МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

КОЛЛЕДЖ ДГУ

ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	*10.02.05 Обеспечение информационной безопасности автоматизированных систем*
Обучение:	
Уровень образования, на базе которого осваивается ППССЗ:	*основное общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

2020

Программа преддипломной практики разработана на основе требований Федерального государственного образовательного стандарта (далее – ФГОС) СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования

Организация-разработчик: Колледж федерального государственного бюджетного образовательного учреждение высшего образования «Дагестанский государственный университет»

Разработчики:

Пирбудагова Д.Ш. - к.ю.н., доцент кафедры конституционного и международного права
Магдилова Л.В. - к.э.н., доцент кафедры информационного права и информатики

Программа преддипломной практики рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин Колледжа ДГУ

Протокол № 7 от «29» февраля 2020 г.

Зав. кафедрой _____ Магдилова Л.В.

Программа преддипломной практики согласована с учебно-методическим управлением

«16» 03 2020 г. _____
подпись)

Программа преддипломной практики согласована с представителем работодателя

1 зам. министра Минсвязи _____ Мочалев Б.А.

СОДЕРЖАНИЕ

1. Паспорт программы преддипломной практики

1.1. Область применения программы преддипломной практики

Преддипломная практика является частью ОПОП ПССЗ по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» в части освоения основных видов профессиональной деятельности: эксплуатация автоматизированных (информационных) систем в защищенном исполнении; защита информации в автоматизированных системах программными и программно-аппаратными средствами; защита информации техническими средствами; выполнение работ по профессии 16199 «Оператор электронно-вычислительных и вычислительных машин»; противодействие отмыванию денег и финансированию терроризма.

Практика направлена на формирование у студента общих компетенций, получение практического опыта по виду профессиональной деятельности, подготовку к осознанному и углубленному изучению отдельных специальных дисциплин. В процессе прохождения практики студент должен собрать и обработать материал, необходимый для написания выпускной квалификационной работы.

1.2. Цели и задачи преддипломной практики, требования к результатам

1.2.1. Цели практики:

- улучшение качества профессиональной подготовки студентов;
- закрепление и систематизация полученных знаний по обеспечению защищенной эксплуатации информационных систем; использованию программно-технических средств защиты;
- овладение профессиональными умениями и навыками по применению организационных, программных, технических и законодательных мер защиты;
- закрепление и углубление теоретических знаний, полученных в процессе обучения;
- формирование у обучающихся нравственных качеств личности;
- повышение мотивации к профессиональному самосовершенствованию, расширение профессионального кругозора;
- приобретение опыта работы в коллективах при решении ситуационных задач; изучение принципов построения систем защиты информации, применяемых на практике, а также приобретение практического опыта их применения; изучение дополнительного материала, публикуемого в периодической печати, с целью актуализации знаний, полученных в процессе обучения.

1.2.2. Задачи практики:

- Получение обучающимися информации о будущей профессиональной деятельности, связанной с защитой информации в автоматизированных системах.
- Ознакомление с информационными ресурсами объекта практики;
- Получение обучающимися навыков работы с программным обеспечением, защищающим информационные системы;
- Ознакомление с технической документацией и аппаратным обеспечением по защите информационных систем;
- Сбор материалов, необходимых для составления отчета о прохождении практики в соответствии с дневником практики.

1.3. Место преддипломной практики в структуре ОПОП ПССЗ

Преддипломная практика согласно ОПОП ПССЗ проводится после прохождения междисциплинарных курсов (МДК) в рамках следующих профессиональных модулей: ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»; ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»; ПМ.03 «Защита информации техническими средствами»; ПМ.04 «Выполнение работ по профессии 16199 «Оператор электронно-

вычислительных и вычислительных машин»»; ПМ.05 «Противодействие отмыванию денег и финансированию терроризма».

1.4. Трудоемкость и сроки проведения практики

Трудоемкость преддипломной практики в рамках освоения профессиональных модулей: ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»; ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»; ПМ.03 «Защита информации техническими средствами»; ПМ.04 «Выполнение работ по профессии 16199 «Оператор электронно-вычислительных и вычислительных машин»»; ПМ.05 «Противодействие отмыванию денег и финансированию терроризма» составляет 144 часа (четыре недели).

