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

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

2021 г.

Рабочая программа учебной практики 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: Володин С.М.- к.т.н. преподаватель ВКК, Маринич А.Л. – преподаватель ІКК, Поколодина Е.В. – к.э.н., преподаватель ІКК, Рой А.В. – к.т.н. преподаватель ІКК, Филатов А.П.- преподаватель ІКК, Мирецкая Е.А.- методист ВКК.

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 учебной практики
по специальности среднего профессионального образования (СПО)
10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

Рабочая программа учебной практики 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 учебной практики направлена на формирование у обучающихся умений и приобретение первоначального практического опыта, соответствует требованиям к результатам освоения профессиональных модулей: ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении (УП 01.01) – 3 нед., 108 ч.; ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами (УП 02.01) – 3 нед., 108 ч.; ПМ.03 Защита информации техническими средствами (УП.03.01) – 2 нед., 72 ч.; ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (УП 04.01) – 3 нед., 108 ч.

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

1. Общая характеристика рабочей программы учебной практики
2. Структура и содержание учебной практики
3. Условия реализации учебной практики
4. Контроль и оценка результатов освоения учебной практики

В рабочей программе учебной практики определены цель и планируемые результаты освоения программы. Структура и содержание программы раскрывает последовательность прохождения тем практики, соответствует тематическому плану, объём часов также соответствует учебному плану. Материально-техническое оснащение, представленное в разделе 3 соответствует ФГОС по специальности. В разделе 4 определены формы и методы контроля результатов обучения.

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 2021г. Солдатов А.Б.

СОДЕРЖАНИЕ стр.

1. ОБЩАЯ ХАРАКТЕРСИТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ 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
ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

1.1. Цель и планируемые результаты освоения программы учебной 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

- выполнение работ по рабочей профессии 16199 Оператор электронно-вычислительных и вычислительных машин.

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
ОК07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК09.	Использовать информационные технологии в профессиональной деятельности.
ОК10.	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.
ПМ.04	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

1.1.3. В результате прохождения учебной практики 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 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; -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 A/03.05); – *эксплуатационную и проектную документацию, регламенты по уничтожению информации и машинных носителей информации автоматизированной системы* (06.033 A/02.05, A/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 A/02.05); – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях, *порядок обеспечения безопасности информации при эксплуатации компьютерных сетей* (06.032 A/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 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; – *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*.*
Вид деятельности: Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.	

Иметь практический опыт	-выполнения требований техники безопасности при работе с вычислительной техникой; -организации рабочего места оператора электронно-вычислительных и вычислительных машин (06.032 А/01.5); -подготовки оборудования компьютерной системы к работе; -инсталяции, настройки и обслуживания программного обеспечения компьютерной системы (06.032 А/01.5); -управления файлами; -применения офисного программного обеспечения в соответствии с прикладной задачей; -использования ресурсов локальной вычислительной сети; -использования ресурсов, технологий и сервисов Интернет; -применения средств защиты информации в компьютерной системе.
Уметь:	-выполнять требования техники безопасности при работе с вычислительной техникой; -производить подключение блоков персонального компьютера и периферийных устройств; -производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; -диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; выполнять инсталляцию системного и прикладного программного обеспечения (06.032 А/01.5); -создавать и управлять содержимым документов с помощью текстовых процессоров; -создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; -создавать и управлять содержимым презентаций с помощью редакторов презентаций; - использовать мультимедиа проектор для демонстрации презентаций; - вводить, редактировать и удалять записи в базе данных; - эффективно пользоваться запросами базы данных; -создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; -производить сканирование документов и их распознавание; -производить распечатку, копирование и тиражирование документов на принтере и других устройствах; -управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; -осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; -осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; -осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ (06.032 А/01.5); осуществлять резервное копирование и восстановление данных (06.033 А/03.5).
Знать:	-требования техники безопасности при работе с вычислительной техникой;

	-основные принципы устройства и работы компьютерных систем и периферийных устройств (06.033 А/01.5); -классификацию и назначение компьютерных сетей; -виды носителей информации; -программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета (06.033 А/01.5); -основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым.

