

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

УП. 01 по ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

УП .02 по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

УП .03 по ПМ.03 Защита информации техническими средствами

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

УП .05 по ПМ.05 Модификация информационных систем

УП .06 по ПМ.06 Осуществление интеграции программных модулей

Обязательный профессиональный блок

2025 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	3
1.2. Планируемые результаты освоения учебной практики	5
1.3. Обоснование часов учебной практики в рамках вариативной части ОПОП-П	9
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	12
2.1. Трудоемкость освоения учебной практики	12
2.2. Структура учебной практики	12
2.3. Содержание учебной практики.....	17
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ..	21
3.1. Материально-техническое обеспечение учебной практики	21
3.2. Учебно-методическое обеспечение	21
3.3. Общие требования к организации учебной практики	26
3.4 Кадровое обеспечение процесса учебной практики.....	26
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	27

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Цель и место учебной практики в структуре образовательной программы:

Рабочая программа учебной практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и реализуется в профессиональном цикле после прохождения междисциплинарных курсов (МДК) в рамках профессиональных модулей в соответствии с учебным планом (п. 5.1. ОПОП-П):

УП.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении МДК 01.05 Эксплуатация компьютерных сетей
УП.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	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
УП.03 Техническая защита информации	ПМ.03 Защита информации техническими средствами	МДК 03.01 Техническая защита информации МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации
УП.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям	МДК 04.01 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин
УП.05 Осуществление модификации информационных систем	ПМ.05 Модификация информационных систем	МДК 05.01 Осуществление модификации информационных систем МДК 05.02 Цифровая экономика в информационных системах
УП.06 Технология разработки программного обеспечения	ПМ.06 Осуществление интеграции программных модулей	МДК 06.01 Технология разработки программного обеспечения

Учебная практика направлена на развитие общих (ОК) и профессиональных компетенций (ПК):

Код ОК / ПК	Наименование ОК / ПК
-------------	----------------------

ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
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.
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.
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 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

ПК 5.3.	Составлять проектную документацию на модификацию информационной системы. Применять полученные знания для решения задач по разработке и модернизации информационной системы
ПК 7.1	Разработка процедур проверки работоспособности и измерения характеристик компьютерного программного обеспечения
ПК 7.2	Разработка тестовых наборов данных для проверки работоспособности компьютерного программного обеспечения
ПК 7.3	Проверка работоспособности компьютерного программного обеспечения

Цель учебной практики: формирование первоначальных практических профессиональных умений в рамках профессиональных модулей данной ОПОП-П по видам деятельности: ВД. 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении; ВД.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами; ВД.03 Защита информации техническими средствами; ВД. 04 Освоение одной или нескольких профессий рабочих, должностей служащих (16199 Оператор электронно-вычислительных и вычислительных машин); ВД.05 Модификация информационных систем; ВД.06 Осуществление интеграции программных модулей и соответствующие ему общие компетенции и профессиональные компетенции.

1.2. Планируемые результаты освоения учебной практики

В результате прохождения учебной практики по видам деятельности, предусмотренным ФГОС СПО и запросам работодателей, обучающийся должен получить практический опыт (сформировать умения):

Наименование вида деятельности	Практический опыт / умения
ВД. 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> <input type="checkbox"/> установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; <input type="checkbox"/> администрирования автоматизированных систем в защищенном исполнении; <input type="checkbox"/> эксплуатации компонентов систем защиты информации автоматизированных систем; <input type="checkbox"/> диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении <p>Уметь:</p> <ul style="list-style-type: none"> <input type="checkbox"/> осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; <input type="checkbox"/> организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; <input type="checkbox"/> осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