Сроки проведения практики определяются рабочим учебным планом по специальности СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и графиком учебного процесса. Практика проводится на 4 курсе, в восьмом семестре.

1.5. Место прохождения преддипломной практики

Практика проводится в организациях: Министерство цифрового развития Республики Дагестан; Государственное автономное учреждение Республики Дагестан «Центр информационных технологий» (ГАУ РД «ЦИТ»); Государственное Бюджетное Учреждение Дополнительного Образования Республики Дагестан «Малая академия наук Республики Дагестан»; Дагестанский филиал ПАО «Ростелеком»; Общество с ограниченной ответственностью "ДАГЕСТАН-ПАРУС".

Преддипломная практика проводится в форме практики по получению первичных профессиональных умений и навыков.

2. Перечень планируемых результатов освоения программы преддипломной практики

Результатом прохождения производственной практики в рамках освоения профессиональных модулей ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»; ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»; ПМ.03 «Защита информации техническими средствами»; ПМ.04 «Выполнение работ по профессии 16199 «Оператор электронно-вычислительных и вычислительных машин»»; ПМ.05 «Противодействие отмыванию денег и финансированию терроризма» является овладение обучающимися видами профессиональной деятельности, в том числе общими (ОК) компетенциями.

Компетенции	Формулировка компетенции из ФГОС	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Знать: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств. Уметь: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в

		защищенном исполнении и компонент систем защиты информации автоматизированных систем. Владеть: навыками установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Знать: теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации. Уметь: организовывать, 6 конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы. Владеть: навыками конфигурирования, настройки компонентов систем защиты информации автоматизированных систем;
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях. Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам. Владеть: навыками эксплуатации компонентов систем защиты информации автоматизированных систем
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Знать: принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации. Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности. Владеть: навыками диагностики компонентов систем защиты информации автоматизированных

		систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации Владеть: установкой, настройкой программных средств защиты информации в автоматизированной системе
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных Уметь: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации Практический опыт: обеспечением защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использованием программных и программно-аппаратных средств для защиты информации в сети
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Знать: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации Уметь: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации Владеть: тестирование функций, диагностика, устранение отказов и восстановление работоспособности

		программных и программно-аппаратных средств защиты информации
ПК 2.4	. Осуществлять обработку, хранение и передачу информации ограниченного доступа	Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации Уметь: 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 Владеть: решением задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применением электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Знать: особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации Уметь: применять средства гарантированного уничтожения информации Владеть: учётом, обработкой, хранением и передачей информации, для которой установлен режим конфиденциальности

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	Знать: порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Владеть: установкой, монтажом и настройкой технических средств защиты информации; техническим обслуживанием технических средств защиты информации; применением основных типов технических средств защиты информации
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии требованиями эксплуатационной документации	Знать: порядок технического обслуживания технических средств защиты информации; Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Владеть: установкой, монтажом и настройкой технических средств защиты информации; техническим обслуживанием технических средств защиты информации; применением основных типов технических средств защиты информации
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Знать: физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах

		информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам Уметь: 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 Владеть: применением основных типов технических средств защиты информации; выявлением технических каналов утечки информации; участием в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановлением работоспособности технических средств защиты информации
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Знать: номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Владеть: проведением измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации

ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Знать: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Владеть: проведением измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявлением технических каналов утечки информации
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации	Знать: основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации Уметь: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации Владеть: установкой, монтажом и настройкой, техническим обслуживанием, диагностикой, устранением отказов и неисправностей, восстановлением работоспособности инженерно-технических средств физической защиты
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Знать: требования техники безопасности при работе с вычислительной техникой; основные принципы устройства и работы компьютерных систем и периферийных устройств (06.033 А/01.5); Уметь: 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; Владеть: техникой безопасности при работе с вычислительной техникой; организацией рабочего места оператора электронно-вычислительных и вычислительных машин (06.032 А/01.5); подготовкой оборудования компьютерной системы к работе; инсталляцией, настройкой и обслуживанием программного обеспечения компьютерной системы (06.032 А/01.5);
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	Знать: классификацию и назначение компьютерных сетей; виды носителей информации; Уметь: выполнять инсталляцию системного и прикладного программного обеспечения (06.032 А/01.5); создавать и управлять содержимым документов с помощью текстовых процессоров; создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; Владеть: офисным программным обеспечением в соответствии с прикладной задачей
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Знать: программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета (06.033 А/01.5); Уметь: 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; Владеть: ресурсами локальной вычислительной сети, технологий и сервисов Интернет
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе	Знать: основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым Уметь: осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ (06.032 А/01.5); осуществлять резервное