1.2. Количество часов на освоение рабочей программы учебной практики:

Всего 396 часов, в том числе:
в рамках освоения ПМ.01 (УП 01.01) – 2 нед., 108 ч.;
в рамках освоения ПМ.02 (УП 02.01) – 3 нед., 108 ч.;
в рамках освоения ПМ.03 (УП.03.01) – 2 нед., 72 ч.;
в рамках освоения ПМ.04 (УП 04.01) – 3 нед., 108 ч.;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Структура учебной практики

Коды профессиональных и общих компетенций	Код и наименования профессиональных модулей	Количество часов по ПМ	Виды работ	Наименование тем учебной практики	Количество часов по темам
ПК 1.2. ПК 1.3 ПК 1.4 ОК. 01-ОК.11	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении: УП.01	**108**	**Раздел1** Установка программного обеспечения в соответствии с технической документацией. Настройка параметров работы программного обеспечения, включая системы управления базами данных. Настройка компонентов подсистем защиты информации операционных систем. Управление учетными записями пользователей. Работа в операционных системах с соблюдением действующих требований по защите информации. Установка обновления программного обеспечения. Контроль целостность подсистем защиты информации операционных систем. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных Использование программных средств для архивирования информации	Тема 1. Работа с учетными записями пользователей и группами. Настройка квот Тема 2. Создание новой базы данных Тема 3. Работа с учетными записями пользователей и группами. Основа мандатного управления доступом. Тема 4. Настройка параметров мандатного управления доступом и мандатного контроля целостности. Тема 5. Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности. Тема 6. Администрирование ОССН в рамках реализации мандатного контроля целостности Тема 7. Настройка механизмов организации программной среды. Контроль целостности КСЗ. Тема 8. Развертывание стенда. Настройка DNS Сервера. Тема 9. Конфигурирование службы Astra Linux Directory.	**36** 2 4 2 4 4 4 4 4 2

			Обеспечение безопасности в операционных системах семейства Windows. *Обеспечение безопасности в операционных системах семейства Linux* *Защита информации с использованием технологии виртуализации*	Тема 10. Управление программными пакетами. Настройка системных служб. Тема 11. Настройка защищенного режима работы ОССН в соответствии с Astra Linux Red-Book.	4 2
			Раздел 2 - *Разработка системы бизнес приложений для пяти операционных систем в единой IDE*.* - *Изучение domain-specific language (DLE)-предметно – ориентированного языка 1С:Предприятие*.* *Разработка автоматизированной системы торговой компании.** *Автоматизация выставления счетов на продажу товаров: ввод, хранение, печать документов*.* *Ввод, хранение и печать накладных на отгрузку товаров*.* *Создание отчетов по продажам товаров, в табличном виде и в виде диаграмм*.* Проведение аудита защищенности автоматизированной системы. Установка, настройка и эксплуатация сетевых операционных систем. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. Организация работ с удаленными хранилищами данных и базами данных. Организация защищенной передачи данных в компьютерных сетях. Выполнение монтажа компьютерных сетей,	Тема 1. Разработка системы бизнес приложений для пяти операционных систем в единой IDE. Тема 2. Разработка автоматизированной системы торговой компании. Тема 3.Установка, настройка и эксплуатация сетевых операционных систем. Тема 4.Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. Тема 5. Организация работ с удаленными хранилищами данных и базами данных. Тема 6. Организация защищенной передачи данных в компьютерных сетях. Тема 7. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Тема 8. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. Тема 9. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	**72** 6 12 6 6 6 6 12 12 6

			организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		
ПК 2.4, ПК 2.6. ОК. 01-ОК.11	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами: УП.02.01	**108**	**Раздел 1** Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Составление документации по учету, обработке, хранению и передаче конфиденциальной информации Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	Тема 1. Программные и программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах. Тема 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Тема 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Тема 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Тема 5. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов,	**58** 6 6 6 6 6

			Устранение замечаний по результатам проверки Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. Применение математических методов для оценки качества и выбора наилучшего программного средства Проведение аудита информационной безопасности *Применение ОС Kali Linux для тестирования информационной системы на проникновение** *Установка и настройка ОС Astra Linux**	помещений, программ, алгоритмов. Устранение замечаний по результатам проверки Тема 6. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. Тема 7. Применение математических методов для оценки качества и выбора наилучшего программного средства Тема 8. Проведение аудита информационной безопасности Тема 9. Применение ОС Kali Linux для тестирования информационной системы на проникновение. Тема 10. Установка и настройка ОС Astra Linux	6 6 4 6 6

