МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
КОЛЛЕДЖ ДГУ

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПРОФЕССИОНАЛЬНЫЕ МОДУЛИ

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.05 Противодействие отмыванию денег и финансированию терроризма

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

Специальность:	*10.02.05 Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовке*
Уровень образования, на базе которого осваивается ППССЗ:	*Основное общее образование*
Квалификация:	*Техник по защите информации*
Форма обучения:	*Очная*

Махачкала, 2021

Рабочая программа производственной практики по профессиональным модулям:
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.05 Противодействие отмыванию денег и финансированию терроризма
разработана на основе требований Федерального государственного образовательного стандарта (далее – ФГОС) СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем по программе базовой подготовке, для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования

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

Автор-разработчик:
Магдилова Л.В. – зав. отделением специальности «Обеспечение информационной безопасности автоматизированных систем» Колледжа ФГБОУ ВО «ДГУ», доцент кафедры информационного права и информатики Юридического института ФГБОУ ВО «ДГУ», к.э.н.

Рецензент:
Камилов М.-К. Б. к.э.н., доцент, зав. кафедрой прикладной информатики ДГУ

Рабочая программа производственной практики рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол № 7 от «27» 03 2021г.

Зав. кафедрой Магдилова Л.В.

Рабочая программа производственной практики согласована с учебно-методическим управлением

«16» 03 2021 г. _____
(подпись)

Программа производственной практики согласована с представителем работодателя

Нач. отдела информационной безопасности Министерства [illegible]
(полное наименование организации и должности руководителя)

Медилов Артур Гаирович
ФИО

(подпись)

М.П.

СОДЕРЖАНИЕ

1. Паспорт программы производственной практики

1.1. Область применения программы производственной практики

Производственная 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; противодействие отмыванию денег и финансированию терроризма.

Практика направлена на формирование у студента общих и профессиональных компетенций, получение практического опыта по каждому из видов профессиональной деятельности, подготовку к осознанному и углубленному изучению отдельных специальных дисциплин.

1.2. Цели и задачи производственной практики, требования к результатам

1.2.1. Цели практики:

- Закрепление и систематизация полученных знаний в сфере профессиональной деятельности;
- Овладение профессиональными умениями и навыками в сфере профессиональной деятельности;
- Углубление теоретических знаний, полученных в процессе обучения;
- Повышение мотивации к профессиональному самосовершенствованию, расширение профессионального кругозора;
- Приобретение опыта работы в коллективах при решении ситуационных задач; изучение методов и средств эффективного анализа функционирования программного обеспечения; основных видов работ на этапе сопровождения программного обеспечения; основных принципов контроля конфигурации и поддержки целостности конфигурации программного обеспечения; средств защиты программного обеспечения в компьютерных системах.

1.2.2. Задачи практики:

- Получение обучающимися информации о будущей профессиональной деятельности;
- Ознакомление с методами, способами и средствами обеспечения защиты автоматизированных информационных систем;
- Получение учащимися навыков работы с программно-техническими системами защиты информации;
- Ознакомление с организационно-правовой документацией, регламентирующей создание и функционирование систем защиты информации;
- Сбор материалов, необходимых для составления отчета о прохождении практики в соответствии с дневником практики.

1.3 Место производственной практики в структуре ОПОП ПССЗ

Производственная практика согласно ОПОП ПССЗ проводится после прохождения основных междисциплинарных курсов (МДК) в рамках профессиональных модулей «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»; «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»; «Защита информации техническими средствами»; «Противодействие отмыванию денег и финансированию терроризма».

1.4 Трудоемкость и сроки проведения практики

Трудоемкость производственной практики в рамках освоения профессиональных модулей «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»; «Защита информации в автоматизированных системах программными и

программно-аппаратными средствами»; «Защита информации техническими средствами»; «Противодействие отмыванию денег и финансированию терроризма» составляет 360 часов (десять недель).

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 3 курсе, в шестом семестре; на 4 курсе, в седьмом и восьмом семестрах.

1.5 Место прохождения производственной практики

Практика проводится в ведомствах и 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".

