Тамбовское государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

Предметно-цикловая комиссия информационных технологий

Астахова Наталия Вениаминовна

Digitally signed by Астахова Наталия Вениаминовна
Date: 2023.11.23 21:27:18 +03'00'

Утверждаю:
Директор ТОГАПОУ «Тамбовский бизнес-колледж»
_____ **Н.В. Астахова**
Приказ № 59 от 28.08.2023 г

ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика»

**(ПМ.1 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ;
ПМ.2 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМ И И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ;
ПМ3. ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ;
ПМ.4. ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ: ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН.**

среднее профессиональное образование
(программа подготовки специалистов среднего звена)

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Тамбов 2023

Лист согласования программы учебной практики
УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика»
(ПМ.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
ПМ.2 Защита информации в автоматизированных системах программным и программно-аппаратными средствами;
ПМ3. Защита информации техническими средствами;
ПМ.4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: оператор электронно-вычислительных и вычислительных машин.

Программа учебной практики УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика» относится к профессиональному циклу основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации.

Программа учебной практики УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика» может быть использована для прохождения дисциплин специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации, изучаемых в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

Организация разработчик:

Тамбовское областное государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

Разработчики:

Машков С.Н. – преподаватель высшей категории ТОГАПОУ «Тамбовский бизнес-колледж».

Чуриков Д.В., – преподаватель ТОГАПОУ «Тамбовский бизнес-колледж».

Программа учебной практики рассмотрена и рекомендована на заседании ПЦК информационных технологий.

Протокол №1 от «28» августа 2023 г.

Аннотация

УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика»
(ПМ.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
ПМ.2 Защита информации в автоматизированных системах программным и программно-аппаратными средствами;
ПМ3. Защита информации техническими средствами;
ПМ.4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: оператор электронно-вычислительных и вычислительных машин.

Цели и задачи учебной практики:

Целью учебной практики является получение обучающимися навыков:

– эксплуатация автоматизированных (информационных) систем в защищенном исполнении;

– защита информации в автоматизированных системах программным и программно-аппаратными средствами;

– защита информации техническими средствами;

– выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: «Оператор электронно-вычислительных и вычислительных машин».

Задачи учебной практики:

– овладение навыками проектирования, разработки и эксплуатации информационных систем в защищенном исполнении; защита информации техническими средствами;

– овладение навыками обработки текстовой, числовой информации и графической информации с помощью современного программного обеспечения;

– формирование у обучающихся умений применять современные информационные технологии для решения задач профессиональной деятельности.

Место учебной практики в структуре ООП

Данная дисциплина относится к профессиональному циклу в структуре ООП среднего профессионального образования по специальности СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», квалификация – техник по защите информации, в части освоения основных видов профессиональной деятельности:

ПМ.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;

МДК 1.1 Эксплуатация подсистем безопасности автоматизированных систем;

МДК 1.2 Эксплуатация компьютерных систем;

ПМ.2 Защита информации в автоматизированных системах программным и программно-аппаратными средствами;

МДК 2.1 Программное и программно-аппаратные средства обеспечения информационной безопасности;

МДК 2.2 Криптографические средства и методы защиты информации;

ПМ3. Защита информации техническими средствами.

МДК 3.1 Применение инженерно-технических средств обеспечения информационной безопасности;

ПМ4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: Оператор электронно-вычислительных и вычислительных машин.

МДК 4.1 Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники.

В результате прохождения учебной практики студент должен:

иметь практический опыт в:

– управлении процессом разработки приложений с использованием инструментальных средств;

– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;

– администрировании автоматизированных систем в защищенном исполнении;

– установке компонентов систем защиты информации автоматизированных информационных систем.

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

– выявлении технических каналов утечки информации;

– применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;

– проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

уметь:

– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку

автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;

– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;

– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– 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.

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;

– применять инженерно-технические средства физической защиты объектов информатизации.

знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ, основных приемов программирования;

– модели баз данных;

– принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического

обслуживания вычислительной техники и других технических средств информатизации;

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации.

