ПРИЛОЖЕНИЕ 1.1.1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ (УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ)

Индекс УП/ПП	**ПМ** (индекс, наименование)	**Вид практики (учебная/ производственная**	**Тип (этап) практики** (при наличии)	**Семестр**	**Объем в часах**
УП. 01	ПМ 01	Учебная практика	*программная*	3, 4 семестр	84
УП. 02	ПМ 02	Учебная практика	*программная*	3 семестр	48
УП. 03	ПМ 03	Учебная практика	*программная*	5 семестр	66
УП. 04	ПМ 04	Учебная практика	*программная*	2 семестр	156
УП. 05	ПМ 05	Учебная практика	*программная*	6 семестр	12
		Всего УП	X	X	366
ПП. 01	ПМ 01	Производственная практика	*программно-технологическая,*	4 семестр	120
ПП. 02	ПМ 02	Производственная практика	*программно-технологическая,*	4 семестр	156
ПП. 03	ПМ 03	Производственная практика	*программно-технологическая,*	5 семестр	168
ПП. 04	ПМ 04	Производственная практика	*программно-технологическая,*	2 семестр	84
ПП. 05	ПМ 05	Производственная практика	*программно-технологическая,*	6 семестр	84
		Всего ПП	X	X	612
		Итого практики	X	X	978

2024г.

ПРИЛОЖЕНИЕ 1.1.1.1

к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

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

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

УП.03 ПМ 03 Защита информации техническими средствами

УП.04 ПМ 04 Оператор электронно-вычислительных и вычислительных машин

УП.05 ПМ 05 Обеспечение комплексной безопасности объекта защиты

99

СОДЕРЖАНИЕ

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 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 защищенном исполнении код и наименование МДК 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 Защита информации техническими средствами	ПМ 03 Защита информации техническими средствами	МДК 03.01 Техническая защита информации МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации
УП 04 Оператор электронно-вычислительных и вычислительных машин	ПМ 04 Оператор электронно-вычислительных и вычислительных машин	МДК 04.01 Технология создания и обработки цифровой информации
УП 05 Обеспечение комплексной безопасности объекта защиты	ПМ 05 Обеспечение комплексной безопасности объекта защиты	МДК 05.02 Организация работы с конфиденциальной информацией МДК 05.03 Обеспечение системы безопасности предприятия

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

Код ОК / ПК	Наименование ОК / ПК
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
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.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
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 (ПЭМИН), 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
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 5.1	Участвовать в разработке и внедрении программ и методик организации защиты информации на объекте
ПК 5.2	Осуществлять планирование и организацию выполнения мероприятий по защите информации
ПК 5.3	Выявлять и анализировать возможные угрозы информационной безопасности объектов

Цель учебной практики: формирование первоначальных практических профессиональных умений в рамках профессиональных модулей данной ОПОП-П по видам деятельности:

ВД 1 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ВД 3 Защита информации техническими средствами

ВД 4 Оператор электронно-вычислительных и вычислительных машин

ВД 5 Обеспечение комплексной безопасности объекта защиты

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 1 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	Выполнять конфигурирование Настраивать автоматизированные системы в защищенном исполнении Производить компонент систем защиты информации автоматизированных систем Организовывать, конфигурировать, производить монтаж диагностику и устранять неисправности КС Работать с сетевыми протоколами разных уровней Осуществлять конфигурирование Выполнять настройку компонент систем защиты информации автоматизированных систем Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации АС Настраивать неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам Устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам Обеспечивать работоспособность Обнаруживать неисправности Устранять неисправности
ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации Устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации Диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации Применять программные и программно-аппаратные средства для защиты информации в базах данных Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации Применять математический аппарат для выполнения криптографических преобразований