		копирование и восстановление данных (06.033 А/03.5); Владеть: средствами защиты информации в компьютерной системе
ПК 5.1.	Использовать нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности в области противодействия отмывания денег и финансированию терроризма, программно-аппаратными средствами.	**Знать:** международные стандарты и институциональные основы международной системы ПОД/ФТ; законодательство Российской Федерации в сфере ПОД/ФТ в том числе про-граммы и процедуры, регламентирующие выполнение требований законодательства в сфере ПОД/ФТ; типологии и схемы отмывания денег; признаки операций, подлежащих обязательному контролю в целях ПОД/ФТ, критерии выявления и признаки необычных сделок, связанных с отмыванием денег или финансированием терроризма, организационные меры по за-щите информации (06.032 А/01.5) программы осуществления внутреннего контроля в целях ПОД/ФТ; структуру государственных органов Российской Федерации, осуществляющих регулирование в сфере ПОД/ФТ, их правовой статус и полномочия, компетенции уполномоченного органа в сфере ПОД/ФТ; требования к оформлению документов и порядок работы с конфиденциальной информацией; порядок предоставления информации в соответствии с требованиями законодательства Российской Федерации в сфере ПОД/ФТ; программные продукты для предоставления информации в Росфинмониторинг (КОМИТА АРМ «Организация - М»), в том числе и порядок их сертификации; порядок оформления эксплуатационной документации, регламентов (06.032 А/01.5); ведение протоколов и журналов учета при осуществлении мониторинга и аудита систем защиты информации (06.033 А/02.5); организационные меры по защите информации; понятие, структуру, функции, этапы, виды общения, информирование персонала о правилах эксплуатации (06.033

		A/02.5); техники и приемы общения, инструктажи пользователей (06.032 A/02.5) **Уметь:** использовать законодательство в сфере ПОД/ФТ, нормативные правовые акты и правила внутреннего контроля в целях ПОД/ФТ; осуществлять мониторинг финансово-хозяйственной деятельности клиентов для выявления необычной / подозрительной деятельности в целях ОД/ФТ; анализировать информацию и выявлять операции (сделки), подлежащие контролю в целях ПОД/ФТ; осуществлять подготовку и направление материалов о выявлении операций (сделок), подлежащих контролю в целях ПОД/ФТ и иной информации в соответствии с требованиями законодательства Российской Федерации в сфере ПОД/ФТ; применять риск-ориентированный подход в вопросах ПОД/ФТ; использовать специализированные программные продукты (КОМИТА АРМ «Организация - М»); находить решение профессиональных проблем. **Иметь практический опыт:** использования международных стандартов ПОД/ФТ; применения норм законодательства Российской Федерации, нормативных правовых актов и правил внутреннего контроля в целях ПОД/ФТ; изучения и идентификации клиентов организации в целях ПОД/ФТ, в том числе осуществление сбора дополнительной информации (сбор сведений о возможных фактах ПОД/ФТ путем мониторинга средств массовой информации, информационно-телекоммуникационной сети «Интернет», получения информации в рамках сотрудничества участников профессиональных объединений); работы с перечнем организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму; анализа финансовых

		операций (сделок) организации и клиентов организации в целях выявления их связи с ПОД/ФТ (выявление операций (сделок), подлежащих обязательному контролю в целях ПОД/ФТ / необычных (сомнительных) операций); оценки степени (уровня) риска совершения клиентом операций, связанных с ПОД/ФТ; разработки модели по автоматизации процессов: проверки клиентов на принадлежность к Перечню организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму и автоматизации процесса заполнения анкет клиентов на базе имеющихся информационных ресурсов; выявления отдельных операций (сделок), подлежащих обязательному контролю, и необычных (сомнительных) операций; подготовки и представления в установленном порядке информации по операциям (сделкам), подлежащим обязательному контролю, и о необычных (сомнительных) операциях (внутренних сообщений и формализованных электронных сообщений (ФЭС)); использования специализированных программных продуктов (ПО АРМ «Организация–М»), организации деловое общение в коллективе или команде, использование приемов саморегуляции поведения в процессе межличностного общения.