– 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;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;

– основные способы физической защиты объектов информатизации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

Прохождение учебной практики направлено на достижение общеобразовательных, воспитательных и практических задач, на подготовку грамотных специалистов в области информационных технологий, на дальнейшее развитие личностных способностей и дальнейшего профессионального роста выпускника-будущего специалиста.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа учебной практики УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика» относится к профессиональному циклу основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации.

Программа может быть использована для изучения в учреждениях среднего профессионального образования, реализующих образовательную программу среднего профессионального образования, при подготовке квалифицированных специалистов среднего звена

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ:

Код и название компетенций	МДК	Компоненты, составные части ОК
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 1. Выбор способов решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 2. Поиск, анализ и интерпретация информации, необходимой для выполнения задач профессиональной деятельности
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 3. Планирование и реализация собственного профессиональное и личностного развития.
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 4. Уметь работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК5. Уметь осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 6. Формирование гражданско-патриотической позиции, осознанного поведения на основе общечеловеческих ценностей
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 7. Сохранение окружающей среды, ресурсосбережение, эффективные действия в чрезвычайных ситуациях
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 8 Поддержание необходимого уровня физической подготовленности для профессиональной деятельности, сохранение и укрепление здоровья
ОК 9. Использовать информационные технологии в профессиональной деятельности	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Использование информационных технологий в профессиональной деятельности
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ОК 9. Использование профессиональной документацией на государственном и иностранном языках
ПК 1.1. Производить установку и настройку компонентов	1.1 – 1.2 2.1 – 2.2	ПК 1.1. Установка, настройка, комплектование,

автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	3.1, 4.1	конфигурирование автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ПК 1.2. Администрирование автоматизированных систем, конфигурирование, настройка компонент систем защиты информации автоматизированных систем; установка, адаптация и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ПК 1.3. Эксплуатация компонентов систем защиты информации автоматизированных систем, поиск и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	ПК 1.4. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Установка и настройка отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Обработка, хранение и передача информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Уничтожение информации и носителей 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.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Регистрация основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Установка, монтаж, настройка 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.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	Эксплуатация 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.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	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.	1.1 – 1.2 2.1 – 2.2 3.1, 4.1	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 – 1.2 2.1 – 2.2 3.1, 4.1	Работы по физической защите объектов информатизации.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика»
(ПМ.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
ПМ.2 Защита информации в автоматизированных системах программным и программно-аппаратными средствами;
ПМ3. Защита информации техническими средствами;
ПМ.4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: оператор электронно-вычислительных и вычислительных машин.

1.1. Область применения программы

Программа учебной практики УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика» относится к профессиональному циклу основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации.

Программа учебной практики УП.1.01, УП.2.01, УП3.01, УП.4.01 «Учебная практика» может быть использована для прохождения дисциплин специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации, изучаемых в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

1.2. Место практики в структуре основной профессиональной образовательной программы.

Учебная практика относится к профессиональному циклу основной профессиональной образовательной программы среднего профессионального образования по специальности СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» в части освоения основных видов профессиональной деятельности:

ПМ.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;

МДК 1.1 Эксплуатация подсистем безопасности автоматизированных систем;

МДК 1.2 Эксплуатация компьютерных систем;

ПМ.2 Защита информации в автоматизированных системах программным и программно-аппаратными средствами;

МДК 2.1 Программное и программно-аппаратные средства обеспечения информационной безопасности;

МДК 2.2 Криптографические средства и методы защиты информации;

ПМ3. Защита информации техническими средствами.

МДК 3.1 Применение инженерно-технических средств обеспечения информационной безопасности;

ПМ4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: Оператор электронно-вычислительных и вычислительных машин.

МДК 4.1 Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники.

.

1.3. Цели и задачи практики – требования к результатам освоения практики:

Целью учебной практики является получение обучающимися навыков:

– эксплуатация автоматизированных (информационных) систем в защищенном исполнении;

– защита информации в автоматизированных системах программным и программно-аппаратными средствами;

– защита информации техническими средствами;

– выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: «Оператор электронно-вычислительных и вычислительных машин».

– овладение навыками проектирования, разработки и эксплуатации информационных систем в защищенном исполнении; защита информации техническими средствами;

– овладение навыками обработки текстовой, числовой информации и графической информации с помощью современного программного обеспечения;

– формирование у обучающихся умений применять современные информационные технологии для решения задач профессиональной деятельности.