	Использовать типовые программные криптографические средства, в том числе электронную подпись Применять средства гарантированного уничтожения информации Устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
ВД 3 Защита информации техническими средствами	Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Применять технические средства для криптографической защиты информации конфиденциального характера Применять технические средства для уничтожения информации и носителей информации Применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Основные принципы действия и характеристики технических средств физической защиты Основные способы физической защиты объектов информатизации Номенклатуру применяемых средств физической защиты объектов информатизации
ВД 4 Оператор электронно-вычислительных и вычислительных машин	Выполнять требования техники безопасности при работе с вычислительной техникой Производить подключение блоков персонального компьютера и периферийных устройств Производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники Диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники Выполнять инсталляцию системного и прикладного программного обеспечения Создавать и управлять содержимым документов с помощью текстовых процессоров Создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц

	Создавать и управлять содержимым презентаций с помощью редакторов презентаций Использовать мультимедиа проектор для демонстрации презентаций Вводить, редактировать и удалять записи в базе данных Эффективно пользоваться запросами базы данных Создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики Производить сканирование документов и их распознавание Производить распечатку, копирование и тиражирование документов на принтере и других устройствах Управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете Осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера Осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет-сайтов Осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ Осуществлять резервное копирование и восстановление данных
ВД 5 Обеспечение комплексной безопасности объекта защиты	Управлять защитой информации на объектах информатизации Проводить аудит защищенности информации на объекте информатизации Внедрять организационные меры по защите информации на объекте информатизации Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации Разработка организационно-распорядительных документов по защите информации на объектах защиты Находить уязвимости системы защиты информации Разрабатывать модели угроз модели угроз объекта информатизации

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- 1.4	Устанавливать компоненты системы защиты информации автоматизированных	Эксплуатация автоматизированных (информаци	84	

		(информационных) систем Настраивать компоненты системы защиты информации автоматизированных (информационных) систем Администрировать автоматизированные система в защищенном исполнении Выполнять эксплуатацию компонентов систем защиты информации автоматизированных систем Выполнять диагностику компонентов систем защиты информации автоматизированных систем Устранять отказы работоспособности автоматизированных (информационных) систем в защищенном исполнении Восстанавливать работоспособности автоматизированных (информационных) систем в защищенном исполнении	онных) систем в защищённом исполнении		
УП. 02	ПК 2.1- 2.6	Выполнять установку, настройку программных средств защиты информации в автоматизированной Обеспечивать защиту автономных автоматизированных систем программными и программно-аппаратными средствами	Защита информации в автоматизированных системах программными и программно-аппаратным	48	

		Использовать программные и программно-аппаратные средства для защиты информации в сети Тестировать функций, диагностировать работоспособности программных и программно-аппаратных средств защиты информации Устранять отказы и восстанавливать работоспособности программных и программно-аппаратных средств защиты информации Решать задачи защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации Применять электронную подпись, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности Выполнять работу с подсистемами регистрации событий Выявлять события и инцидентов безопасности в автоматизированной системе	и средствами		

УП. 03	ПК 3.1-3.5	Установка, монтаж и настройка технических средств защиты информации Техническое обслуживание технических средств защиты информации Применение основных типов технических средств защиты информации Применять основные типы технических средств защиты информации Выявлять технические каналы утечки информации Участвовать в мониторинге эффективности технических средств защиты информации Диагностировать, устранять отказы и неисправности, восстанавливать работоспособности технических средств защиты информации Проводить измерения параметров пэмин, созданные техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации	Защита информации техническими средствами	66	

		Проводить измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации Выявлять технические каналы утечки информации Устанавливать, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей Восстанавливать работоспособности инженерно-технических средств физической защиты			
УП. 04	ПК 4.1-4.4	Выполнять требования техники безопасности при работе с вычислительной техникой, Организовывать рабочее места оператора электронно-вычислительных и вычислительных машин, Подготовки оборудования компьютерной системы к работе Инсталлировать, настраивать и обслуживать программное обеспечение компьютерной системы Управлять файлами Применять офисное программное обеспечение в	Оператор электронно-вычислительных и вычислительных машин	156	