3. Структура и содержание преддипломной практики

№ п/п	Разделы (этапы) практики	Кол-во часов/ недель			Форма контроля (Компетенции)
		Всего	аудиторные		
			практика	консультация	
1	Ознакомление с целями и задачами практики. Инструктаж по технике безопасности и пожарной безопасности Составление плана и графика работы на	25	22	3	Отчет, дневник практики (ОК 1-10)

	период практики, опираясь на индивидуальное задание дипломного проекта и учитывая специфику и режим работы организации – места прохождения практики.				
2	Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Анализ вида, структуры, функций организации.	25	22	3	Отчет, дневник практики (ОК 1-10, ПК 1.1-1.6; 2.1-2.6; 3.1-3.5)
3	Практическое изучение предмета проектирования. Изучение проблемы, которую необходимо решить в ходе дипломного проектирования. Поиск уже существующих решений, их анализ. Оценка перспективы и возможности практического применения решения проблемы в условиях конкретного предприятия, организации – месте прохождения практики.	30	28	2	Обобщение собранного материала в отдельном разделе отчета (ОК 1-10, ПК 1.1-1.6; 2.1-2.6; 3.1-3.5)
4	Поиск дополнительной информации, необходимость в которой возникла для решения вопросов, возникших в ходе знакомства с предметной областью выполнения ВКР.	20	18	2	Перечень используемых нормативных правовых актов и информационных программ (ОК 1-10, ПК 1.1-1.6; 2.1-2.6; 3.1-3.5)
5	Подготовка данных для реализации системы защиты информационной системы: организационное, программное, техническое, правовое обеспечени и т.п.	20	18	2	Обобщение собранного материала в отдельном разделе отчета (ОК 1-10, ПК 1.1-1.6; 2.1-2.6; 3.1-3.5)
6	Практическое изучение средств реализации предмета проектирования.	18	16	2	Отчет, дневник практики (ОК 1-10, ПК 1.1-1.6; 2.1-2.6; 3.1-3.5)
7	Анализ собранного материала по средствам защиты информационных систем. Оценка перспектив и возможности применения программно-технических средств защиты в условиях	6	6		Обобщение собранных материалов по теме дипломной работы. Оформление отчета по практике

	предприятия, организации – места прохождения практики. Оформление отчета по практике				(ОК 1-10, ПК 1.1-1.6; 2.1-2.6; 3.1-3.5)
8	Защита отчета				Отчет
	Итого:	144 часа			

4. Условия реализации программы преддипломной практики

4.1. Требования к проведению преддипломной практики

Продолжительность рабочей недели обучающихся при прохождении практики составляет не более 36 часов в неделю.

С момента зачисления обучающихся в период практики в качестве практикантов на рабочие места на них распространяются правила охраны труда и правила внутреннего распорядка, действующие в организации.

Обязанности обучающегося-практиканта:

● до начала практики обучающийся должен ознакомиться с Правилами внутреннего трудового распорядка организации, техники безопасности и охраны труда.

● подчиняться требованиями трудовой и производственной дисциплины, установленной в организации, являющейся базой практики;

● подготовить отчет о практике и защитить его в установленные сроки.

Руководство практикой обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю или наличие высшего профессионального образования и дополнительного профессионального образования по специальности «Информационная безопасность». Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за руководство производственной практикой. Руководитель практики определяется университетом в начале учебного года. Руководитель по практике консультирует обучающихся по всем вопросам данной программы практики, осуществляет прием отчетов и проводит аттестацию по результатам практики.

Контроль за работой обучающихся осуществляют руководитель практики.

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и отзыва преподавателя - руководителя практики. По итогам практики выставляется оценка «зачтено» или «не зачтено».

4.2. Требования к минимальному материально-техническому обеспечению

Реализация программы преддипломной практики требует наличия: рабочих мест прохождения практики.

Оборудование рабочих мест проведения учебной практики:

- ПК с доступом к сети Интернет
- калькуляторы
- принтер
- сканер
- программное обеспечение общего и профессионального назначения
- комплекс учебно-методической документации.