В результате прохождения учебной практики студент должен:

иметь практический опыт в:

– управлении процессом разработки приложений с использованием инструментальных средств;

– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;

– администрировании автоматизированных систем в защищенном исполнении;

– установке компонентов систем защиты информации автоматизированных информационных систем.

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

– выявлении технических каналов утечки информации;

– применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;

– проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

уметь:

– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;

– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;

– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– 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.

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;

– применять инженерно-технические средства физической защиты объектов информатизации.

знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ, основных приемов программирования;

– модели баз данных;

– принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации.

– 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;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;

– основные способы физической защиты объектов информатизации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

Прохождение учебной практики направлено на достижение общеобразовательных, воспитательных и практических задач, на подготовку грамотных специалистов в области информационных технологий, на дальнейшее развитие личностных способностей и дальнейшего профессионального роста выпускника-будущего специалиста.

1.4. Рекомендуемое количество часов на освоение программы практики:

УП.1.01 – всего – **36** часов, в том числе:
- максимальной учебной нагрузки обучающегося – 36 часов, включая:
- обязательной аудиторной учебной нагрузки обучающегося –36 часов;
- практической работы обучающегося – 36 часов;

УП.2.01 – всего – **36** часов, в том числе:
- максимальной учебной нагрузки обучающегося – 36 часов, включая:
- обязательной аудиторной учебной нагрузки обучающегося –36 часов;
- практической работы обучающегося – 36 часов;

УП.3.01 – всего – **36** часов, в том числе:
- максимальной учебной нагрузки обучающегося – 36 часов, включая:
- обязательной аудиторной учебной нагрузки обучающегося –36 часов;
- практической работы обучающегося – 36 часов;

УП.4.01 – всего **288** часов, в том числе:
- максимальной учебной нагрузки обучающегося – 288 часов, включая:
- обязательной аудиторной учебной нагрузки обучающегося –288 часов;
- практической работы обучающегося – 288 часов;

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом учебной практики является освоение:
общих (ОК) компетенций:

Код	Наименование результата обучения
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках

профессиональных (ПК) компетенций:

Вид профессиональной деятельности	Код	Наименование результатов практики
ПМ.1 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.2 Защита информации в автоматизированных системах программным 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
ПМ3. 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.4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: Оператор электронно-вычислительных и вычислительных машин		Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.
		Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности
		Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения
		Участвовать в экспериментальном тестировании информационной системы на этапе опытной эксплуатации, фиксировать выявленные ошибки кодирования в разрабатываемых модулях информационной системы.
		Разрабатывать фрагменты документации по эксплуатации информационной системы.
		Участвовать в оценке качества и экономической эффективности информационной системы.
		Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.

		Консультировать пользователей информационной системы и разрабатывать фрагменты методики обучения пользователей информационной системы
		Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.
		Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.
		Участвовать в разработке технического задания.
		Программировать в соответствии с требованиями технического задания.
		Применять методики тестирования разрабатываемых приложений.
		Формировать отчетную документацию по результатам работ
		Формировать отчетную документацию по результатам работ.
		Оформлять программную документацию в соответствии с принятыми стандартами.
		Использовать критерии оценки качества и надежности функционирования информационной системы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

2.1. Тематический план учебной практики

Коды формируемых компетенций	Наименование профессионального модуля	Объем времени, отводимый на практику (час.,нед.)	Сроки проведения
ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5	ПМ.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	36 ч аудиторной нагрузки	2 курс 4 семестр
ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5	ПМ.2 Защита информации в автоматизированных системах программным и программно-аппаратными средствами	36 ч аудиторной нагрузки	3 курс 6 семестр
ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5	ПМ.3. Защита информации техническими средствами	36 ч аудиторной нагрузки	4 курс 8 семестр
ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5	ПМ4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: Оператор электронно-вычислительных и вычислительных машин.	288 ч аудиторной нагрузки	2 курс 3 семестр, 4 семестр
Текущая аттестация проходит в форме д. зачета. Итоговая аттестация в форме квалификационного экзамена по модулю			
Итого 396 часов			