	<ul style="list-style-type: none"> <input type="checkbox"/> производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы <input type="checkbox"/> настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; <input type="checkbox"/> обеспечивать работоспособность, обнаруживать и устранять неисправности
<p>ВД.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>	<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> <input type="checkbox"/> установки, настройки программных средств защиты информации в автоматизированной системе; <input type="checkbox"/> обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; <input type="checkbox"/> тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ; <input type="checkbox"/> решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; <input type="checkbox"/> применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; <input type="checkbox"/> учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; <input type="checkbox"/> работы с подсистемами регистрации событий; <input type="checkbox"/> выявления событий и инцидентов безопасности в автоматизированной системе. <p>Уметь:</p> <ul style="list-style-type: none"> <input type="checkbox"/> устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; <input type="checkbox"/> устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; <input type="checkbox"/> диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; <input type="checkbox"/> применять программные и программно-аппаратные средства для защиты информации в базах данных; <input type="checkbox"/> проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; <input type="checkbox"/> применять математический аппарат для выполнения криптографических преобразований; <input type="checkbox"/> использовать типовые программные криптографические средства, в том числе электронную подпись; <input type="checkbox"/> применять средства гарантированного уничтожения информации; <input type="checkbox"/> устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; <input type="checkbox"/> 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
ВД.03 Защита информации техническими средствами	<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> <input type="checkbox"/> установки, монтажа и настройки технических средств защиты информации; <input type="checkbox"/> технического обслуживания технических средств защиты информации; <input type="checkbox"/> применения основных типов технических средств защиты информации; <input type="checkbox"/> выявления технических каналов утечки информации; <input type="checkbox"/> участия в мониторинге эффективности технических средств защиты информации; <input type="checkbox"/> диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; <input type="checkbox"/> 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; <input type="checkbox"/> проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; <input type="checkbox"/> установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. <p>Уметь:</p> <ul style="list-style-type: none"> <input type="checkbox"/> применять технические средства для криптографической защиты информации конфиденциального характера; <input type="checkbox"/> применять технические средства для уничтожения информации и носителей информации; <input type="checkbox"/> применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; <input type="checkbox"/> применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; <input type="checkbox"/> применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; <input type="checkbox"/> применять инженерно-технические средства физической защиты объектов информатизации
ВД. 04 Освоение одной или нескольких профессий рабочих,	Иметь практический опыт:

<p>должностей служащих (16199 Оператор электронно-вычислительных и вычислительных машин)</p>	<ul style="list-style-type: none"> <input type="checkbox"/> выполнения требований техники безопасности при работе с вычислительной техникой; <input type="checkbox"/> организации рабочего места оператора электронно-вычислительных и вычислительных машин; <input type="checkbox"/> подготовки оборудования компьютерной системы к работе; <input type="checkbox"/> инсталляции, настройки и обслуживания программного обеспечения компьютерной системы; <input type="checkbox"/> управления файлами; <input type="checkbox"/> применения офисного программного обеспечения в соответствии с прикладной задачей; <input type="checkbox"/> использования ресурсов локальной вычислительной сети; <input type="checkbox"/> использования ресурсов, технологий и сервисов Интернет; <input type="checkbox"/> применения средств защиты информации в компьютерной системе. <p>Уметь:</p> <ul style="list-style-type: none"> <input type="checkbox"/> выполнять требования техники безопасности при работе с вычислительной техникой; <input type="checkbox"/> производить подключение блоков персонального компьютера и периферийных устройств; <input type="checkbox"/> производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; <input type="checkbox"/> диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; <input type="checkbox"/> выполнять инсталляцию системного и прикладного программного обеспечения; <input type="checkbox"/> создавать и управлять содержимым документов с помощью текстовых процессоров; <input type="checkbox"/> создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; <input type="checkbox"/> создавать и управлять содержимым презентаций с помощью редакторов презентаций; <input type="checkbox"/> использовать мультимедиа проектор для демонстрации презентаций; <input type="checkbox"/> вводить, редактировать и удалять записи в базе данных; <input type="checkbox"/> эффективно пользоваться запросами базы данных; <input type="checkbox"/> создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; <input type="checkbox"/> производить сканирование документов и их распознавание; <input type="checkbox"/> производить распечатку, копирование и тиражирование документов на принтере и других устройствах; <input type="checkbox"/> управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; <input type="checkbox"/> осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; <input type="checkbox"/> осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; <input type="checkbox"/> осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;
--	---

