	

		средств шифрования в соответствии с решаемой задачей Подключение, установка драйверов, настройка программных средств абонентского шифрования Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств РКІ Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием. Подбор фактического материала по теме ДР с учетом профессионального модуля и его изучение		
		Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами Сбор и изучение научно-практического материала по разделам ДР, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ДР. Разработка состава технических и инженерно-технических средств для решения поставленной в ТЗ	Тема 1. Поиск дополнительной информации Тема 2. Практическое изучение средств реализации предмета разработки Тема 3. Сбор информации и подготовка практической части Тема 4. Подготовка заключения, приложений и списка используемых источников и интернет-ресурсов	

		задачи. Расчет параметров утечки информации. Разработка схемы соединений. Оформление пояснительной записки к выпускной квалификационной работе.		
		Анализ собранного материала, оценка перспектив возможности его применения в условиях предприятия, организации – места прохождения практики; подготовка и сдача отчета по практике в соответствии с содержанием тематического плана преддипломной практики, аттестационного листа по форме, установленной данной рабочей программой. Согласование содержания доклада и презентации к защите дипломного проекта с руководителем.	Раздел4 Тема 1. Подготовка доклада и презентации к защите дипломного проекта Тема 2. Подготовка отчета по практике	

3.2. Содержание производственной практики (преддипломной)

Профессиональные модули и междисциплинарных курсы, темы	Содержание практики	Объем в часах
		144
Раздел 1 Тема 1. Цели и задачи практики	Определение ключевых целей производственной преддипломной практики. Формулировка конкретных задач, которые студент должен решить для достижения этих целей в рамках подготовки к диплому.	
Тема 2. Знакомство с рабочим местом	Ознакомление с организацией, структурой подразделения и своим рабочим местом. Изучение правил внутреннего распорядка, техники безопасности и специфики деятельности предприятия.	
Тема 3. Практическое изучение предмета проектирования	Непосредственная работа с реальным объектом или системой, являющейся темой дипломного проекта. Понимание его устройства, принципов работы и актуальных задач на практике.	
Тема 4. Сбор информации для введения дипломной	Поиск и систематизация данных, необходимых для обоснования	

работы (проекта).	актуальности темы, формулировки целей, задач, объекта и предмета исследования во введении диплома.	
Раздел 2 Тема 1. Анализ и обобщения научно-технической информации по теме дипломного проекта (работы) Тема 2. Подбор и изучение фактического материала Тема 3. Подготовка плана дипломного проекта (работы). Тема 4. Описание предметной области и объекта исследования и входных параметров задачи Тема 5. Сбор информации для теоретической части дипломного проекта (работы)	Изучение литературных источников (книги, статьи, патенты, стандарты) по теме проекта. Критический анализ и структурирование полученных знаний для теоретической части. Сбор конкретных данных, спецификаций, чертежей, результатов измерений или эксплуатационных характеристик, относящихся непосредственно к объекту исследования. Их детальное изучение. Разработка структуры дипломной работы (проекта). Определение последовательности глав, разделов и параграфов, логично раскрывающих тему. Четкое определение области знаний, к которой относится проект. Детальное описание исследуемого объекта/системы и исходных данных (входных параметров) для решения поставленной задачи. Поиск и отбор теоретических основ, методик, моделей, алгоритмов, необходимых для научного обоснования выбранного подхода в дипломной работе.	
Раздел 3 Тема 1. Поиск дополнительной информации Тема 2. Практическое изучение средств реализации предмета разработки Тема 3. Сбор информации и подготовка практической части	Актуализация и расширение собранных данных по мере углубления в тему проекта. Поиск недостающих сведений для полноты исследования. Освоение на практике инструментов, технологий, программного обеспечения, оборудования, которые будут использоваться для реализации проектного решения (разработки, модернизации, расчета). Получение данных, необходимых для выполнения расчетов, проектирования, разработки, моделирования или эксперимента. Формирование содержания практического раздела диплома на основе	

Тема 4. Подготовка заключения, приложений и списка используемых источников и интернет-ресурсов	этих данных и проведенной работы. Формулировка выводов по всей работе, оценка достижения целей. Оформление приложений (чертежи, схемы, таблицы, код). Составление библиографического списка использованной литературы и ресурсов.	
Раздел 4 Тема 1. Подготовка доклада и презентации к защите Тема 2. Подготовка отчета по практике	Разработка краткого, структурированного устного выступления (доклада), отражающего суть дипломной работы. Создание наглядной презентации для сопровождения доклада на защите. Систематизация и оформление результатов, полученных за период практики, в соответствии с требованиями. Фиксация выполненных задач, изученных вопросов и приобретенных навыков.	

4. Условия реализации производственной практики (преддипломной)

4.1. Требования к минимальному материально-техническому обеспечению

Производственную практику (преддипломную) обучающиеся проходят в следующих организациях и учреждениях на основе договоров:

ПАО «Ростелеком»; АО «Особое Конструкторское Бюро Систем автоматизированного Проектирования» (АО «ОКБ «САПР»), ООО «РусБИТех-Астра», АО «ИнфоВотч», АО «ИнфоТеКС», АО «Научно-производственное предприятие «САПФИР» (АО «НПП «САПФИР»», АО «НПП «Пульсар», Инспекция ФНС России по г. Москве, МРУ Росфинмониторинга по ЦФО, ПАО "Сбербанк России", Консорциум "Интегра-С".

4.2. Общие требования к организации производственной (преддипломной) практики

Производственная (преддипломная) практика проводится концентрировано

5. Контроль и оценка результатов освоения производственной практики (преддипломной)

Контроль и оценка результатов освоения производственной практики (преддипломной) осуществляется руководителем практики в процессе проведения практики. В результате освоения производственной практики (преддипломной) студенты проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты обучения (освоенные умения в рамках вида профессиональной деятельности)	Формы и методы контроля и оценки
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – 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 – обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения*; – устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами*; – формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;*; – регистрировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктур*; – использовать программные средства для архивирования информации применять типовые программные средства резервирования и восстановления информации в значимых объектах критической информационной*	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, отзыв, дневник прохождения практики)
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации, проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; - оформлять эксплуатационную документацию программно аппаратных средств защиты информации;* - определять цели и задачи в изучении проекта;* -разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты; – осуществлять установку, развёртывание, настройку и использованием DLP-систем.*	
Защита информации техническими средствами	
– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, технических средств защиты акустической речевой информации от утечки по техническим каналам*; – применять инженерно-технические средства физической	

защиты объектов информатизации, – производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов .*	
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих -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.	