3.2. Содержание учебной практики УП.04.01 «Учебная практика (Оператор электронно-вычислительных и вычислительных машин)

ТЕМАТИКА УЧЕБНЫХ ЗАНЯТИЙ		**288**	
МДК.4.1 ОБСЛУЖИВАНИЕ АППАРАТНОГО ОБЕСПЕЧЕНИЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ, СЕРВЕРОВ, ПЕРИФЕРИЙНЫХ УСТРОЙСТВ, ОБОРУДОВАНИЯ И КОМПЬЮТЕРНОЙ ОРГТЕХНИКИ 3 семестр		**108**	
Тема 4.1.1. Установка и подключение основных устройств ПК.	Содержание	40	
	1. Установка основных устройств на рабочем месте 2. Подключения основных устройств 3. Установка периферийных устройств на рабочем месте 4. Подключения периферийных устройств 5. Разборка системного блока 6. Сборка системного блока 7. Снятие и установка блока питания 8. Подключение блока питания 9. Снятие и установка материнской платы 10. Снятие и установка процессора 11. Снятие и установка видеокарты 12. Снятие и установка оперативной памяти 13. Снятие и установка кулера и радиатора системы охлаждения ПК 14. Подключение карт расширения 15. Правила эксплуатации системы охлаждения и карт расширения. 16. Снятие, установка и подключение оптических приводов 17. Снятие, установка и подключение жесткого диска.		3
Тема 4.1.2. Техническое обслуживание системного блока, клавиатуры, мыши	Содержание	18	
	1. Профилактика системного блока. Проверка всех рабочих параметров системного блока 2. Оптимизация внутреннего пространства системного блока 3. Диагностика / тестирование системного блока 4. Поиск простых неисправностей в работе оборудования 5. Устранение простых неисправностей в работе оборудования 6. Проверка работоспособности блок питания 7. Проверка подключения блок питания 8. Снятие и установка кулера и радиатора системы охлаждения ПК		3
Тема 4.1.3.	Содержание	18	

Техническое обслуживание оргтехники.	1. Техническое обслуживание сканера 2. Техническое обслуживание телефонных станций 3. Техническое обслуживание принтера 4. Заправка картриджей. 5. Восстановление картриджей. 6. Техническое обслуживание картриджей лазерных принтеров		3
Тема 4.1.4. Организация локальной сети.	Содержание	28	
	1. Организация топологии «кольцо» 2. Организация топологии «звезда» 3. Организация смешанной топологии 4. Подготовка локального кабеля 5. Монтаж локальной сети 6. Обжим конвекторов 7. Распиновка розеток и патч-панелей 8. Установка розеток 9. Настройка рабочей группы 10. Настройка домена 11. Настройка сетевых адресов 12. Настройка доступа		3
Промежуточная аттестация		4	
МДК.4.1 ОБСЛУЖИВАНИЕ АППАРАТНОГО ОБЕСПЕЧЕНИЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ, СЕРВЕРОВ, ПЕРИФЕРИЙНЫХ УСТРОЙСТВ, ОБОРУДОВАНИЯ И КОМПЬЮТЕРНОЙ ОРГТЕХНИКИ 4 семестр		**178**	
Тема 4.1.5. Работа с системой BIOS	Содержание	6	
	1. Загрузка и настройка параметров системы BIOS 2. Изучение параметров настройки BIOS 3. Обновление прошивки BIOS		3
Тема 4.1.6. Обслуживание жесткого диска.	Содержание	10	
	1. Загрузка и работа с HDD программ комплексом Hirens 2. Ремонт и проверка секторов HDD программным комплексом HDD Regenerator 3. Проверка и ремонт HDD программным комплексом Victoria 4. Проверка и ремонт HDD программным комплексом MHDD 5. Подготовка HDD к установке ОС разметка диска.		3