		соответствии с прикладной задачей Использовать ресурсы локальной вычислительной сети Использовать ресурсы, технологии и сервисов Интернет Применять средства защиты информации в компьютерной системе			
УП. 05	ПК 5.1-5.3	Внедрять программы и методики защиты на объектах Участвовать в оценке качества защиты объекта Готовить организационные документы, регламентирующие работу по защите информации Вести учет работ и объектов, подлежащих защите Анализировать уязвимости системы защиты информации Определять причины возникновения угроз безопасности	Обеспечение комплексной безопасности объекта защиты	12	
Всего академических часов учебной практики в рамках вариативной части ОПОП-П -366					

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	84	концентрированно	3 курс/ 3, 4 семестр	ДЗ
УП. 02	48	концентрированно	3 курс/ 3 семестр	ДЗ
УП. 03	66	концентрированно	4 курс/ 5 семестр	ДЗ
УП. 04	156	концентрированно	2 курс/ 2 семестр	ДЗ
УП. 05	12	концентрированно	4 курс/ 6 семестр	ДЗ
Всего УП	366	X	X	X

2.2. Структура учебной практики

Код ПК	Наименование разделов профессионального модуля	Виды работ	Наименование тем учебной практики	Объем часов
УП 01. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении				84
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	– 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	Тема 1.1. Основные меры защиты информации в автоматизированных системах	10
			Тема 1.2. Защита информации в распределенных автоматизированных системах	10
			Тема 1.3 Администрирование автоматизированных систем	10

		работоспособности операционной системы и базы данных – использование программных средств для архивирования информации. – проведение аудита защищенности автоматизированной системы.	Тема 1.4 Эксплуатация средств защиты информации в компьютерных сетях	10
ВСЕГО ПО РАЗДЕЛУ 1				**40**
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	Раздел 2. Эксплуатация компьютерных сетей	– установка, настройка и эксплуатация сетевых операционных систем. – диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. – организация работ с удаленными хранилищами данных и базами данных. – организация защищенной передачи данных в компьютерных сетях. – выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. – осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. – заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	Тема 2.1. Начальная настройка коммутатора	10
			Тема 2.2 Адресация сетевого уровня и маршрутизация	10
			Тема 2.3 Функции управления коммутаторами	12
			Тема 2.4 Приоритизация трафика и создание альтернативных маршрутов	12
ВСЕГО ПО РАЗДЕЛУ 2				44
УП 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами				48

ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.	Раздел 1. Программные и программно-аппаратные средства защиты информации	– Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах – Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности – Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности – Составление документации по учету, обработке, хранению и передаче конфиденциальной информации – Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации – Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. – Устранение замечаний по результатам проверки – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	Тема 1.1. Принципы программно-аппаратной защиты информации от несанкционированного доступа	4
			Тема 1.2. Защита программ от изучения	4
			Тема 1.3. Защита программ и данных от несанкционированного копирования	4
			Тема 1.4 Системы обнаружения атак и вторжений	6
			Тема 1.5 Основы построения защищенных сетей	6
			Тема 1.6 Изучение современных программно-аппаратных комплексов.	6
			ВСЕГО ПО РАЗДЕЛУ 1	**30**
ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5.	Раздел 2. Криптографические средства защиты информации	– Применение математических методов для оценки качества и выбора наилучшего программного средства	Тема 2.1 Кодирование информации. Компьютеризация шифрования.	6

ПК 2.		– Применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	Тема 2.2. Алгоритмы обмена ключей и протоколы аутентификации	6
			Тема 2.3. Защита информации в электронных платежных системах	6
ВСЕГО ПО РАЗДЕЛУ 2				18
УП 03. Защита информации в автоматизированных системах программными и программно-аппаратными средствами				66
ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5	Раздел 1. Техническая защита информации	– Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации. – Освоение методики выявления возможных угроз информационной безопасности объектов защиты. – Проектирование установки системы пожарно-охранной сигнализации по заданию. – Применение промышленных осциллографов, частотомеров и	Тема 1.1 Методы и средства технической разведки	10
			Тема 1.2 Физические процессы при подавлении опасных сигналов	10
			Тема 1.3. Системы защиты от утечки информации	10
			Тема 1.4. Эксплуатация технических средств защиты информации	12

