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

УТВЕРЖДАЮ

Заместитель директора по УПР и СР

_____ О.М. Сумлинова
«30» июня 2022г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

по специальности среднего профессионального образования
10.02.05 Обеспечение информационной безопасности автоматизированных систем

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

Москва 2022 г.

Рабочая программа производственной практики разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. №1553, зарегистрированного в Министерстве юстиции Российской Федерации 26 декабря 2016 г. №44938, и Примерной основной образовательной программы по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем (регистрационный номер в федеральном реестре примерных образовательных программ СПО 10.02.05-170703, дата регистрации 03.07.2017).

Разработчики:
Володин С.М., к.т.н., преподаватель ВКК Колледжа информатики и программирования; Панюкова Е.В. методист ВКК Колледжа информатики и программирования

Рецензент:

(ФИО, ученая степень, звание, должность)

Рабочая программа учебной практики рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии Обеспечение информационной безопасности автоматизированных систем
Протокол от «12» мая 2022 г.№ 4
Председатель ПЦК _____ С.М. Володин

Рабочая программа учебной практики рассмотрена и одобрена Методическим советом Колледжа информатики и программирования Финансового университета при Правительстве Российской Федерации

Протокол от «23» июня 2022 г.№ 3

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРСИТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ 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

1.1. Цель и планируемые результаты освоения программы производственной практики

- формирование у обучающихся практических умений и приобретение первичного практического опыта в рамках освоения профессиональных модулей образовательной программы СПО по основным видам деятельности в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем и личностных результатов в соответствии с программой воспитания

1.1.1 Перечень общих компетенций

Код	Общие компетенции
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, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

1.1.2 Перечень профессиональных компетенций

Код	Профессиональные компетенции
ПМ. 01	**Эксплуатация автоматизированных (информационных) систем в защищенном исполнении:**
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ПМ.02	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами:**
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
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.
ПМ.03	**Защита информации техническими средствами:**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.3. Перечень личностных результатов

Код	Личностные результаты реализации программы воспитания
ЛР1	Осознающий себя гражданином и защитником великой страны
ЛР3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности
ЛР14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР15	Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем
ЛР16	Соответствующий ожиданиям работодателей: креативно мыслящий, эффективно сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, распределяющий время и другие ресурсы для выполнения поставленной задачи в установленный срок, ответственный, дисциплинированный, целеустремленный, стрессоустойчивый.

ЛР17	Демонстрирующий культуру речи, в том числе в деловой переписке/переговорах, способный презентовать себя и продукт профессиональной деятельности
ЛР18	Демонстрирующий способность использовать в цифровой среде различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

1.1.4. В результате прохождения производственной практики по видам профессиональной деятельности, обучающийся должен:

Вид деятельности: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
иметь практический опыт	– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; – эксплуатации компонентов систем защиты информации автоматизированных систем; диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении, *контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации**; *– администрирования автоматизированных систем в защищенном исполнении информационной системы 1С: Предприятие;** *– установки и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности**; *– обнаружения и устранения ошибок при передаче данных в компьютерных сетях**; *– работы с протоколами разных уровней**.
уметь	– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

	– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности – *обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения**; – *устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами**; – *формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;** – *создавать, редактировать и обслуживать автоматизированную систему управления предприятием на базе «1С: Предприятие»;** – *проверять правильность передачи данных.**
знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных, *порядок настройки систем управления базами данных и средств электронного документооборота**; – принципы построения, физические основы работы периферийных устройств*;* – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях, *порядок обеспечения безопасности информации при эксплуатации компьютерных сетей**; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – *типовые уязвимости программного обеспечения, методы их эксплуатации и порядок обеспечения безопасности информации при эксплуатации программного обеспечения**; – *особенности источников угроз, связанных с эксплуатацией программного обеспечения**; – *эксплуатационную и проектную документацию, регламенты по уничтожению информации и машинных носителей*

