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» 06 2021г.

РАБОЧАЯ ПРОГРАММА

производственной практики (преддипломной)
по специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

2021 г.

Рабочая программа производственной практики (преддипломной) разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 №15553.Зарегистрирован Министерством Юстиции Российской Федерации 26.12.2016, регистрационный № 44938

Организация-социальный партнер: ЗАО "ОКБ САПР"

Разработчики: Демкина Н.И., к.э.н., преподаватель 1КК Колледжа информатики и программирования, Володин С.М., к.т.н, преподаватель ВКК Колледжа информатики и программирования, Поколодина Е.В., к.э.н., доцент, преподаватель 1КК Колледжа информатики и программирования,

Рецензент: Солдатов А.Б. - старший менеджер отдела по работе с ключевыми клиентами Департамента продаж Коммерческой дирекции Общества с ограниченной ответственностью «РусБИТех-Астра» ГК Astra Linux

Рабочая программа рассмотрена и рекомендована к утверждению на заседании предметной (цикловой комиссии) обеспечения информационной безопасности автоматизированных систем
Протокол № 10 от 14.05 2021г.

Председатель ПЦК _____ С.М. Володин

Рабочая программа рассмотрена и одобрена Методическим советом Колледжа информатики и программирования Финансового университета при Правительстве Российской Федерации. Протокол № 3 от 24.06 2021г.

Согласована: Каннер Т.М., руководитель учебного центра ЗАО "ОКБ САПР"

М.П. от 24.06 2021г.

РЕЦЕНЗИЯ
на рабочую программу производственной практики (преддипломной)
специальности среднего профессионального образования (СПО)
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа производственной практики (преддипломной) разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа производственной практики (преддипломной) направлена на углубление первоначального практического опыта студента, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности.

Содержание представленной на рецензирование рабочей программы включает в себя следующие разделы:

1. Общая характеристика рабочей программы производственной практики (преддипломной)
2. Структура и содержание производственной практики (преддипломной)
3. Условия реализации производственной практики (преддипломной)
4. Контроль и оценка результатов освоения производственной практики (преддипломной)

В рабочей программе производственной практики (преддипломной) определены цель и планируемые результаты освоения программы. Структура и содержание программы раскрывает последовательность этапов подготовки к выпускной квалификационной работе. Объём часов соответствует учебному плану. В разделе 3 перечислены предприятия – партнеры Финансового университета, профиль деятельности которых соответствует специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. В разделе 4 определены формы и методы контроля результатов обучения, требования к отчетной документации.

Представленная на рецензирование рабочая программа соответствует ФГОС по специальности и рекомендуется для использования в учебном процессе при подготовке обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рецензент: Солдатов А.Б. - старший менеджер отдела по работе с ключевыми клиентами Департамента продаж Коммерческой дирекции Общества с ограниченной ответственностью «РусБИТех-Астра» ГК Astra Linux

«24» 06 2021 Солдатов А.Б.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРСИТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Цель и планируемые результаты освоения программы производственной практики (преддипломной)

- направлена на углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы.

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. В результате прохождения производственной (преддипломной) 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* (06.033 А/01.5); - эксплуатации компонентов систем защиты информации автоматизированных систем, *их диагностике, устранении отказов и восстановлении работоспособности, контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации* (06.033 А/01.5); - диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении; - *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 (на примере конкретного стека протоколов: TCP/IP)*.*

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* (06.032 A/03.05); – устанавливать*, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами* (06.032 A/02.05); – 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, *типовые уязвимости программного обеспечения, методы их эксплуатации и порядок обеспечения безопасности информации при эксплуатации программного обеспечения* (06.032 A/03.05); – принципы разработки алгоритмов программ, основных приемов программирования, *особенности источников угроз, связанных с эксплуатацией программного обеспечения* (06.032 A/03.05);