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

2. Перечень планируемых результатов освоения программы производственной практики

Результатом прохождения производственной практики в рамках освоения профессиональных модулей «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»; «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»; «Защита информации техническими средствами»; «Противодействие отмыванию денег и финансированию терроризма», в том числе профессиональными (ПК) и общими (ОК) компетенциями.

Результатом практики является освоение общих компетенций, включающих в себя способность:

Код компетенции	Наименование результата освоения практики
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

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

Компетенции	Формулировка компетенции из ФГОС	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ПМ. 01 Эксплуатация автоматизированных систем в защищенном исполнении		
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,	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

	устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
ПМ. 02 Защита информации в автоматизированных системах программами и программно-аппаратными средствами		
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
ПМ. 03 Защита информации техническими средствами		
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
ПМ. 05 Противодействие отмыванию денег и финансированию терроризма		
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 А/02.5); техники и приемы общения, инструктажи пользователей (06.032 А/02.5) **Уметь:** использовать законодательство в сфере ПОД/ФТ, нормативные правовые акты и правила внутреннего контроля в целях ПОД/ФТ; осуществлять
ПК 5.2.	Использовать нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности в области противодействия отмывания денег и финансированию терроризма, инженерно-техническими средствами.	
ПК 5.3.	Самостоятельно ориентироваться в организационно-правовой системе противодействия легализации денег, полученных преступным путем и	

	финансированию терроризма.	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
ПК 5.4.	Знать и уметь использовать специализированное программное обеспечение финансового мониторинга предприятий и организаций.	
ПК 5.5.	Осуществлять анализ информации экономико-правового характера для противодействия негативным процессам, подрывающим экономическую безопасность России.	

		АРМ «Организация–М»), организации деловое общение в коллективе или команде, использование приемов саморегуляции поведения в процессе межличностного общения.

3. Структура и содержание производственной практики

№ п/п	Разделы (этапы) практики	Кол-во часов/ недель			Форма контроля (Компетенции)
		Всего	аудиторные		
			практические	консультации	
ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении					
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	6	4	2	Отчет, дневник практики (ПК 1.1-1.6)
2	Участие в ведении основных этапов проектирования системы безопасности автоматизированных систем. Эксплуатация компонентов подсистем безопасности автоматизированных систем, их диагностики, устранение отказов и восстановление работоспособности.	30	28	2	Отчет, дневник практики (ПК 1.1-1.6)
3	Участие в организации работ по эксплуатации подсистем и средств безопасности автоматизированных систем. Администрирование подсистем безопасности автоматизированных информационных систем.	36	34	2	Отчет, дневник практики (ПК 1.1-1.6)
4	Ознакомление с особенностями функционирования систем обеспечения безопасности организации.	36	34	2	Отчет, дневник практики (ПК 1.1-1.6)
5	Установка компонентов подсистем безопасности автоматизированных информационных систем	30	28	2	
6	Оформление отчета по практике	6	4	2	Отчет, дневник практики (ПК 1.1-1.6)
7	Защита отчета		Отчет	5	Защита отчета
	Итого	144			

ПМ.02 Защита информации в автоматизированных системах программами и программно-аппаратными средствами					
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	6	4	2	Отчет, дневник практики (2.1-2.6)
2	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Диагностика, устранение отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности.	30	28	2	Отчет, дневник практики (2.1-2.6)
3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. Осуществлять обработку, хранение и передачу информации ограниченного доступа. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. Мониторинг эффективности программно-аппаратных средств обеспечения информационной безопасности; обеспечения учета, обработки, хранения и передачи конфиденциальной информации.	18	16	2	Отчет, дневник практики (2.1-2.6)
4	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах,	12	10	2	Отчет, дневник практики (2.1-2.6)

	в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. Решение технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов; применения нормативных правовых актов по обеспечению информационной безопасности программно-аппаратными средствами.				
5	Оформление отчета по практике	6	4	2	Отчет, дневник практики (2.1-2.6)
6	Защита отчета				Отчет
	Итого	72			
ПМ.03 Защита информации техническими средствами					
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	6	4	2	Отчет, дневник практики (ПК 3.1-3.5)
2	Применять инженерно-технические средства обеспечения информационной безопасности. Выбор технических средств обеспечения информационной безопасности.	30	28	2	(ПК 3.1-3.5)
3	Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. Определение видов и способов технической защиты информационной безопасности.	18	16	2	(ПК 3.1-3.5)
4	Выявление и устранение	12	10	2	(ПК 3.1-3.5)