Тема 4.1.7. Установка и настройкаОС Windows	Содержание	16	
	1. Установка ОС Windows различных версий 2. Настройка интерфейса ОС Windows различных версий 3. Установка драйверов в Windows различных версий		3 3 3
Тема 4.1.8. Безопасность, обновления, защита в ОС Windows	Содержание	6	
	1. Настройка параметров безопасности ОС Windows 2. Установка и настройка антивирусных программ 3. Обновления ОС Windows настройка параметров		3
Тема 4.1.9. Установка пакетов прикладных программ и утилит в ОС Windows	Содержание	10	
	Установка пакета кодеков и плеера для воспроизведения видео		3
	Поиск и установка ПО для записи DVD дисков с открытым кодом		3
	Установка и настройка пакетов MS Office		3
	Установка и настройка пакетов Open Office		3
	Установка и настройка браузера		3
Тема 4.1.10. Применение служебных программ и стороннего ПО для оптимизации работы ОС Windows	Содержание	10	
	Применение служебных программ ОС Windows для оптимизации работы		3
	Применение сторонних программ для оптимизации ОС Windows		3
	Работа с диспетчером устройств. Работа с диспетчером задач изучение процессов Windows		3
	Изменение размера раздела диска без потери информации		3
	Изменение размера и типа диска программой Acronis Disk Director		3
Тема 4.1.11. Сохранение и восстановление ОС Windows и пользовательской информации	Содержание	16	
	Настройка центра восстановления Windows		3
	Создание образа диска программой Acronis True Images		3
	Восстановление раздела из образа программой Acronis True Images		3
	Создание резервной области в программе Acronis True Images		3
	Восстановление ОС Windows с применением центра восстановления ОС Windows 10		3
	Восстановление информации с повреждённых носителей HDD		3
	Восстановление информации со съёмных носителей		3
	Восстановление поврежденной информации		3
Тема 1. Информация и информационные технологии	Содержание	2	
	Организация хранения информации на дисковом пространстве ПК.		3
	Содержание	6	

Тема 2. Правила подготовки и оформления информационного контента	Поиск и сохранение информации Оформление информации согласно требованиям Редактирование и форматирование документа		3
Тема 3. Правила допечатной обработки информационного контента	Содержание	2	
	Изучение требований к редактированию и форматированию документа		3
Тема 4. Текстовые процессоры. Работа с текстовыми документами	Содержание	8	
	Редактирование текста в ячейке Редактирование и форматирование таблиц. Редактирование и форматирование диаграмм Редактирование и форматирование графических объектов Форматирование сложных документов		3
Тема 5 Текстовые процессоры. Работа с деловой документацией Защита документов и файлов.	Содержание	4	
	Создание и форматирование деловой документации Защита документов и файлов средствами ОС Windows и сторонним программным обеспечением		3
Тема 6. Разработка и создание веб - страницы в среде MS Word	Содержание		
	Разработка и создание документа в среде MS Word Создание веб - страницы в среде MS Word	2	3
Тема 7. Табличные процессоры. Приемы работы с электронными таблицами	Содержание	4	
	Создание электронной книги. Создание и переименование листов книги		3
Тема 8. Ввод данных. Редактирование и форматирование таблиц.	Содержание	4	
	Ввод данных различного рода. Редактирование и форматирование данных различного рода. Редактирование и форматирование таблиц.		3
Тема 9. Вставка диаграмм. Редактирование и форматирование диаграмм.	Содержание	4	
	Вставка диаграмм в MS Excel. Редактирование и форматирование диаграмм.		3
Тема 10. Применение расчетов по формулам	Содержание	4	
	Ввод в ячейку таблицы формул различного рода. Применение расчетов по формулам. Расчет заработной платы сотрудников средствами MS Excel.		3
Тема 11. Применение формул и функций при расчетах.	Содержание	6	
	Ввод в ячейку таблицы формул и функций различного рода.		3