	– модели баз данных, *порядок настройки систем управления базами данных и средств электронного документооборота* (06.032 А/03.05); – *эксплуатационную и проектную документацию, регламенты по уничтожению информации и машинных носителей информации автоматизированной системы* (06.033 А/02.05, А/03.5); – принципы построения, физические основы работы периферийных устройств, – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации (06.032 А/02.05); – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях, *порядок обеспечения безопасности информации при эксплуатации компьютерных сетей* (06.032 А/02.05); - принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – принципы *построения и функционирования современных операционных систем, примеры их реализаций;** – состав *программно-аппаратных средств обеспечения информационной безопасности в типовых операционных системах;** – адресацию *в сетях, организацию межсетевого 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 и настройки программных средств защиты информации (06.032 А/01.5) в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации (06.032 А/01.5); − 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* (06.033 A/02.5) − 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 (06.032 A/01.5); − 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* (06.032 A/01.5); − 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 (06.033 A/03.5); − применять средства гарантированного уничтожения 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* (06.032 A/01.5); − *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 автоматизированных системах (06.033 A/01.5), 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 (06.033 A/01.5); − основные понятия криптографии и типовых криптографических методов и средств защиты информации; *общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации (*06.033 A/01.5), − 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 (06.033 A/01.5); − *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; − 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(06.034 А/01.5)*;* − *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам(06.034 А/02.5)*.*
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 (06.034 А/02.5);*

	− 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 (06.034 А/01.5)*.* − *составлять план работы, тезисы доклада (выступления), конспекты лекций, первоисточников;* − *работать с источниками учебной информации, пользоваться ресурсами библиотеки (в том числе электронными), образовательными ресурсами сети Интернет, в том числе с учетом имеющихся ограничений здоровья;* − *выступать с докладом или презентацией перед аудиторией, вести дискуссию и аргументированно отстаивать собственную позицию**
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; − основные способы физической защиты объектов информатизации; − *порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации* (06.034 А/01.5)*;

	− *нормативно правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации* (06.034 А/01.5)*; − номенклатуру применяемых средств *защиты информации от несанкционированной утечки по техническим каналам** и физической защиты объектов информатизации. (06.034 А/01.5) − *особенности интеллектуального труда студента на различных видах аудиторных занятий;* − *основы методики самостоятельной работы**.

1.2. Количество часов, отводимое на освоение производственной практики (преддипломной)

Всего часов 144 часа - 4 недели**.**

1. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Структура производственной (преддипломной) практики

Коды профессиональных и общих компетенций	Код и наименование профессиональных модулей	Виды работ	Наименование тем практики	Количество часов
1	2	3	4	5
ОК.1 - ОК.11 ПК 1.1- 1.4	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Выполнение 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 Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием	- установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. - администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении. - обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями	144

			эксплуатационной документации. -проверка технического состояния, техническое обслуживание и текущий ремонт, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении.	
ОК.1 - ОК.11 ПК 2.1- 2.6	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Выполнение 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 Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием	- установка и настройка отдельных программных, программно-аппаратных средств защиты информации. - защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. - тестирование функций отдельных программных и программно-аппаратных средств защиты информации. - обработка, хранение и передача информации ограниченного доступа. - уничтожение информации и носителей информации с использованием	

			программных и программно-аппаратных средств. - регистрация основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
ОК.1 - ОК.11 ПК 3.1- 3.5	ПМ.03 Защита информации техническими средствами	Выполнение 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 Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР	- установка, монтаж, настройка и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. - эксплуатация технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	

		Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием	- измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. - измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. - организация отдельных работ по физической защите объектов информатизации.	