	<input type="checkbox"/> осуществлять резервное копирование и восстановление данных.
ВД.05 Модификация информационных систем	<input type="checkbox"/> Уметь: <input type="checkbox"/> проводить анализ данных и составлять отчетную документацию по результатам анализа; <input type="checkbox"/> разрабатывать проектную документацию на модификацию информационной системы; <input type="checkbox"/> выявлять основные тенденции в развитии современной мировой экономики; <input type="checkbox"/> анализировать последствия управленческих решений в сфере бизнеса в условиях цифровизации экономики; <input type="checkbox"/> осуществлять поиск, анализ и управление информацией в цифровой среде.
ВД.06 Осуществление интеграции программных модулей и соответствующие ему общие компетенции и профессиональные компетенции	<p>Иметь практический опыт:</p> <input type="checkbox"/> разработка процедуры проверки работоспособности компьютерного программного обеспечения; <input type="checkbox"/> разработка процедуры сбора диагностических данных проверки работоспособности компьютерного программного обеспечения; <input type="checkbox"/> разработка процедуры измерения требуемых характеристик компьютерного программного обеспечения; <input type="checkbox"/> оформление технической документации на компьютерное программное обеспечение по заданному стандарту или шаблону; <input type="checkbox"/> оценка и согласование сроков выполнения поставленных задач; <input type="checkbox"/> подготовка тестовых наборов данных в соответствии с выбранной методикой тестирования компьютерного программного обеспечения; <input type="checkbox"/> проверка работоспособности компьютерного программного обеспечения на основе разработанных тестовых наборов данных; <input type="checkbox"/> оценка соответствия компьютерного программного обеспечения требуемым характеристикам; <input type="checkbox"/> сбор и анализ полученных результатов проверки работоспособности компьютерного программного обеспечения.

1.3. Обоснование часов учебной практики в рамках вариативной части ОПОП-П

УП	Код ПК/дополнительные (ПК*, ПКц)	Практический опыт	Наименование темы практики	Объем часов	Обоснование увеличения объема практики
УП. 01	ПК 1.1 ПК 1.2 ПК 1.3 ПК 1.4	Иметь практический опыт: установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; администрирования автоматизированных систем в защищенном исполнении;	Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	16	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в

		эксплуатации компонентов систем защиты информации автоматизированных систем; диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении	Тема 2.2. Администрирование автоматизированных систем Тема 2.4. Защита от несанкционированного доступа к информации Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры		рамках Регионального чемпионата «Профессионалы»
УП. 02	ПК 2.1. ПК 2.2. ПК 2.3 ПК 2.4. ПК 2.5 ПК 2.6	Иметь практический опыт: установки, настройки программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе.	Тема 2.4. Защита программ и данных от несанкционированного копирования Тема 2.5. Защита информации на машинных носителях Тема 2.7. Системы обнаружения атак и вторжений Тема 5.1. Защита информации в базах данных Тема 6.1. Мониторинг систем защиты Тема 3.6. Криптозащита информации в сетях передачи данных	41	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»
УП. 05	ПК 5.3	Уметь: проводить анализ данных и составлять отчетную документацию по результатам анализа; разрабатывать проектную документацию на модификацию информационной системы; выявлять основные тенденции в развитии современной мировой экономики; анализировать последствия управленческих решений в сфере бизнеса в условиях цифровизации экономики;	Тема 1.1. Разработка документации информационных систем Тема 1.2. Отладка и тестирование информационных систем Тема 1.3. Система обеспечения качества информационных систем	36	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»

		осуществлять поиск, анализ и управление информацией в цифровой среде	Тема 1.4. Оценка экономической эффективности информационных систем Тема 2.4 Инструменты коммуникации в цифровой экономике Тема 2.5 Информационная безопасность в цифровой экономике		
УП. 06	ПК 7.1 ПК 7.2 ПК 7.3	Иметь практический опыт: разработка процедуры проверки работоспособности компьютерного программного обеспечения; разработка процедуры сбора диагностических данных проверки работоспособности компьютерного программного обеспечения; разработка процедуры измерения требуемых характеристик компьютерного программного обеспечения; оформление технической документации на компьютерное программное обеспечение по заданному стандарту или шаблону; оценка и согласование сроков выполнения поставленных задач; подготовка тестовых наборов данных в соответствии с выбранной методикой тестирования компьютерного программного обеспечения; проверка работоспособности компьютерного программного обеспечения на основе разработанных тестовых наборов данных; оценка соответствия компьютерного программного обеспечения требуемым характеристикам; сбор и анализ полученных результатов проверки работоспособности компьютерного программного обеспечения.	Тема 2.1.1 Основные понятия и стандартизация требований к программному обеспечению Тема 2.1.2. Описание и анализ требований. Диаграммы IDEF Тема 2.1.3. Оценка качества программных средств Тема 2.2.1 Современные технологии и инструменты интеграции. Тема 2.2.2 Инструментарий тестирования и анализа качества программных средств	72	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»
Всего академических часов учебной практики в рамках вариативной части ОПОП-II -165					