	Работа с Мастером функций MS Excel. Применение расчетов по формулам и функциям MS Excel.		
Тема 12. Проектирование и реализация многотабличных баз данных	Содержание	6	
	Проектирование и реализация однотабличных баз данных Проектирование и реализация многотабличных баз данных Установка связей при реализация многотабличных баз данных		3
Тема 13. Приемы работы с базами данных.	Содержание	4	
	Установка ключевых полей. Заполнение таблиц. Редактирование текста в таблицах Редактирование данных и структуры таблиц в мастере Конструктор таблиц.		3
Тема 14. Создание запросов многотабличных баз данных	Содержание	2	
	Конфигурирование и создание запросов однотабличных баз данных Конфигурирование и создание запросов многотабличных баз данных		3
Тема 15. Создание форм многотабличных баз данных	Содержание	6	
	Конфигурирование и создание форм однотабличных баз данных Конфигурирование и создание форм многотабличных баз данных с помощью мастера Конфигурирование и создание форм многотабличных баз данных с помощью конструктора форм		3
Тема 16. Создание отчетов многотабличных баз данных	Содержание	2	
	Конфигурирование и создание отчетов многотабличных баз данных с помощью мастера отчетов		3
Тема 17. Создание презентации.	Содержание	2	
	Создание презентации с помощью мастера презентаций Создание презентации с помощью слайдов		3
Тема 18. Обработка графической информации	Содержание	2	
	Создание графической информации в различных приложениях Обработка графической информации в различных приложениях Преобразование формата графической информации		
Тема 9. Основные визуальные компоненты прикладных программ.	Содержание	4	
	Основные визуальные компоненты прикладных программ.		3
Тема 10. Организация подпрограмм.	Содержание	4	
	Организация подпрограмм.		3
Тема 11. Основы объектно-ориентированного программирования.	Содержание	4	
	Основы объектно-ориентированного программирования.		3

Тема 12. ООП. Конструкторы и деструкторы.	Содержание	4	
	ООП. Конструкторы и деструкторы.		3
Тема 13. Создание модулей пользователя	Содержание	4	
	Создание модулей пользователя		3
Тема 14. Обработка исключительных ситуаций	Содержание	4	
	Обработка исключительных ситуаций		3
Тема 15. Файловый ввод-вывод в C++	Содержание	4	
	Файловый ввод-вывод в C++		3
Тема 16. Сетевое взаимодействие на основе сокетов	Содержание	4	
	Сетевое взаимодействие на основе сокетов		3
Тема 17. Общие правила конструирования интерфейсов	Содержание	4	
	Общие правила конструирования интерфейсов		3
МДК.1.2 ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СИСТЕМ 4 семестр		**36**	
Тема 1.2.1 Передача информации по типовым каналам связи	Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала Телекоммуникационные среды Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ. Основные элементы и стандарты беспроводных сетей. Принципы функционирования систем сотовой связи. Спутниковые системы передачи данных	10	
Тема 1.2.2 Разработка защищенных автоматизированных информационных систем	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании) Задачи и этапы проектирования автоматизированных систем в защищенном исполнении Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Анализ угроз безопасности информации Построение модели угроз Управление доступом Регистрация событий безопасности	10	

	Резервное копирование и восстановление данных Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн		
Тема 1.2.3 Эксплуатация защищенных автоматизированных систем	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении Организация администрирования автоматизированных систем. Управление, тестирование и эксплуатация автоматизированных систем Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам Установка и настройка СЗИ от НСД Защита входа в систему (идентификация и аутентификация пользователей) Настройка контроля целостности и замкнутой программной среды Использование принтеров для печати конфиденциальных документов. Контроль печати Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	10	
Тема 1.2.4 Безопасность компьютерных сетей	Установка, настройка и эксплуатация сетевых операционных систем. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетево 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.	6	
МДК.1.1 ЭКСПЛУАТАЦИЯ ПОДСИСТЕМ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ 6 семестр		**12**	
Тема 1.1.1 Элементы теории операционных систем. Свойства операционных систем	Работа в консольном и графическом режимах Виртуальные машины. Создание, модификация, работа Установка ОС Создание и изучение структуры разделов жесткого диска Мониторинг за использованием памяти Наблюдение за использованием ресурсов системы Изучение штатных средств защиты информации в операционных системах	6	
Тема 1.1.2 Основы теории баз данных	Проектирование инфологической модели данных Проектирование базы данных с использованием CASE-средств	6	