			Раздел 2 Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи *Исследование алгоритмов современных зарубежных симметричного шифров FEAL, IDEA, RC4, RC5, RC6. Их программная реализация и современные методы криптоанализа** *Исследование алгоритмов современных отечественных симметричного шифров Магма и Кузнечик. Их программная реализация и современные методы криптоанализа** *Исследование алгоритмов хэширования MD4, MD5, SHA-1, SHA-2 и SHA-256. Применение функций хэширования в ЭЦП и аутентификации сообщений на примере Kerberos** *Изучение квантовых методов в криптографии. Квантовые методы криптоанализа и программная реализация квантовых алгоритмов на примере алгоритма факторизации Шора**	Тема 1. Типовые криптографические средства и методы защиты информации, в том числе и электронной подписи Тема 2. Алгоритмы современных зарубежных симметричного шифров FEAL, IDEA, RC4, RC5, RC6. Тема 3. Алгоритмы современных отечественных симметричного шифров Магма и Кузнечик. Тема 4 Алгоритмы хэширования MD4, MD5, SHA-1, SHA-2 и SHA-256. Применение функций хэширования в ЭЦП и аутентификации сообщений на примере Kerberos. Тема 5. Квантовые методы криптоанализа и программная реализация квантовых алгоритмов на примере алгоритма факторизации Шора.	**25** 6 6 4 5 4
			Раздел 3 Проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его;	Тема 1. Комплекс технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его;	**25** 4

			Проведение всего цикла работ по установке, развёртыванию, настройке, использованию DLP-систем; Разработка политик информационной безопасности; Применение технологий фильтрации различных видов трафика; Фильтрация перехваченного трафика для поиска найденных инцидентов; Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности; Диагностика работоспособности системы; Подготовка отчета о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой); Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.	Тема 2. Цикл работ по установке, развёртыванию, настройке, использованию DLP-систем; Тема 3. Разработка политик информационной безопасности; Тема 4. Технологии фильтрации различных видов трафика; Тема 5. Диагностика работоспособности системы; Тема 6. Гостевые виртуальные машины и практическая работа с ними с использованием современных гипервизоров; Тема 7. Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.	4 4 2 3 4 4
ПК.3.1-ПК.3.5 ОК.01-ОК.11	ПМ.03 Защита информации техническими средствами: УП.03.01	**72**	**Раздел1** Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок.	Тема 1.Измерение параметров физических полей. Тема 2. Определение каналов утечки ПЭМИН. Тема 2. Измерение параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Тема 3. Установка и настройка технических средств защиты информации.	**47** 6 6 6 6

			Проведение аттестации объектов информатизации. *Осуществление электромагнитного экранирования различными способами*.* *Выбор электромагнитных экранов *.* *Расчет основных параметров экрана*.* *Расчет и инструментальный контроль показателей защиты информации различными средствами измерения при инструментальном контроле*.*	Тема 4. Измерения параметров побочных электромагнитных излучений и наводок. Тема 5. Аттестация объектов информатизации. Тема 6. Электромагнитное экранирование различными способами. Тема 7. Выбор электромагнитных экранов. Расчет основных параметров экрана. Тема 8. Расчет и инструментальный контроль показателей защиты информации различными средствами измерения при инструментальном контроле.	6 4 3 4 6
			Раздел 2 Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по	Тема 1. Монтаж различных типов датчиков. Тема 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Тема 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Тема 4. Система контроля и управления доступом. Тема 5. Принципы работы системы видеонаблюдения и ее проектирование. Тема 6. Датчики периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Тема 7. Реализация защиты от утечки по цепям электропитания и заземления. Тема 8. Разработка организационных и технических мероприятий по заданию преподавателя;	**25** 2 4 4 2 2 2 4 3 2

			инженерно-технической защите информации.	Тема 9. Разработка основной документации по инженерно-технической защите информации.	
ПК.4.1-ПК.4.4 ОК. 01-ОК.11	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	**108**	**Раздел 1.** Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения	Тема 1.Работа с устройствами компьютерной системы Тема 2.Работа с программным обеспечением компьютерной системы Тема 3.Диагностика неисправностей системы, ведение документации	**28** 8 10 10
			Раздел 2 Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах	Тема 1.Работа в текстовом процессоре Тема 2.Работа в редакторе электронных таблиц Тема 3.Работа в программе подготовки и просмотра презентаций Тема 4.Работа в системе управления базами данных Тема 5.Работа в графических редакторах	**56** 16 16 8 8 8
			Раздел 3 Использование ресурсов технологий и сервисов Интернета	Тема 1.Работа с ресурсами Интернета	**10**
			Раздел 4. Обеспечение защиты информации в компьютерной системе	Тема 1. Защита информации при работе с офисными приложениями	**14**