	недостатков инженерно-технических средств обеспечения информационной безопасности; соблюдение правил эксплуатации оборудования. Определение технологических возможностей.				
5	Оформление отчета по практике	6	4	2	(ПК 3.1-3.5)
6	Защита отчета				Отчет
	Итого	72			
ПМ.05 Противодействие отмыванию денег и финансированию терроризма					
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	6	4	2	Отчет, дневник практики (ПК 5.1-5.5)
2	Осуществлять сбор дополнительной информации в целях ПОД/ФТ, в том числе сбор информации о возможных фактах ОД/ФТ путем мониторинга средств массовой информации, информационно-телекоммуникационной сети "Интернет", полученной в рамках сотрудничества участников профессиональных объединений. Ориентирование в организационно-правовой системе противодействия легализации денег, полученных преступным путем и финансированию терроризма Использование специализированного программного обеспечения финансового мониторинга предприятий и организаций	30	28	2	Отчет, дневник практики (ПК 5.1-5.5)
3	Выявлять операции по открытию счетов, приобретению и продаже ценных бумаг обществами, имеющими стратегическое значение для оборонно-промышленного комплекса и безопасности Российской Федерации, а также	30	28	2	Отчет, дневник практики (ПК 5.1-5.5)

	обществами, находящихся под их прямым или косвенным контролем. Осуществление анализа информации экономико-правового характера для противодействия негативным процессам, подрывающим экономическую безопасность России.				
4	Оформление отчета по практике	6	4	2	Отчет, дневник практики (ПК 5.1-5.5)
5	Защита отчета				Отчет
	Итого	72			
	Итого:	360 часов			

4. Условия реализации программы производственной практики

4.1. Требования к проведению производственной 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 производственной 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 10.02.05 «Обеспечение информационной безопасности автоматизированных систем». 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 производственной практики требует наличия рабочих мест прохождения практики.

Оборудование рабочих мест проведения учебной практики:

- ПК с доступом к сети Интернет
- 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 результатов 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 (освоенные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Общие компетенции		
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	Оценка практической работы. Анализ характеристики на студента с места прохождения практики.
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 решения ситуационных задач. 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.
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.	Анализ характеристики на студента с места прохождения практики.

	Уметь устанавливать, настраивать программных средств защиты информации в автоматизированной системе	
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.	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)
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	Анализ характеристики на студента с места прохождения практики.
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	Оценка решения ситуационных задач.
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с	Установка, монтажом и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение	Оценка решения ситуационных задач.

использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	основных типов технических средств защиты информации	
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 практической работы.
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Определять физические основы, структуру и условия формирования 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	Оценка практической работы.
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	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)
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также	Применять технические средства для защиты информации в условиях	Оценка решения ситуационных задач.

физических полей, создаваемых техническими средствами защиты информации.	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	
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	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)
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	Первичные навыки использования	Оценка практической работы. Анализ

специализированное программное обеспечение финансового мониторинга предприятий и организаций	специализированного ПО АРМ «Организация – М»	характеристики на 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

Индивидуальные задания по разделам:

Вариант № 1

Опишите способы непосредственного воздействия на носители защищаемой информации. Приведите способы вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи. Опишите виды дестабилизирующего воздействия на защищаемую информацию со стороны источника воздействия — технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Вариант № 2

Составьте документацию на заданное контролируемое помещение, определите возможные разведопасные направления и возможные виды разведки. Составьте план проведения визуального осмотра помещения и выявите объекты, требующие при обследовании использования имеющихся средств видеонаблюдения.

Вариант № 3

Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля?

Вариант № 4

Каково назначение экранирования в системах обработки и передачи информации? Расскажите об экранировании электрических полей (типы полей, диапазон частот). Какие способы уменьшения паразитной емкости при экранировании низкочастотных электрических полей Вам известны? Как взаимосвязаны толщина и магнитная проницаемость экрана? Из каких материалов изготавливают экраны против высокочастотных магнитных полей? На каком принципе осуществляется экранирование высокочастотных магнитных полей?