	информации автоматизированной системы;* *– принципы построения и функционирования, примеры реализаций современных операционных систем;** *– программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах;** *– адресацию в сетях, организацию межсетового взаимодействия;** *– основные этапы разработки простого прикладного решения в системе «1С:Предприятие»**
Вид деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
иметь практический опыт	– установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации*;* – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе; – *применения технологии фильтрации различных видов трафика*; * – *осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.**
уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать

	работоспособность и тестировать функции программно-аппаратных средств защиты информации, *проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;* – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; *- оформлять эксплуатационную документацию программно аппаратных средств защиты информации;** *- определять цели и задачи в изучении проекта;** *-разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;* – *осуществлять установку, развёртывание, настройку и использованием DLP-систем.**
знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации, *общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации*;* – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

	– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. – *теоретические основы корпоративной защиты информации от внутренних ИТ-угроз;** – *методику проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; современные стандарты и средства корпоративной защиты.* *
Вид деятельности: Защита информации техническими средствами	
иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения 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; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок;* * – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от 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; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, *технических средств защиты акустической речевой информации от утечки по техническим каналам*;* – применять инженерно-технические средства физической защиты объектов информатизации, – *производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов .**
знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – 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 и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – номенклатуру применяемых средств физической защиты объектов информатизации; – основные способы физической защиты объектов информатизации; – *порядок технического обслуживания, устранение*

	неисправностей и организацию ремонта технических средств защиты информации ;* *– нормативно правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации *;* *– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.* .*

1.2. Количество часов на освоение рабочей программы производственной практики:

Всего 468 часов, в том числе:

в рамках освоения ПМ.01 (ПП 01.01) – 5 нед., 180 ч.;
в рамках освоения ПМ.02 (ПП 02.01) – 4 нед., 144 ч.;
в рамках освоения ПМ.03 (ПП.03.01) – 4 нед., 144 ч.;

2.СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

2.1.Структура производственной практики

Коды профессиональных и общих компетенций, личностные результаты	Код и наименование профессиональных модулей	Суммарный объём нагрузки, час.	Виды работ	Наименование тем производственной практики	Количество часов по темам
ПК 1.1.-1.4. ОК.01-ОК.11	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**5 нед./180 ч**	Составление организационной структуры управления предприятием – базы практики Анализ программной и технической архитектуры ИС предприятия Определение места проектируемой задачи в комплексе задач и ее описание Анализ информационных потоков проектируемой задачи Анализ системы обеспечения информационной безопасности и защиты информации Анализ существующих разработок для автоматизации задачи* Выбор и обоснование стратегии автоматизации задачи Выбор и обоснование способа приобретения ИС для автоматизации комплекса задач Обслуживание средств защиты информации в компьютерных системах и сетях	Тема 1. Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; Тема 2. Администрирование автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; Тема 3 Эксплуатация компонентов систем защиты информации автоматизированных систем; Тема 4. Диагностика компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении,	24 24 24 26

			Обслуживание систем защиты информации в автоматизированных системах Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем Проверка работоспособности системы защиты информации автоматизированной системы Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации Контроль стабильности характеристик системы защиты информации автоматизированной системы Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	*контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации*;* Тема 5. *Администрирование информационной системы 1С: Предприятие;** *Тема 6. Установка и настройка операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности*;* *Тема 7. Обнаружение и устранение ошибок при передаче данных в компьютерных сетях*;* *Тема 8. Работа с протоколами разных уровней*.*	22 20 20 20
ПК 2.1-2.6. ОК.01-ОК.11	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	**4 нед./144 ч**	Анализ принципов построения систем информационной защиты производственных подразделений; Техническая эксплуатация элементов программной и	Тема 1. Установка, настройка программных средств защиты информации в автоматизированной системе;	16

			аппаратной защиты автоматизированной системы; Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении; Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики; Администрирование автоматизированных технических средств управления и контроля информации и информационных потоков* Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом* Выявление потоков передачи данных и возможных каналов утечки информации*	Тема 2. Обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; Тема 3. Тестирование функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; Тема 4. Решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; Тема 5. Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; Тема 6. Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации*;*	16 16 14 14 14