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Трудоемкость освоения учебной практики

Код УП	Объем, ак.ч.	Форма проведения учебной практики (концентрированно/ рассредоточено)	Курс / семестр	Форма промежуточной аттестации
УП. 01	108	рассредоточено	2/4 3/5 3/6	По текущим оценкам
УП. 02	108	рассредоточено	3/5 3/6 4/7	По текущим оценкам
УП. 03	72	рассредоточено	4/7 4/8	По текущим оценкам
УП. 04	36	рассредоточено	2/4	По текущим оценкам
УП. 05	36	рассредоточено	4/8	По текущим оценкам
УП. 06	72	рассредоточено	3/6	По текущим оценкам
Всего УП	432	X	X	X

2.2. Структура учебной практики

Код ПК	Наименование разделов профессионального модуля	Виды работ	Наименование тем учебной практики
УП 01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении			
ПК 1.1 ПК 1.2 ПК 1.3 ПК 1.4	Тема 1.4. Основные меры защиты информации в автоматизированных системах Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении Тема 1.6. Защита информации в распределенных автоматизированных системах Тема 1.7. Особенности разработки информационных систем персональных данных Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении. Тема 2.2. Администрирование автоматизированных систем Тема 2.4. Защита от несанкционированного доступа к информации Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры Тема 3.2. Межсетевые экраны Тема 3.3.	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.	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.

	<p>Системы обнаружения и предотвращения проникновений Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов</p>	<p>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.</p>	<p>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.</p>
<p>УП.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>			
<p>ПК 2.1. ПК 2.2. ПК 2.3 ПК 2.4. ПК 2.5 ПК 2.6</p>	<p>Тема 2.2. Защита программ от изучения Тема 2.3. Вредоносное программное обеспечение Тема 2.4. Защита программ и данных от несанкционированного копирования Тема 2.5. Защита информации на машинных носителях Тема 2.7. Системы обнаружения атак и вторжений Тема 5.1. Защита информации в базах данных Тема 6.1. Мониторинг систем защиты Тема 3.6. Криптозащита информации в сетях передачи данных</p>	<p>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</p>	<p>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</p>

		<p>конфиденциальной информации</p> <p>Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.</p> <p>Устранение замечаний по результатам проверки</p> <p>Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.</p> <p>Применение математических методов для оценки качества и выбора наилучшего программного средства</p> <p>Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи</p>	<p>конфиденциальной информации</p> <p>Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.</p> <p>Устранение замечаний по результатам проверки</p> <p>Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.</p> <p>Применение математических методов для оценки качества и выбора наилучшего программного средства</p> <p>Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи</p>
УП.03 Техническая защита информации			
<p>ПК 3.1.</p> <p>ПК 3.2.</p>	<p>Тема 5.1. Применение технических средств защиты информации</p> <p>Тема 5.2. Эксплуатация технических средств защиты информации</p> <p>Тема 3.1 Применение инженерно-технических средств физической защиты</p> <p>Тема 3.2. Эксплуатация инженерно-технических средств физической защиты</p>	<p>Измерение параметров физических полей.</p> <p>Определение каналов утечки ПЭМИН.</p> <p>Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</p> <p>Установка и настройка технических средств защиты информации.</p> <p>Проведение измерений параметров побочных электромагнитных излучений и наводок.</p> <p>Проведение аттестации объектов информатизации.</p> <p>Монтаж различных типов датчиков.</p> <p>Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.</p> <p>Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.</p> <p>Рассмотрение системы контроля и управления доступом.</p> <p>Рассмотрение принципов работы системы</p>	<p>Измерение параметров физических полей.</p> <p>Определение каналов утечки ПЭМИН.</p> <p>Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</p> <p>Установка и настройка технических средств защиты информации.</p> <p>Проведение измерений параметров побочных электромагнитных излучений и наводок.</p> <p>Проведение аттестации объектов информатизации.</p> <p>Монтаж различных типов датчиков.</p> <p>Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.</p> <p>Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.</p> <p>Рассмотрение системы контроля и управления доступом.</p> <p>Рассмотрение принципов работы системы</p>