4.3. Учебно-методическое и информационное обеспечение практики

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Нормативно-правовые акты:

1. Конституция Российской Федерации: принята всенар. голосованием 12.12.1993 г. // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.
2. Гражданский кодекс РФ (часть 4): Федеральный закон от 18.12.2006 N 230-ФЗ //СЗ РФ. – 2006. - №52. – Ст. 5496.
3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008
20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2 Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
21. Приказ ФАПСИ при Президенте Российской Федерации 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».
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3 Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4 Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5 Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2 Функциональные требования безопасности
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3 Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014
36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000
37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006
38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005

39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993
40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014
41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных электромагнитных воздействий. Общие требования. Росстандарт, 2014
42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель. Росстандарт, 2012
43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2 Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013
44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002
46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006
47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006
48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002
49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17
50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Основная литература:

1. Инженерная и компьютерная графика : учебник и практикум для среднего профессионального образования / Р. Р. Анамова [и др.] ; под общей редакцией С. А. Леоновой, Н. В. Пшеничновой. — Москва : Издательство Юрайт, 2021. — 246 с. — (Профессиональное образование). — ISBN 978-5-534-02971-0. — С. 90 — 106 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471039/p.90-106
2. Информационные технологии в 2 т. Том 2 : учебник для среднего профессионального образования / В. В. Трофимов, О. П. Ильина, В. И. КИЯЕВ, Е. В. Трофимова ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2021. — 390 с. — (Профессиональное образование). — ISBN 978-5-534-03966-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469958
3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:

https://urait.ru/bcode/475889
4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548
5. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для среднего профессионального образования / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2020. — 291 с. — (Профессиональное образование). — ISBN 978-5-534-08140-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455865
6. Шишмарёв, В. Ю. Диагностика и надежность автоматизированных систем : учебник для среднего профессионального образования / В. Ю. Шишмарёв. — 2-е изд. — Москва : Издательство Юрайт, 2021. — 341 с. — (Профессиональное образование). — ISBN 978-5-534-13629-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475872

Дополнительная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356
4. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638
5. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455863

Интернет-ресурсы:

1. Электронно-библиотечная система издательства ЮРАЙТ - URL: www.: urait.ru
2. Электронно-библиотечная система «Университетская библиотека онлайн» www.biblioclub.ru
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. URL: http://elibrary.ru
4. Национальная электронная библиотека [Электронный ресурс]. URL: http://нэб.рф/.
5. Справочно-правовая система «КонсультантПлюс». URL: http://www.consultant.ru
6. Справочно-правовая система «Гарант». URL: http://www.garant.ru.

5. Контроль и оценка результатов производственной практики

5.1. Формы отчетности по практике

К защите по итогам практики студенты должны представить следующую документацию:

- характеристику студента с места прохождения практики;
- дневник;
- в качестве приложения к дневнику практики обучающийся оформляет графические, аудио-, фото-, видео-, материалы, наглядные образцы изделий, документы соответствующих организаций подтверждающие практический опыт, полученный на практике;
- отчет по практике;
- аттестационный лист.

В характеристике фиксируется степень подготовленности студента для работы по данной специальности, уровень теоретических знаний, умение организовать свой рабочий день и другие качества, проявленные студентом в период практики, замечания и пожелания студенту, а также общий вывод руководителя практики о выполнении студентом программы практики.

По окончании практики, каждый студент составляет в письменном виде отчет о прохождении практики (далее – отчет):

- отчет утверждается практическим работником, осуществлявшим непосредственное руководство практикой студента.
- отчет выполняется в машинописной форме на листе формата А4, шрифт Times New Roma№, размер 14, интервал полуторный, левое поле 3 см, правое поле 1 см, верхнее и нижнее поля 2-2,5 см. Объем отчета должен составлять 1-5 страниц.

Содержание отчета должно включать в себя:

- место и время прохождения практики;
- информацию об организации, отделе, структуре организации, анализ ее деятельности;
- краткое описание работы по отдельным разделам программы практики;
- определение проблем, возникших в процессе практики и предложения по их устранению;
- выводы по итогам практики о приобретенных навыках и практическом опыте.