Вариант № 5

Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей. Приведите основные причины утечки информации в волоконно-оптических линиях. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон. Приведите примеры технических средств защиты от утечки информации по проводному каналу.

Вариант № 6

Что является основой анализа разборчивости речевой информации? Каков диапазон уровней человеческой речи? Какие звуки являются наиболее информативными с точки зрения разборчивости речевой информации? На каком расстоянии от источника производится измерение уровней речи? Что используют для количественной оценки качества перехваченной речевой информации? Приведите примеры технических средств защиты от утечки по виброакустическому каналу.

Вариант № 7

Опишите способы перехвата побочных электромагнитных излучений технических средств передачи, обработки, информации ограниченного доступа (ТСПИ). Приведите методы защиты информации от ПЭМИН. Опишите технологию исследования ПЭМИН-монитора.

Вариант № 8

Опишите варианты утечки информации по цепям заземления и электропитания. Приведите меры по предотвращению утечки защищаемой информации по цепям заземления и электропитания. Опишите принцип действия прибора РНИ-1.1

Вариант № 9

Назовите и охарактеризуйте пассивные технические средства защиты телефонной линии. Как осуществляется контроль состояния телефонной линии и обнаружение атак? Приведите методы активной защиты информации в телефонных линиях. Опишите технологию защита речевой информации в IP-телефонии.

Вариант № 10

Опишите оптические каналы утечки информации, способы получения информации в оптическом канале. Опишите технологию работы телевизионных систем наблюдения.

Контрольные вопросы

1. Компоненты автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
2. Средства защиты информации прикладного и системного программного обеспечения Программное обеспечение с соблюдением требований по защите информации
3. Средства антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам
4. Инструкции пользователей о соблюдении требований по защите информации при работе с программным обеспечением
5. Средства защиты информации программного обеспечения
6. Встроенные средства защиты информации программного обеспечения
7. Своевременное обнаружение признаков наличия вредоносного программного обеспечения
8. Обслуживание средств защиты информации в компьютерных системах и сетях
9. Обслуживание систем защиты информации в автоматизированных системах
10. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем
11. Проверка работоспособности системы защиты информации автоматизированной системы

12. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации
13. Контроль стабильности характеристик системы защиты информации автоматизированной системы
14. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем
15. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем
16. Анализ принципов построения систем информационной защиты производственных подразделений.
17. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.
18. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;
19. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении
20. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации
21. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.
22. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации
23. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
24. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам
25. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.
26. Изучение порядка применения нормативных правовых актов
27. Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами
28. Выявление технических каналов утечки информации
29. Применение существующих способов выявления опасности целостности информации
30. Анализ объектов информатизации предприятий, учреждений, организаций
31. Анализ ресурсов обеспечения инженерно-технической защиты информации
32. Изучение основных этапов проектирования системы защиты информации техническими средствами
33. Проектирование рабочих проектов по системам пожарно-охранной сигнализации, видеонаблюдения, СКУД
34. Оформление технической и технологической документации
35. Выявление физических лиц и организаций из Перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму
36. Выявление операций, подлежащих обязательному контролю, с ценной сделки 600 000 рублей и выше
37. Выявление операций по открытию счетов, приобретению и продаже ценных бумаг обществами, имеющими стратегическое значение для оборонно-промышленного комплекса и безопасности Российской Федерации, а также обществами, находящихся под их прямым или косвенным контролем
38. Выявление операций по получению (зачислению) некоммерческой организацией ценных бумаг от иностранных государств, международных и иностранных

организаций, иностранных граждан и лиц без гражданства, а равно по расходованию (списанию) ценных бумаг указанной организацией

39. Выявление операции с ценными бумагами, если хотя бы одной из сторон является физическое или юридическое лицо, имеющее соответственно регистрацию, место жительства или место нахождения в государстве (на территории), которое (которая) не выполняет рекомендации ФАТФ, либо если указанные операции проводятся с использованием счета в банке, зарегистрированном в указанном государстве (на указанной территории