2.2 Тематический план и содержание учебной 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 МДК.01.05. Эксплуатация компьютерных сетей		**108**
Раздел 1. Тема 1. Работа с учетными записями пользователей и группами. Настройка квот Тема 2. Создание новой базы данных Тема 3. Работа с учетными записями пользователей и группами. Основа мандатного управления доступом. Тема 4. Настройка параметров мандатного управления доступом и мандатного контроля целостности. Тема 5. Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности. Тема 6. Администрирование ОССН в рамках реализации мандатного контроля целостности Тема 7. Настройка механизмов организации программной среды. Контроль целостности КСЗ. Тема 8. Развертывание стенда. Настройка DNS Сервера. Тема 9. Конфигурирование службы Astra Linux Directory. Тема 10. Управление программными пакетами. Настройка системных служб. Тема 11. Настройка защищенного режима работы ОССН в соответствии с Astra Linux Red-Book.	Администрирование локальных учётных записей пользователей и групп в ОССН с использованием командной строки и графического интерфейса Создание новой базы данных Администрирование локальных учётных записей пользователей и групп в ОССН на основе мандатного управления доступом Администрирование основных параметров мандатного управления доступом и мандатного контроля целостности в ОССН с применением графических утилит и консольных команд Настройка мандатного управления доступом и мандатного контроля целостности к каталогам файловой системы ОССН для совместной работы от имени учётных записей пользователей с различными уровнями доступа с документами (файлами) с различными уровнями конфиденциальности Администрирование основных параметров мандатного управления доступом в ОССН с применением графических утилит и консольных команд при активированном мандатном контроле целостности Изучение принципов и технологий контроля целостности данных (в том числе, комплекса средств защиты — КСЗ), реализованных в ОССН.	

	Решение задач подсчёта контрольных сумм файлов и оптических носителей, контроля соответствия дистрибутиву, регламентного контроля целостности и создания замкнутой программной среды. Настройка DNS-сервера Установка и настройки параметров службы Astra Linux Directory (ALD) в ОССН Администрирование пакетов ОССН, в том числе используемых для этого команд и графических утилит, а также особенности настройки системных служб (демонов). Настройка безопасной конфигурации компьютера для работы с ОССН в соответствии с Astra Linux Red-Book	
Раздел2. Тема 1. Разработка системы бизнес приложений для пяти операционных систем в единой IDE. Тема 2. Разработка автоматизированной системы торговой компании. Тема 3.Установка, настройка и эксплуатация сетевых операционных систем. Тема 4.Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. Тема 5. Организация работ с удаленными хранилищами данных и базами данных. Тема 6. Организация защищенной передачи данных в компьютерных сетях. Тема 7. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Тема 8. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.	Разработка системы бизнес приложений для пяти операционных систем в единой IDE. Изучение domain-specific language (DLE)-предметно – ориентированного языка 1С:Предприятие. Разработка автоматизированной системы торговой компании. Автоматизация выставления счетов на продажу товаров: ввод, хранение, печать документов. Ввод, хранение и печать накладных на отгрузку товаров. Создание отчетов по продажам товаров, в табличном виде и в виде диаграмм. Проведение аудита защищенности автоматизированной системы. Установка, настройка и эксплуатация сетевых операционных систем. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. Организация работ с удаленными хранилищами данных и базами данных. Организация защищенной передачи данных в компьютерных сетях. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	

Тема 9. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		
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		**108**
Раздел1 Тема 1. Программные и программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах. Тема 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Тема 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Тема 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Тема 5. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. Устранение замечаний по результатам проверки Тема 6. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. Тема 7. Применение математических методов для оценки	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. Устранение замечаний по результатам проверки. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. Применение математических методов для оценки качества и выбора наилучшего программного средства. Проведение аудита информационной безопасности. Применение ОС Kali Linux для тестирования информационной системы на проникновение.Установка и настройка ОС Astra Linux	