		<p>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 инженерно-технической защите информации.</p>	<p>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 инженерно-технической защите информации.</p>
<p>УП.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин</p>			
<p>ПК 4.1. ПК 4.2. ПК 4.3. ПК 4.4.</p>	<p>Тема 1.1. Основы информационных технологий в работе оператора ЭВМ Тема 1.2. Техническое и программное обеспечение информационных технологий Тема 1.3 Особенности обработки текстовой информации Тема 1.4. Особенности обработки экономической и статистической информации Тема 1.5 Оформление служебной документации Тема 1.6 Технологии обработки растровой графики Тема 1.7 Электронные презентации MS PowerPoint Тема 1.8 Технологии обработки аудиоинформации Тема 1.9 Технологии обработки видеоинформации</p>	<p>Создание, форматирование и редактирование документов. Сохранение и открытие документов. Работа со списками и формами документов. Создание и форматирование многоколоночного документа. Создание и импортирование графических объектов в документ. Способы создания таблиц, вычисление в таблицах. Создание сложных документов. Создание математических формул. Форматирование таблиц в ЭТ MS Excel. Создание формул различной сложности. Построение и форматирование диаграмм. Обработка списков: сортировка, фильтрация, консолидация, итоги. Анализ и распределение данных. Создание и настройка слайдов, презентаций, слайд-шоу. Вставка на слайд аудио эффектов, видео, анимации. Использование гиперссылок. Запись и монтаж звука. Улучшение качества звуковой дорожки. Использование эффектов, накладываемых на трек. Выполнение монтажа фильма. Создание различных видеороликов. Установка, настройка, восстановление операционной системы.</p>	<p>Создание, форматирование и редактирование документов. Сохранение и открытие документов. Работа со списками и формами документов. Создание и форматирование многоколоночного документа. Создание и импортирование графических объектов в документ. Способы создания таблиц, вычисление в таблицах. Создание сложных документов. Создание математических формул. Форматирование таблиц в ЭТ MS Excel. Создание формул различной сложности. Построение и форматирование диаграмм. Обработка списков: сортировка, фильтрация, консолидация, итоги. Анализ и распределение данных. Создание и настройка слайдов, презентаций, слайд-шоу. Вставка на слайд аудио эффектов, видео, анимации. Использование гиперссылок. Запись и монтаж звука. Улучшение качества звуковой дорожки. Использование эффектов, накладываемых на трек. Выполнение монтажа фильма. Создание различных видеороликов. Установка, настройка, восстановление операционной системы.</p>

		Подключение периферийных устройств. Установка драйверов периферийных устройств. Технического обслуживание персонального компьютера, принтера, сканера. Санитарные нормы и правила. Определение задач и ресурсов, необходимых для решения данных задач на ЭВМ.	Подключение периферийных устройств. Установка драйверов периферийных устройств. Технического обслуживание персонального компьютера, принтера, сканера. Санитарные нормы и правила. Определение задач и ресурсов, необходимых для решения данных задач на ЭВМ.
УП.05 Осуществление модификации информационных систем			
ПК 5.3.	Тема 1.1. Разработка документации информационных систем Тема 1.2. Отладка и тестирование информационных систем Тема 1.3. Система обеспечения качества информационных систем Тема 1.4. Оценка экономической эффективности информационных систем Тема 2.4 Инструменты коммуникации в цифровой экономике Тема 2.5 Информационная безопасность в цифровой экономике	Разработка документации информационных систем. Отладка и тестирование информационных систем Система обеспечения качества информационных систем Основные технологические составляющие цифровой экономики Инструменты коммуникации в цифровой экономике Информационная безопасность в цифровой экономике	Добавление, удаление и обновление данных. Выполнение запросов на выборку и обработку данных на языке SQL Осуществление основных функций по администрированию баз данных. Обслуживание и поддержка работы современных баз данных и серверов. Проведение сертификации программного средства
УП.06 Технология разработки программного обеспечения			
ПК 7.1 ПК 7.2 ПК 7.3	Тема 2.1.1 Основные понятия и стандартизация требований к программному обеспечению Тема 2.1.2. Описание и анализ требований. Диаграммы IDEF Тема 2.1.3. Оценка качества программных средств Тема 2.2.1 Современные технологии и инструменты интеграции. Тема 2.2.2 Инструментарий тестирования и анализа качества программных средств	Методы организации работы в команде разработчиков. Системы контроля версий Основные подходы к интегрированию программных модулей. Стандарты кодирования. Диаграммы UML. Сущности UML (Структурные, Поведенческие, Поведенческие). Связи UML . Описание требований (спецификация). Оформление требований. Анализ требований. Анализ стратегии выбора решения. Стандарты качества программной документации. Меры и метрики. Тестовое покрытие. Тестовый сценарий. Тестовый пакет. Анализ спецификаций. Верификация и аттестация программного обеспечения.	Методы организации работы в команде разработчиков. Системы контроля версий Основные подходы к интегрированию программных модулей. Стандарты кодирования. Диаграммы UML. Сущности UML (Структурные, Поведенческие, Поведенческие). Связи UML . Описание требований (спецификация). Оформление требований. Анализ требований. Анализ стратегии выбора решения. Стандарты качества программной документации. Меры и метрики. Тестовое покрытие. Тестовый сценарий. Тестовый пакет. Анализ спецификаций. Верификация и аттестация программного обеспечения.