- отчет должен отражать выполнение индивидуального задания программы практики, заданий и поручений, полученных от руководителя практики от организации.

В период прохождения практики студентом ведется дневник практики. В дневнике практики записываются краткие сведения о проделанной работе в течение дня в соответствии с планом работы. В качестве приложения к дневнику практики обучающийся оформляет графические, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

Контроль и оценка результатов прохождения производственной практики осуществляется руководителями практики от образовательного учреждения и организации в процессе выполнения обучающимися заданий, проектов, выполнения практических проверочных работ.

5.2. Формы и методы контроля и оценки результат обучения

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты обучения	Основные показатели оценки результата	Формы и методы контроля и оценки

(освоенные компетенции)		
Общие компетенции		
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.	Оценка на защите отчета по практике
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.	Оценка на защите отчета по практике
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения. Обоснованность самоанализа и коррекция результатов собственной работы.	Интерпретация результатов наблюдений за деятельностью обучающихся в процессе освоения образовательной программы; мониторинг и оценка эффективной организации профессиональной деятельности
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных).	Мониторинг развития личностно-профессиональных качеств обучающегося
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы.	Мониторинг развития личностно-профессиональных качеств обучающегося
ОК 6. Проявлять гражданско-патриотическую позицию,	Определять сущность гражданско-патриотической позиции, общечеловеческих ценностей; -	Мониторинг развития личностно-профессиональных качеств обучающегося

демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	описывать значимость своей специальности.	
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.	Мониторинг развития личностно-профессиональных качеств обучающегося
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Соблюдать основы здорового образа жизни и условия профессиональной деятельности; использовать физкультурно-оздоровительную деятельность для укрепления здоровья; пользоваться средствами профилактики перенапряжения характерными для данной специальности.	Интерпретация результатов наблюдений за деятельностью обучающихся в процессе освоения образовательной программы; мониторинг и оценка эффективной организации профессиональной деятельности
ОК 9. Использовать информационные технологии в профессиональной деятельности.	Применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение.	Накопительная оценка за решения нестандартных ситуаций на практике.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	Знать правила оформления документов и построения устных сообщений; уметь грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке.	Интерпретация результатов наблюдений за деятельностью обучающихся в процессе освоения образовательной программы.
ПК 1.1. Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Мониторинг и оценка эффективной организации профессиональной деятельности

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной системы в защищенном состоянии.	Оценка практической работы. Анализ характеристики на студента с места прохождения практики.
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Оценка решения ситуационных задач. Оценка практической работы. Анализ характеристики на студента с места прохождения практики.
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении.	Оценка решения ситуационных задач. Оценка практической работы. Анализ характеристики на студента с места прохождения практики.
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Проявлять знания особенностей и способов применения программных и программно-аппаратных средств защиты информации в целях установки, настройки, применения программно-аппаратных средств защиты информации. Уметь устанавливать, настраивать программных средств защиты информации в автоматизированной системе	Оценка решения ситуационных задач. Оценка практической работы.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Устанавливать и настраивать программно-аппаратные средства защиты информации, в том числе средства антивирусной защиты Обеспечивать защиту автономных автоматизированных систем программными и программно-аппаратными средствами.	Анализ характеристики на студента с места прохождения практики.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	Оценка решения ситуационных задач.
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Решать задачи защиты от НСД и информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	Анализ характеристики на студента с места прохождения практики.
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Применять средства гарантированного уничтожения информации	Анализ характеристики на студента с места прохождения практики.
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.	Установка, монтажом и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации	Оценка решения ситуационных задач.
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Проводить техническое обслуживание технических средств защиты информации в соответствии с номенклатурой применяемых средств защиты информации от несанкционированной утечки по техническим каналам	Оценка решения ситуационных задач.
ПК 3.2. Осуществлять эксплуатацию	Определять физические основы, структуру и условия формирования	Оценка практической работы.

технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	технических каналов утечки информации, способы их выявления и методы оценки опасности, классификации существующих физических полей и технических каналов утечки информации. Устанавливать порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Проводить измерения параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации	Анализ характеристики на студента с места прохождения практики.
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Проводить измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявлять технические каналы утечки информации	Оценка практической работы.
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, инженерно-технические средства физической защиты объектов информатизации	Анализ характеристики на студента с места прохождения практики.
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Защита отчета Отзыв руководителя практики от организации
ПК 4.2 Создавать и управлять на персональном компьютере	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и	Защита отчета Отзыв руководителя практики от организации

текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	презентациями ,а также базами данных	
ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	Защита отчета Отзыв руководителя практики от организации
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютерной системе	Защита отчета Отзыв руководителя практики от организации
ПК 5.1. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами	Разработка спецификаций, разработка алгоритма поставленной задачи, реализация алгоритма средствами автоматизированного проектирования	Оценка решения ситуационных задач.
ПК 5.2. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами	Разработка спецификаций, разработка алгоритма поставленной задачи, реализация алгоритма средствами автоматизированного проектирования	Оценка решения ситуационных задач.
ПК 5.3. Знать и уметь ориентироваться в организационно-правовой системе противодействия легализации доходов, полученных преступным путем и финансированию терроризма	умение ориентироваться и использовать в своей деятельности организационно-правовую систему ПОД/ФТ	Оценка практической работы. Анализ характеристики на студента с места прохождения практики.
ПК 5.4. Знать и уметь использовать специализированное	Первичные навыки использования специализированного ПО АРМ «Организация – М»	Оценка практической работы. Анализ характеристики на

программное обеспечение финансового мониторинга предприятий и организаций		студента с места прохождения практики.
ПК 5.5. Осуществлять анализ информации экономико-правового характера для противодействия негативным процессам, подрывающим экономическую безопасность России	Практическое применение совокупности знаний, полученных при освоении модуля ПОД/ФТ, в том числе умение получать и анализировать информацию экономико-правового характера для противодействия негативным процессам, подрывающим экономическую безопасность России	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)

Типовые индивидуальные (контрольные) задания

1. Состав и принципы работы автоматизированных систем, операционных систем и сред.
2. Принципы разработки алгоритмов программ, основных приемов программирования.
3. Модели баз данных.
4. Принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.
5. Теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации.
6. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.
7. Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных. типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации.
8. Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.
9. Основные понятия криптографии и типовых криптографических методов и средств защиты информации.
10. Физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации.
11. Номенклатура и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - пэмин), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

12. Основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации.
13. Основные способы физической защиты объектов информатизации.
14. Методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации.
15. Номенклатура применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.
16. Назначение и виды операционных систем, утилит, файловых менеджеров.
17. Выбор оптимального использования.
18. алгоритмы установки аппаратного обеспечения и инструкции использования периферийных устройств
19. Средства защиты персонального компьютера и данных
20. Сообщения об ошибках аппаратных средств и программного обеспечения, рекомендации по их ликвидации
21. Методы восстановления данных, профилактические меры работоспособности электронно-вычислительных и вычислительных машин.
22. Международные стандарты и институциональные основы международной системы под/фт.
23. Законодательство российской федерации в сфере под/фт в том числе программы и процедуры, регламентирующие выполнение требований законодательства в сфере под/фт.
24. Типологии и схемы отмывания денег.
25. Признаки операций, подлежащих обязательному контролю в целях под/фт, критерии выявления и признаки необычных сделок, связанных с отмыванием денег или финансированием терроризма, организационные меры по защите информации (06.032 а/01.5)
26. Программы осуществления внутреннего контроля в целях под/фт.
27. Структура государственных органов российской федерации, осуществляющих регулирование в сфере под/фт, их правовой статус и полномочия, компетенции уполномоченного органа в сфере под/фт.
28. Требования к оформлению документов и порядок работы с конфиденциальной информацией.
29. Порядок предоставления информации в соответствии с требованиями законодательства российской федерации в сфере под/фт.
30. Программные продукты для предоставления информации в росфинмониторинг (комита арм «организация - м»), в том числе и порядок их сертификации.
31. Порядок оформления эксплуатационной документации, регламентов (06.032 а/01.5)
32. ведение протоколов и журналов учета при осуществлении мониторинга и аудита систем защиты информации (06.033 а/02.5).
33. Организационные меры по защите информации.
34. Понятие, структура, функции, этапы, виды общения, информирование персонала о правилах эксплуатации (06.033 а/02.5) техники и приемы общения, инструктажи пользователей (06.032 а/02.5).