качества и выбора наилучшего программного средства Тема 8. Проведение аудита информационной безопасности Тема 9. Применение ОС Kali Linux для тестирования информационной системы на проникновение. Тема 10. Установка и настройка ОС Astra Linux		
Раздел 2 Тема 1. Типовые криптографические средства и методы защиты информации, в том числе и электронной подписи Тема 2. Алгоритмы современных зарубежных симметричного шифров FEAL, IDEA, RC4, RC5, RC6. Тема 3. Алгоритмы современных отечественных симметричного шифров Магма и Кузнечик. Тема 4 Алгоритмы хэширования MD4, MD5, SHA-1, SHA-2 и SHA-256. Применение функций хэширования в ЭЦП и аутентификации сообщений на примере Kerberos. Тема 5. Квантовые методы криптоанализа и программная реализация квантовых алгоритмов на примере алгоритма факторизации Шора.	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи. Исследование алгоритмов современных зарубежных симметричного шифров FEAL, IDEA, RC4, RC5, RC6. Их программная реализация и современные методы криптоанализа. Исследование алгоритмов современных отечественных симметричного шифров Магма и Кузнечик. Их программная реализация и современные методы криптоанализа. Исследование алгоритмов хэширования MD4, MD5, SHA-1, SHA-2 и SHA-256. Применение функций хэширования в ЭЦП и аутентификации сообщений на примере Kerberos. Изучение квантовых методов в криптографии. Квантовые методы криптоанализа и программная реализация квантовых алгоритмов на примере алгоритма факторизации Шора	
Раздел 3 Тема 1. Комплекс технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; Тема 2. Цикл работ по установке, развёртыванию, настройке, использованию DLP-систем; Тема 3. Разработка политик информационной безопасности; Тема 4. Технологии фильтрации различных видов трафика; Тема 5. Диагностика работоспособности системы; Тема 6. Гостевые виртуальные машины и практическая работа с ними с использованием современных гипервизоров; Тема 7. Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.	Проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; Проведение всего цикла работ по установке, развёртыванию, настройке, использованию DLP-систем; Разработка политик информационной безопасности; Применение технологий фильтрации различных видов трафика; Фильтрация перехваченного трафика для поиска найденных инцидентов; Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности; Диагностика работоспособности системы; Подготовка отчета о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой); Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.	

ПМ.03 Защита информации техническими средствами МДК.03.01 Техническая защита информации МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации МДК 03.03 Физические основы защиты информации		**72**
Раздел 1 Тема 1.Измерение параметров физических полей. Тема 2. Определение каналов утечки ПЭМИН. Тема 2. Измерение параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Тема 3. Установка и настройка технических средств защиты информации. Тема 4. Измерения параметров побочных электромагнитных излучений и наводок. Тема 5. Аттестация объектов информатизации. Тема 6. Электромагнитное экранирование различными способами. Тема 7. Выбор электромагнитных экранов. Расчет основных параметров экрана. Тема 8. Расчет и инструментальный контроль показателей защиты информации различными средствами измерения при инструментальном контроле.	Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Осуществление электромагнитного экранирования различными способами. Выбор электромагнитных экранов. Расчет основных параметров экрана. Расчет и инструментальный контроль показателей защиты информации различными средствами измерения при инструментальном контроле.	
Раздел 2. Тема 1. Монтаж различных типов датчиков. Тема 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Тема 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Тема 4. Система контроля и управления доступом. Тема 5. Принципы работы системы видеонаблюдения и ее проектирование.	**Раздел 2** Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по	

Тема 6. Датчики периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Тема 7. Реализация защиты от утечки по цепям электропитания и заземления. Тема 8. Разработка организационных и технических мероприятий по заданию преподавателя; Тема 9. Разработка основной документации по инженерно-технической защите информации.	цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации.	
ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих		**108**
Тема 1.1.Работа с устройствами компьютерной системы Тема 1.2.Работа с программным обеспечением компьютерной системы Тема 1.3. Диагностика неисправностей системы, ведение документации Тема 2.1. Работа в текстовом процессоре Тема 2.2. Работа в редакторе электронных таблиц Тема 2.3. Работа в программе подготовки и просмотра презентаций Тема 2.4. Работа в системе управления базами данных Тема 2.5. Работа в графических редакторах Тема 3.1. Работа с ресурсами Интернета Тема 4.1. Защита информации при работе с офисными приложениями Промежуточная аттестация по учебной практике	Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка Установка и замена расходных материалов для принтеров, ксерокса, плоттера. Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ Сканирование текстовых документов и их распознавание Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов Форматирование и редактирование документов в текстовом процессоре.	