2.3. Содержание учебной практики

Наименование разделов профессионального модуля и тем учебной практики	Содержание работ	Объем, ак.ч.
УП 01 Инструментальные средства разработки программного обеспечения		
Тема 1.4. Основные меры защиты информации в автоматизированных системах	Установка программного обеспечения в соответствии с технической документацией.	6
	Организация защищенной передачи данных в компьютерных сетях.	6
	Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.	12
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Управление учетными записями пользователей.	6
Тема 1.6. Защита информации в распределенных автоматизированных системах	Контроль целостность подсистем защиты информации операционных систем.	6
Тема 1.7. Особенности разработки информационных систем персональных данных	Организация работ с удаленными хранилищами данных и базами данных.	6
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Работа в операционных системах с соблюдением действующих требований по защите информации.	6
	Проведение аудита защищенности автоматизированной системы	6
Тема 2.2. Администрирование автоматизированных систем	Установка, настройка и эксплуатация сетевых операционных систем.	6
Тема 2.4. Защита от несанкционированного доступа к информации	Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.	6
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	Настройка параметров работы программного обеспечения, включая системы управления базами данных. Настройка компонентов подсистем защиты информации операционных систем. Установка обновления программного обеспечения.	12
Тема 3.2. Межсетевые экраны	Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	6
Тема 3.3. Системы обнаружения и предотвращения проникновений	Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.	12
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	Использование программных средств для архивирования информации.	6
	Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	6
УП.02 Управление проектами		

Тема 2.2. Защита программ от изучения копирования	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	12
	Применение математических методов для оценки качества и выбора наилучшего программного средства	12
Тема 2.3. Вредоносное программное обеспечение	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	12
Тема 2.4. Защита программ и данных от несанкционированного	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	12
Тема 2.5. Защита информации на машинных носителях	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	6
Тема 2.7. Системы обнаружения атак и вторжений	Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	12
Тема 5.1. Защита информации в базах данных	Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	12
Тема 6.1. Мониторинг систем защиты	Устранение замечаний по результатам проверки	12
	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	12
Тема 3.6. Криптозащита информации в сетях передачи данных	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	6
УП.03 Разработка кода информационных систем		
Тема 5.1. Применение технических средств защиты информации	Измерение параметров физических полей. Определение каналов утечки ПЭМИН	6
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	6
Тема 5.2. Эксплуатация технических средств защиты информации	Установка и настройка технических средств защиты информации.	6
	Проведение измерений параметров побочных электромагнитных излучений и наводок.	6
	Проведение аттестации объектов информатизации.	6
Тема 3.1 Применение инженерно-технических средств физической защиты	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.	6
	Рассмотрение системы контроля и управления доступом.	6