	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL Управление доступом к объектам базы данных Резервное копирование и восстановление баз данных		
МДК.2.1 ПРОГРАММНОЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6 семестр		**12**	
Тема 2.1.1 Основные принципы программной и программно-аппаратной защиты информации	Изучение нормативных правовых актов, нормативных методических документов, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами Идентификация и аутентификация пользователей Криптографическая защита. Обзор программ шифрования данных Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	6	
Тема 2.1.2 Защита автономных автоматизированных систем	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) Применение специализированного программно средства для восстановления удаленных файлов Применение программ для безвозвратного удаления данных Применение программ для шифрования данных на съемных носителях	6	
МДК.2.2 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 6 семестр		**12**	
Тема 2.2.1 Математические основы защиты информации	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений Проверка чисел на простоту	4	
Тема 2.2.2 Классическая криптография	Применение классических шифров замены Применение классических шифров перестановки Применение метода гаммирования Криптоанализ шифра простой замены методом анализа частотности символов Криптоанализ классических шифров методом полного перебора ключей	4	

	Криптоанализ шифра Вижинера Применение методов генерации ПСЧ		
Тема 2.2.3 Современная криптография	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4 Применение различных асимметричных алгоритмов Изучение программной реализации асимметричного алгоритма RSA Применение различных функций хеширования, анализ особенностей хешей Изучение программно-аппаратных средств, реализующих основные функции ЭП	4	
МДК.3.1 ПРИМЕНЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 8 семестр		**36**	
Тема 3.1.1 Концепция инженерно-технической защиты информации	Измерение параметров физических полей Защита от утечки по акустическому каналу Защита от утечки по виброакустическому каналу Защита от утечки по цепям электропитания и заземления	12	
Тема 3.1.2 Основные компоненты комплекса инженерно-технических средств физической защиты	Монтаж датчиков пожарной и охранной сигнализации Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя Рассмотрение принципов устройства, работы и применения средств видеонаблюдения Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации	12	
Тема 3.1.3 Применение и эксплуатация инженерно-технических средств физической защиты	Управление системой телевизионного наблюдения с автоматизированного рабочего места Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты	12	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы учебной практики предполагает наличие:

Учебных кабинетов:

– программирования и баз данных

– информационных систем;

Лабораторий:

– архитектуры вычислительных систем;

– технических средств информатизации;

Оборудования:

– экран,

– программное обеспечение,

– выход в Интернет.

Технических средств обучения:

– компьютеры,

– мультимедийный проектор,

– сканер,

– принтер,

– видеокамера,

– фотоаппарат.

4.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Нормативные правовые акты:

1 Доктрина информационной безопасности Российской Федерации (утв.9 сентября 2000 года Президентом Российской Федерации В.В. Путиным).

2 Федеральный закон об информации, информационных технологиях и защите информации (Принят Гос. Думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года, Редакция от 25.11.2017 (с изм. и доп., вступ. в силу с 01.01.2018)

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

Основные источники:

1. Михеева Е.В. Информационные технологии в профессиональной деятельности: учебное пособие для студентов среднего профессионального образования – 7-е издание. – М.: «Академия», 2011 г. -384 с

2. Михеева Е.В. Практикум по информационным технологиям в профессиональной деятельности: учебное пособие для студентов среднего профессионального образования – 7-е издание – М.: «Академия», 2011 г. -256 с.

3. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

5. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

6. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

7. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

8. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

9. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

10. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

11. Богомазова Г.Н. Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования 2015 ОИЦ «Академия»

12. Остроух А.В. Основы информационных технологий 2015 ОИЦ «Академия»

13. Угринович Н.Д. Информатика и ИКТ (профильный уровень) 11 кл. – М. "БИНОМ. Лаборатория знаний" – 2010.

14. Тозик В.Т., Корпан Л.М. Компьютерная графика и дизайн 2014 ОИЦ «Академия»

15. Курилова А.В., Оганесян В.О. Ввод и обработка цифровой информации. Практикум 2015 ОИЦ «Академия»

16. Курилова А.В., Оганесян В.О. Хранение, передача и публикация цифровой информации 2015 ОИЦ «Академия»

17. Максимов, Н. В. Архитектура ЭВМ и вычислительных систем [Электронный ресурс]: учебник для учрежд. СПО/Н.В. Максимов, Т. Л. Партыка, И. И. Попов. Электронные текстовые данные - М.: Издательство Юрайт, 2015 - Гриф УМО СПО - Режим доступа: https://www.biblio-online.ru/book/389866 - ЭБС ЮРАЙТ по паролю.