	Работа с таблицами в текстовом процессоре. Работа с диаграммами в текстовом процессоре. Работа с графическими объектами в текстовом процессоре. Печать документов в текстовом процессоре. Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице Работа со встроенными функциями в электронной таблице Работа со списками в электронной таблице Создание форм для ввода данных в таблицы Создание и работа с диаграммами и графиками Обмен данными между текстовым процессором и электронной таблицей Построение презентации различными способами Обработка объектов слайдов презентации Настройка анимации объектов Настройка показа и демонстрация результатов работы средствами мультимедиа Ввод данных в таблицы базы данных Создание простых запросов без параметров и с параметрами. Создание отчетов Рисование объектов средствами графического редактора. Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики. Работа с эффектами программе векторной графики. Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики. Создание и обмен письмами электронной почты.	

	Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов. Пересылка и публикация файлов данных в Интернете Использование штатных средств защиты операционной системы и прикладных программ. Применение парольной защиты. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение

Лаборатория информационных технологий, программирования и баз данных

Специализированная мебель:
Стол студенческий одноместный – 26 шт.
Стулья компьютерные – 26 шт.
Стол (учительский) – 1 шт.
Стул (учительский) – 1 шт.
Доска (меловая) – 1 шт.
Технические средства обучения:
Компьютер студенческий – 25 шт.
Компьютер преподавателя – 1 шт.
Перечень лицензионного программного обеспечения:
1) Антивирусная защита: ESET NOD32
2) Windows, Microsoft Office
3) Project Expert, Microsoft SQL Server, Microsoft Visual Studio, 1С Предприятие (учебная версия), Консультант Плюс
Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет

Лаборатория сетей и систем передачи информации

Специализированная мебель:
Стол студенческий двухместный – 22 шт.
Стол студенческий одноместный – 25 шт.
Стулья студенческие –67 шт.
Стол (учительский) – 1 шт.
Стул (учительский) – 1 шт.
Доска меловая – 1 шт.
Технические средства обучения:
Компьютер студенческий – 15 шт.
Компьютер преподавателя – 1 шт.
Мультимедиа-проектор - 1 шт.
Экран с электроприводом – 1 шт.
Колонки для воспроизведения аудио – 1 шт.

Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет
Перечень лицензионного программного обеспечения:
1) Антивирусная защита: ESET NOD32
2) Windows, Microsoft Office

3) Microsoft Visio, Microsoft Project, Microsoft SQL Server, Microsoft Visual Studio, 1С Предприятие (учебная версия), эмуляторы активного сетевого оборудования, программное обеспечение сетевого оборудования
Комплект учебно-наглядных пособий. Плакаты, стенды

Лаборатория программных и программно-аппаратных средств защиты информации
Специализированная мебель:
Стол студенческий двухместный – 14 шт.
Стол студенческий одноместный – 20 шт.
Стулья студенческие – 48 шт.
Стол (учительский) – 1 шт.
Стул (учительский) – 1 шт.
Доска меловая – 1 шт.
Технические средства обучения:
Компьютер студенческий – 18 шт.
Компьютер преподавателя – 1 шт.
Мультимедиа-проектор - 1 шт.
Экран – 1 шт.
Колонки для воспроизведения аудио – 1 шт.
Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет
Перечень лицензионного программного обеспечения:
1) Антивирусная защита: ESET NOD32
2) Windows, Microsoft Office
3) Microsoft Visio, Microsoft Project, Microsoft SQL Server, Microsoft Visual Studio, 1С Предприятие (учебная версия)
Комплект учебно-наглядных пособий, плакатов, программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности, программные и программно-аппаратные средства обнаружения вторжений, средства уничтожения остаточной информации в запоминающих устройствах,
программные средства выявления уязвимостей в АС и СВТ,
программные средства криптографической защиты информации,
программные средства защиты среды виртуализации.

Лаборатория технических средств защиты информации
Специализированная мебель:
Стол студенческий двухместный – 17 шт.
Стол студенческий одноместный – 3 шт.
Стулья студенческие – 29 шт.
Стол (учительский) – 1 шт.
Стул (учительский) – 1 шт.
Доска меловая – 1 шт.