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Реализация защиты от утечки по цепям электропитания и заземления.	
	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы.	6
	Выполнение звукоизоляции помещений системы шумления.	6
	Разработка организационных и технических мероприятий по заданию преподавателя;	6
	Разработка основной документации по инженерно-технической защите информации.	6
УП.04 Устройство и функционирование информационной системы		
Тема 1.1. Основы информационных технологий в работе оператора ЭВМ	Установка, настройка, восстановление операционной системы.	6
	Подключение периферийных устройств. Установка драйверов периферийных устройств	
Тема 1.2. Техническое и программное обеспечение информационных технологий	Техническое обслуживание персонального компьютера, принтера, сканера. Санитарные нормы и правила. Определение задач и ресурсов, необходимых для решения данных задач на ЭВМ.	6
Тема 1.3 Особенности обработки текстовой информации	Создание, форматирование и редактирование документов. Сохранение и открытие документов.	6
Тема 1.4. Особенности обработки экономической и статистической информации	Работа со списками и формами документов. Создание и форматирование многоколоночного документа. Создание и импортирование графических объектов в документ.	
Тема 1.5 Оформление служебной документации	Создание сложных документов.	6
Тема 1.6 Технологии обработки растровой графики	Создание математических формул. Форматирование таблиц в ЭТ MS Excel. Создание формул различной сложности. Построение и форматирование диаграмм. Обработка списков: сортировка, фильтрация, консолидация, итоги. Анализ и распределение данных.	
Тема 1.7 Электронные презентации MS PowerPoint	Создание и настройка слайдов, презентаций, слайд-шоу.	6
Тема 1.8 Технологии обработки аудиоинформации	Вставка на слайд аудио эффектов, видео, анимации. Использование гиперссылок. Запись и монтаж звука. Улучшение качества звуковой дорожки. Использование эффектов, накладываемых на трек.	
Тема 1.9 Технологии обработки видеоинформации	Выполнение монтажа фильма. Создание различных видеороликов.	6
УП.05 Управление и автоматизация баз данных		

Тема 1.1. Разработка документации информационных систем	Разработка документации информационных систем.	6
Тема 1.2. Отладка и тестирование информационных систем	Отладка и тестирование информационных систем	6
Тема 1.3. Система обеспечения качества информационных систем	Система обеспечения качества информационных систем	6
Тема 1.4. Оценка экономической эффективности информационных систем	Основные технологические составляющие цифровой экономики	6
Тема 2.4 Инструменты коммуникации в цифровой экономике	Инструменты коммуникации в цифровой экономике	6
Тема 2.5 Информационная безопасность в цифровой экономике	Информационная безопасность в цифровой экономике	6
УП.06 Осуществление модификации информационных систем		
Тема 2.1.1 Основные понятия и стандартизация требований к программному обеспечению	Методы организации работы в команде разработчиков. Системы контроля версий.	6
	Основные подходы к интегрированию программных модулей. Стандарты кодирования.	12
	Диаграммы UML. Сущности UML (Структурные, Поведенческие, Поведенческие). Связи UML .	12
Тема 2.1.2. Описание и анализ требований. Диаграммы IDEF	Меры и метрики Описание требований (спецификация). Оформление требований. Анализ требований.	12
Тема 2.1.3. Оценка качества программных средств	Анализ стратегии выбора решения. Стандарты качества программной документации.	6
Тема 2.2.1 Современные технологии и инструменты интеграции.	Тестовое покрытие. Тестовый сценарий. Тестовый пакет.	12
Тема 2.2.2 Инструментарий тестирования и анализа качества программных средств	Анализ спецификаций. Верификация и аттестация программного обеспечения.	12

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение учебной практики

Кабинет:

- Общеобразовательных дисциплин;
- Социально-экономических дисциплин;
- Иностранного языка (лингвфонный);
- Математических дисциплин;
- Информатики и информационных технологий;
- Безопасности жизнедеятельности;
- Метрологии и стандартизации, оснащенный(е) в соответствии с приложением 3

ОПОП-П.

Лаборатории:

- Вычислительной техники, архитектуры персонального компьютера и периферийных устройств
- Организации и принципов построения информационных систем
- Информационных ресурсов, оснащенная(ые) в соответствии с приложением 3 ОПОП-П.

Мастерские и зоны по видам работ, оснащенные в соответствии с приложением 3 ОПОП-П:

- Лаборатория архитектуры персонального компьютера и периферийных устройств
- Лаборатория инженерной и компьютерной графики
- Лаборатория разработки дизайна веб-приложений
- Лаборатория разработки веб-приложений
- Лаборатория программирования и баз данных
- Лаборатория информационных ресурсов
- Лаборатория программного обеспечения и сопровождения компьютерных систем
- Лаборатория вычислительной техники и дистанционных систем передачи информации

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2022.- 175 с.
2. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2022.
3. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2022.
4. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2022.- 248 с.
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2021.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2022. – 416 с.

7. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2020.
8. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - 2-е изд.- М.: Горячая линия-Телеком, 2022.
9. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2022.
10. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2021
11. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2022. – 184 с.
12. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2021. – 172 с.
13. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2021. – 336с
14. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2022.
15. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2021.
16. Сеницын С.В., Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2020.
17. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2022.
18. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2022.
19. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019

3.2.2. Дополнительные источники

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность <http://www.itsec.ru> –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
11. Федеральный портал «Российское образование www.edu.ru

12. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г
13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
14. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
15. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
16. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
17. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
18. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
19. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
20. 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».
21. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
22. 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.
23. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
24. 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.
25. 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.
26. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
27. от 30 августа 2002 г. № 282.
28. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
29. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
30. от 31 августа 2010 г. № 416/489.
31. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

32. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
33. 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 недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
34. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.
35. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
36. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
37. 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
38. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
39. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
40. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
41. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
42. 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
43. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
44. 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
45. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
46. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
47. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
48. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

49. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
50. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
51. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
52. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
53. Номенклатура показателей качества. Ростехрегулирование, 2005.
54. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
55. 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.
56. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
57. 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.
58. 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.
59. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
60. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
61. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
62. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
63. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
64. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
65. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
66. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
67. в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и

виброакустическому каналам, специальных исследований средств вычислительной техники;

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

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. справочно-правовая система «Консультант Плюс» www.consultant.ru
5. справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование» www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
10. Сайт Научной электронной библиотеки www.elibrary.ru

3.3. Общие требования к организации учебной практики

Учебная практика проводится в учебно-производственных мастерских, лабораториях и иных структурных подразделениях образовательного учреждения, либо в организациях в специально оборудованных помещениях на основе договоров между организацией, осуществляющей деятельность по образовательной программе соответствующего профиля (далее – Профильная организация), и образовательным учреждением.

Сроки проведения учебной практики устанавливаются образовательной организацией в соответствии с ОПОП-П по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Учебная практика реализуется в форме практической подготовки и проводится путем чередования с теоретическими занятиями по дням (неделям) при условии обеспечения связи между теоретическим обучением и содержанием практики.

3.4 Кадровое обеспечение процесса учебной практики

Учебная практика проводится мастерами производственного обучения и (или) преподавателями дисциплин профессионального цикла.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Индекс УП	Код ПК, ОК	Основные показатели оценки результата	Формы и методы контроля и оценки
УП. 01	ПК 1.1 ПК 1.2 ПК 1.3 ПК 1.4 ОК 01 ОК 02 ОК 03 ОК 04	<p>Демонстрировать умения установки и настройки компонентов, автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации</p> <p>Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении</p> <p>Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации</p> <p>Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении</p>	<p>Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах практики</p> <p>Экспертное наблюдение за ходом выполнения заданий учебной практики</p>
УП. 02	ПК 2.1. ПК 2.2. ПК 2.3 ПК 2.4. ПК 2.5 ПК 2.6 ОК 01 ОК 02 ОК 03 ОК 04	<p>Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации</p> <p>Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами</p> <p>Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации</p> <p>Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа</p> <p>Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств</p> <p>Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и</p>	<p>Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах практики</p> <p>Экспертное наблюдение за ходом выполнения заданий учебной практики</p>

		ликвидации последствий компьютерных атак	
УП 03	ПК 3.1 ПК 3.2 ОК 01 ОК 02 ОК 03 ОК 04	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах практики Экспертное наблюдение за ходом выполнения заданий учебной практики
УП 04	ПК 4.1. ПК 4.2. ПК 4.3. ПК 4.4. ОК 01 ОК 02 ОК 03 ОК 04	Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации Применение средств защиты информации в компьютерной системе	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах практики Экспертное наблюдение за ходом выполнения заданий учебной практики
УП. 05	ПК 5.3	Эффективно планировать свою деятельность по сбору данных для функционирования информационной системы, грамотно использовать полученные данные для оптимизации работы системы. Проводить работу с различными видами проектной документации.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах практики Экспертное наблюдение за ходом выполнения заданий учебной практики
УП. 06	ПК 7.1 ПК 7.2 ПК 7.3	Разрабатывать и обосновывать вариант интеграционного решения с помощью графических средств среды разработки, выбирать альтернативное решение; учитывать бизнес-процессы в полном объеме; отчет оформлять в полном соответствии с требованиями стандартов; результаты верно сохранять в системе контроля версий.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах практики Экспертное наблюдение за ходом выполнения заданий учебной практики