			Использование механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов* Проведение детектирования атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме.*	Тема 7. Работа с подсистемами регистрации событий; Тема 8. Выявление событий и инцидентов безопасности в автоматизированной системе; *Тема 9. Применение технологии фильтрации различных видов трафика; ** *Тема 10. Осуществление фильтрации перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/ запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.**	14 14 14 14
ПК 3.1-3.5. ОК.01-ОК.11	ПМ.03 Защита информации техническими средствами	**4 нед./144ч**	Анализ объектов информатизации предприятий, учреждений и организаций*. Анализ ресурсов обеспечения инженерно-технической защиты информации*. Изучение основных этапов проектирования системы защиты информации техническими средствами*.	Тема 1. Установка, монтаж и настройка технических средств защиты информации; Тема 2. Техническое обслуживание технических средств защиты информации; Тема 3. Применение основных типов технических средств защиты информации; Тема 4. Выявление технических каналов утечки информации;	12 12 12 14

			Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. Оценка эффективности защиты информации*.	Тема 5. Участие в мониторинге эффективности технических средств защиты информации; Тема 6. Диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; Тема 7. Проведение 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; Тема 8. Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; Тема 9. Установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление	12 12 12 12 12

				работоспособности инженерно-технических средств физической защиты; *Тема 10. Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок; ** *Тема 11. Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам. **	12 12
	Всего часов	**468**			

1.1. Тематический план и содержание производственной практики

Профессиональные модули и междисциплинарные курсы, темы	Содержание практики	Объём часов
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении МДК.01.01 Операционные системы МДК.01.02 Базы данных МДК.01.03 Сети и системы передачи информации МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		180

МДК.01.05. Эксплуатация компьютерных сетей		
Тема 1. Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; Тема 2. Администрирование автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; Тема 3 Эксплуатация компонентов систем защиты информации автоматизированных систем; Тема 4. Диагностика компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении, *контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации**; Тема 5. *Администрирование информационной системы 1С: Предприятие;** *Тема 6. Установка и настройка операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности**; *Тема 7. Обнаружение и устранение ошибок при передаче данных в компьютерных сетях**; *Тема 8. Работа с протоколами разных уровней**.	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями. Изучение специализированного и прикладного программного обеспечения, СУБД, топология ЛВС. Оценка информационных активов, уязвимостей, угроз и рисков информационной безопасности. Участие в настройке и сопровождении аппаратных и программных средств, администрировании баз данных, средств ИБиЗИ. Сбор и изучение научно-практического материала по разделам ВКР, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР. Проведение анализа и обобщения научно-технической информации по теме ВКР. Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение. Подготовка плана пояснительной записки к ВКР. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием. Подготовка отчета.	
ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами МДК.02.01. Программные и программно-аппаратные средства защиты информации МДК.02.02. Криптографические средства защиты информации МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности		144

Тема 1. Установка, настройка программных средств защиты информации в автоматизированной системе; Тема 2. Обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; Тема 3. Тестирование функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; Тема 4. Решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; Тема 5. Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; Тема 6. Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации*;* Тема 7. Работа с подсистемами регистрации событий; Тема 8. Выявление событий и инцидентов безопасности в автоматизированной системе; *Тема 9. Применение технологии фильтрации различных видов трафика*; * Тема 10. *Осуществление фильтрации перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/ запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.**	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями. Разработка базовой программной и технической архитектуры и формулирование предложений по их модернизации. Анализ деятельности предприятия/подразделения, определение методов и средств повышения эффективности обработки и защиты информации. Сбор и изучение научно-практического материала по разделам ВКР, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР. Проведение анализа и обобщения научно-технической информации по теме ВКР. Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Подготовка отчета.	
ПМ. 03 Защита информации техническими средствами МДК.03.01 Техническая защита информации МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		144
Тема 1. Установка, монтаж и настройка технических средств защиты информации; Тема 2. Техническое обслуживание технических средств защиты информации;	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями.	