Шкаф – 1 шт.
Тумба – 1 шт.
Технические средства обучения:
Компьютер студенческий – 8 шт.
Компьютер преподавателя – 1 шт.
Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет
Перечень лицензионного программного обеспечения:
1) Антивирусная защита: ESET NOD32
2) Windows, Microsoft Office
3) Microsoft Visio, Microsoft Project, Microsoft SQL Server, Microsoft Visual Studio, 1С Предприятие (учебная версия)
Комплект учебно-методической документации, тематические папки дидактических материалов, приборы и оборудование для проведения наглядных и практических занятий: аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок, средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.), стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов, система акустических и виброакустических помех. Многофункциональный поисковый прибор, Рентгенметры, Дозиметр индивидуальный
*Оснащение специализированного кабинета для инвалидов: посадочных мест, специализированные регулируемые столы, рабочее место преподавателя, проектор, экран, персональный компьютер, звукоусилительная система.

Компьютерный класс
Специализированная мебель:
Стол студенческий одноместный – 15 шт.
Стулья студенческие - 21 шт.
Стол (учительский) – 1 шт.
Стул (учительский) – 1 шт.
Технические средства обучения:
Компьютер студенческий – 15 шт.
Компьютер преподавателя – 1 шт.
Мультимедиа-проектор - 1 шт.
Интерактивная доска – 1 шт.
Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет
Перечень лицензионного программного обеспечения:
1) Антивирусная защита: ESET NOD32
2) Windows, Microsoft Office

3) Microsoft Visio, Microsoft Project, Microsoft SQL Server, Microsoft Visual Studio, 1С Предприятие (учебная версия)
Комплект учебно-наглядных пособий:
Образцы различных комплектующих системного блока (включая:
материнские платы, процессоры, видео карты, сетевые карты, блоки питания, оперативную память, специальные платы)
Стенды по устройству принтеров (матричный, струйный, лазерный, цветной лазерный)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляются руководителем практики в процессе проведения практики, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ. В результате освоения учебной практики в рамках профессионального модуля студенты проходят промежуточную аттестацию в форме дифференцированного зачёта

Результаты обучения (освоенные умения (практический опыт) в рамках ВД)	**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 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)*.*	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике. Дифференцированный зачет
- **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.**	
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; – *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*	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике. Дифференцированный зачет

*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.**	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике. Дифференцированный зачет
Вид деятельности - Защита информации техническими средствами	
иметь практический опыт: – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации;	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике.

− 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)*.*	Дифференцированный зачет
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*	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике. Дифференцированный зачет

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**	
Вид деятельности: Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.	
иметь практический опыт: выполнения требований техники безопасности при работе с вычислительной техникой; -организации рабочего места оператора электронно-вычислительных и вычислительных машин (06.032 А/01.5); -подготовки оборудования компьютерной системы к работе; -инсталяции, настройки и обслуживания программного обеспечения компьютерной системы (06.032 А/01.5); -управления файлами; -применения офисного программного обеспечения в соответствии с прикладной задачей; -использования ресурсов локальной вычислительной сети; -использования ресурсов, технологий и сервисов Интернет; -применения средств защиты информации в компьютерной системе.	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике. Дифференцированный зачет
уметь: -выполнять требования техники безопасности при работе с вычислительной техникой; -производить подключение блоков персонального компьютера и периферийных устройств; -производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; -диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; выполнять инсталляцию системного и прикладного программного обеспечения (06.032 А/01.5); -создавать и управлять содержимым документов с помощью текстовых процессоров; -создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; -создавать и управлять содержимым презентаций с помощью редакторов презентаций;	Наблюдение за деятельностью обучающегося на учебной практике. Оценка деятельности обучающегося на учебной практике. Дифференцированный зачет

- использовать мультимедиа проектор для демонстрации презентаций; - вводить, редактировать и удалять записи в базе данных; - эффективно пользоваться запросами базы данных; -создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; -производить сканирование документов и их распознавание; -производить распечатку, копирование и тиражирование документов на принтере и других устройствах; -управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; -осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; -осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; -осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ (06.032 A/01.5); осуществлять резервное копирование и восстановление данных (06.033 A/03.5).	