18. Миленина, С. А. Электроника и схемотехника[Электронный ресурс]: учебник и практикум для СПО / С. А. Миленина ; под ред. Н. К. Миленина. Электронные текстовые данные — М. : Издательство Юрайт, 2017. — 208 с. — Гриф УМО СПО - Режим доступа: https://www.biblio-online.ru/book/3906E501-84A4-4A0D-9D83-54403F783EE5- ЭБС ЮРАЙТ по паролю.

19. Рыбальченко, М. В. Архитектура информационных систем [Электронный ресурс]: учебное пособие для СПО / М. В. Рыбальченко. Электронные текстовые данные — М. : Издательство Юрайт, 2017. — 91 с. — (Профессиональное образование). — Гриф УМО СПО - Режим доступа: https://www.biblio-online.ru/book/F490757C-8BC3-4897-86C7-B54F649CBE93 - ЭБС ЮРАЙТ по паролю.

20. Таненбаум Э., Современные операционные системы. 3-е изд. - СПб.:Питер, 2015. — 1120 с.:

21. А.В. Батаев, Н.Ю. Налютин, С.В. Синицын Операционные системы и среды: учебник для студ. учреждений сред. проф. Образования пособие. – М.: Издательский дом «Академия», 2016. -.272 с.

Дополнительные источники:

22. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

23. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

24. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

25. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

26. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

27. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

28. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

29. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

30. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

31. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

32. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

33. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

34. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

35. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

36. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

37. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

38. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

39. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

40. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

41. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

42. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

43. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

44. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

45. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

46. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

47. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

48. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

49. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

50. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

51. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

52. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

53. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

54. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

55. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

56. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

58. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

59. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

60. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

61. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

62. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

63. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

64. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

65. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

66. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

67. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

68. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

69. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

70. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

71. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

72. в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

73. г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

74. Электронная библиотечная система IPRbooks (http://www.iprbookshop.ru)

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения практики осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения		***Критерии оценки***	***Методы оценки***
Перечень знаний и умений, осваиваемых в рамках практики:	*Выработанные и освоенные компетенции*		
эксплуатация компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5	**Отлично:** – все необходимые умения сформированы полностью, – все предусмотренные программой учебные задания выполнены полностью, без ошибок и в установленные сроки, – оформление отчетной документации полностью соответствует требованиям; тексты не имеют стилистических и грамматических ошибок. **Хорошо:** – все необходимые умения сформированы, – все предусмотренные программой учебные задания выполнены полностью. – оформление отчетной документации соответствует требованиям; – имеются незначительные ошибки в выполненных заданиях; – сроки выполнения заданий не соблюдены; – тексты отчетов имеют стилистические ошибки. **Удовлетворительно:** – необходимые умения сформированы в основном, – все предусмотренные программой учебные задания выполнены в основном. – оформление отчетной документации соответствует требованиям в основном; – имеются ошибки в выполненных заданиях;	устный опрос тестирование выполнение индивидуальных заданий различной сложности оценка ответов в ходе беседы, оценка докладов по тематике подготовка презентаций оценка выполнения лабораторных работ
администрирование автоматизированных систем в защищенном исполнении;	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
установка компонентов систем защиты информации автоматизированных информационных систем	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
установка и настройка программных средств защиты информации;	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
тестирование функций, диагностика, устранение отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
учет, обработка, хранение и передача информации, для которой установлен режим конфиденциальности	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
выявление технических каналов утечки информации;	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
применение, техническое обслуживание, диагностика, устранение отказов, восстановление работоспособности, установка, монтаж и настройка инженерно-технических средств физической защиты и технических средств защиты информации;	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		
проведение измерений параметров ПЭМИН, создаваемых техническими	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6		

Результаты обучения		***Критерии оценки***	***Методы оценки***
Перечень знаний и умений, осваиваемых в рамках практики:	*Выработанные и освоенные компетенции*		
средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; .	ПК 3.1 – ПК 3.5	– сроки выполнения заданий не соблюдены; – тексты отчетов имеют стилистические и грамматические ошибки. **Неудовлетворительно:** – необходимые умения не сформированы, – предусмотренные программой учебные задания не выполнены. – оформление отчетной документации не соответствует требованиям;	
проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	ОК1 – ОК10, ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5		