Тема 3. Применение основных типов технических средств защиты информации; Тема 4. Выявление технических каналов утечки информации; Тема 5. Участие в мониторинге эффективности технических средств защиты информации; Тема 6. Диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; Тема 7. Проведение 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; Тема 8. Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; Тема 9. Установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты; *Тема 10. Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок; ** *Тема 11. Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам.**	Разработка базовой программной и технической архитектуры и формулирование предложений по их модернизации. Анализ деятельности предприятия/подразделения, определение методов и средств повышения эффективности обработки и защиты информации. Сбор и изучение научно-практического материала по разделам ВКР, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР. Проведение анализа и обобщения научно-технической информации по теме ВКР. Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Подготовка отчета.	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение

Производственная практика проходит в организациях, с которыми заключены договоры о проведении практики.

- Федеральная служба государственной статистики по г. Москве (Мосгорстат), Договор № 01/2012 от 03.09.2012;
- ФГУП «НПП «Пульсар», Договор № ДИР/4740 от 01.07.2014;
- ФГБУ «Транспортный комбинат «Россия» Управления делами Президента, Договор № 01/2015 от 15.06.2015;
- ЗАО «Научно-производственный центр информационных региональных систем», Договор № 3/2015 от 25.10.2015;
- ООО Самсунг Электроникс, Договор №и 4/2015 от 28.10.2015;
- ООО «ЦЛОТ «Здоровье», Договор №6/2015 от 01.11.2015;
- ФБУ Российский федеральный центр судебной экспертизы при Министерстве юстиции РФ, Договор № 02/2015 от 08.09.2015;
- Аппарат Совета депутатов муниципального округа «Аэропорт», Договор №76-СР/2016 от 30.12.2016;
- ООО «Дело Системы», Договор № 01/КИП-18/67а-СР/2018 от 09.01.2018;
- ООО «Такском», Договор №02/2013 от 09.04.2013;
- По гарантийным письмам и договорам о проведении практики обучающимся от предприятий.

Для прохождения производственной практики организациями предоставляются автоматизированные рабочие места с программным обеспечением, соответствующим профилю профессионального модуля производственной практики.

Руководство практикой осуществляется преподавателями профессионального цикла.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения производственной практики осуществляются с использованием следующих форм и методов: 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). В результате освоения производственной практики в рамках профессионального модуля студенты проходят промежуточную аттестацию в форме дифференцированного зачёта.

Результаты обучения (освоенные умения, практический опыт в рамах вида деятельности)	**Формы и методы контроля и оценки результатов обучения**
Вид деятельности: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
Иметь практический опыт: – установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; – эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении, *контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации*;* – *администрирования автоматизированных систем в защищенном исполнении информационной системы 1С: Предприятие;** – *установки и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности*;* – *обнаружения и устранения ошибок при передаче данных в компьютерных сетях*;* – *работы с протоколами разных уровней*.* **Уметь:** - осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	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)

– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности – *обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения**; – *устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами**; – *формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;** – *создавать, редактировать и обслуживать автоматизированную систему управления предприятием на базе «1С: Предприятие»;** – *проверять правильность передачи данных.**	
Вид деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
Иметь практический опыт: – установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации**; – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе; – *применения технологии фильтрации различных видов трафика*; * – *осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.** **Уметь:** – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты 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)

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации, *проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;* – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; – *оформлять эксплуатационную документацию программно аппаратных средств защиты информации;* * *- определять цели и задачи в изучении проекта;* * *-разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;* *- осуществлять установку, развёртывание, настройку и использованием DLP-систем.* *	
Вид деятельности: Защита информации техническими средствами	
Иметь практический опыт: – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим	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)

конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок;* * – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от 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; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, *технических средств защиты акустической речевой информации от утечки по техническим каналам**; – применять инженерно-технические средства физической защиты объектов информатизации, – *производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов .**	