1.2. Тематический план и содержание производственной (преддипломной) практики

Профессиональные модули и междисциплинарные курсы, темы	Содержание практики	Объём часов
1	2	3
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	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	144
МДК 01.01 Операционные системы		
Тема 1. Свойства операционных систем		
Тема 2. Безопасность операционных систем		

Тема 3. Особенности работы в современных операционных системах	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. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием.	
МДК 01.02 Базы данных		
Тема 1. Проектирование баз данных		
Тема 2. Организация баз данных		
Тема 3. Управление базой данных с помощью SQL		
Тема 4. Организация распределённых баз данных		
Тема 5 Администрирование и безопасность		
МДК 01.03 Сети и системы передачи информации		
Тема 1. Сети передачи данных		
МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		
Тема 1. Разработка защищенных автоматизированных (информационных) систем		
Тема 2. Эксплуатация защищенных автоматизированных систем.		
МДК 01.05 Эксплуатация компьютерных сетей		
Тема 1. Передача данных в компьютерных сетях		
Тема 2. Технологии коммутации и маршрутизации современных сетей Ethernet		
Тема 3. Межсетевые экраны		
ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	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.	
МДК 02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности		
Тема 1. Защита автономных автоматизированных систем		
Тема 2. Защита информации в локальных сетях		
Тема 3. Защита информации в сетях общего доступа		

Тема 4. Защита информации в базах данных	Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием.	
Тема 5. Мониторинг систем защиты		
МДК 02.02 Криптографические средства и методы защиты информации		
Тема 1. Классическая криптография		
Тема 2. Современная криптография		
МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности		
Тема 1. Защита корпоративной информации с использованием автоматизированных систем контроля информационных потоков		
ПМ. 03 Защита информации техническими средствами	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. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием.	
МДК 03.01 Техническая защита информации		
Тема 1. Физические основы технической защиты информации		
Тема 2. Системы защиты от утечки информации		
Тема 3. Применение и эксплуатация технических средств защиты информации		
МДК 03.02 Инженерно-технические средства физической защиты информации		
Тема 1. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2. Применение и эксплуатация инженерно-технических средств физической защиты		
МДК 03.03 Физические основы защиты информации		
Тема 1. Физические принципы утечки и защиты информации		
Тема 2. Радио- и электросвязь		
Тема 3. Защита информации		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

3.1. Материально-техническое обеспечение

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

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

Для прохождения производственной практики (преддипломной) организациями предоставляются автоматизированные рабочие места с необходимым оборудованием и программным обеспечением.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Контроль и оценка результатов освоения производственной (преддипломной) 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 (преддипломной) 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 (06.033 A/01.5); - эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности, контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации (06.033 A/01.5); - диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении; - 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 (на примере конкретного стека протоколов: TCP/IP)*. **Уметь:** - осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;	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)

- 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 (06.032 A/03.05); – устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами (06.032 A/02.05); – 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 и настройки программных средств защиты информации (06.032 A/01.5) в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации (06.032 A/01.5); − 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 (06.033 A/02.5) − работы с подсистемами регистрации событий; − выявления событий и инцидентов безопасности в автоматизированной системе;	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)

− применения технологии фильтрации различных видов трафика, **Уметь:** − 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.* − устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями (06.032 A/01.5); − 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 (06.032 A/01.5); − 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 (06.033 A/03.5); − применять средства гарантированного уничтожения 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 (06.032 A/01.5); − 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.* - особенности и способы применения программных и программно-аппаратных средств защиты информации в автоматизированных системах (06.033 A/01.5), 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 (06.033 A/01.5);	

− основные понятия криптографии и типовых криптографических методов и средств защиты информации; общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации (06.033 А/01.5), − 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 (06.033 А/01.5); − 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; − установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты;	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)

− технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок(06.034 A/01.5)*; − технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам(06.034 A/02.5)*. **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 (06.034 A/02.5); − 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 (06.034 A/01.5)*. − составлять план работы, тезисы доклада (выступления), конспекты лекций, первоисточников; − работать с источниками учебной информации, пользоваться ресурсами библиотеки (в том числе электронными), образовательными ресурсами сети Интернет, в том числе с учетом имеющихся ограничений здоровья; − выступать с докладом или презентацией перед аудиторией, вести дискуссию и аргументированно отстаивать собственную позицию*	