		генераторов, и другого оборудования для защиты информации.		
			ВСЕГО ПО РАЗДЕЛУ 1	42
ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5	Раздел 2. Инженерно-технические средства физической защиты объектов информатизации	– Рассмотрение системы контроля и управления доступом и её проектирование. – Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	Тема 2.1 Применение инженерно-технических средств физической защиты	12
		– Рассмотрение датчиков периметра, их принципов работы. – Рассмотрение звукоизоляции помещений, обоснование зашумления и его проектирование. – Реализация защиты от утечки по цепям электропитания и заземления. – Разработка организационных и технических мероприятий по заданию. – Разработка основной документации по инженерно-технической защите информации.	Тема 2.2 Эксплуатация инженерно-технических средств физической защиты	12
			ВСЕГО ПО РАЗДЕЛУ 2	24
УП 04. Оператор электронно-вычислительных и вычислительных машин				156
ПК 4.1 - ПК 4.4	Раздел 1 Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения	– Подключение периферийных устройств к разъемам системного блока. – Настройка и подготовка к работе принтера, сканера.	Тема 1.1 Работа с программным обеспечением компьютерной системы	12
			ВСЕГО ПО РАЗДЕЛУ 1	12
	Раздел 2. Создание и управление на		Тема 2.1 Работа в	24

ПК 4.1 - ПК 4.4	персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах	– Создание схем, таблиц и формул в программе Microsoft Word. – Создание буклетов в программе Microsoft Publisher. – Ведение расчетов и построение диаграмм в программе Microsoft Excel. – Создание таблиц, форм, запросов и отчетов в программе Microsoft Access. – Создание презентации в программе PowerPoint. – Обработка графических объектов в Corel и PhotoShop. – Настройка локальной вычислительной сети.	текстовом процессоре	
			Тема 2.2. Работа в редакторе электронных таблиц	24
			Тема 2.3. Работа в программе подготовки и просмотра презентаций	24
			Тема 2.4. Работа в системе управления базами данных	24
			Тема 2.5. Работа в графических редакторах	24
ВСЕГО ПО РАЗДЕЛУ 2				120
ПК 4.1 - ПК 4.4	Раздел 3. Использование ресурсов технологий и сервисов Интернета	– Поиск информации в сети Интернет. – Создание комплексного документа с использованием информации различных типов	Тема 3.1. Работа с ресурсами Интернета	24
ВСЕГО ПО РАЗДЕЛУ 3				24
УП 05. Обеспечение комплексной безопасности объекта защиты				12
ПК 5.1, ПК 5.2, ПК 5.3	Раздел 1. Организация и технология работы с конфиденциальной информацией	– Разграничение уровней политики информационной безопасности – Составление частной модели угроз для организации – Определение категории информационных ресурсов, подлежащих защите – информационной безопасности	Тема 1.1 Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ	2
			Тема 1.2 Организацион но-	4

		− Подготовка документа − Политики информационной безопасности	распорядительные документы по обеспечению безопасности объектов в том числе объектов КИИ	
ВСЕГО ПО РАЗДЕЛУ 1				6
ПК 5.1, ПК 5.2, ПК 5.3	Раздел 2. Обеспечение системы безопасности объекта защиты	− Разработка мер обеспечения информационной безопасности» − Разработка основных принципов построения системы Подбор антивирусного средства для конкретного объекта − Выявление требований к аппаратным и программным средствам	Тема 2.1 Состав и структура системы безопасности	2
			Тема 2.2 Построение системы защиты информации	4
ВСЕГО ПО РАЗДЕЛУ 2				**6**

2.3. Содержание учебной практики

Наименование разделов профессионального модуля и тем учебной практики	**Содержание работ**	**Объем, ак.ч.**
УП 01. ПМ 01. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		**84**
Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		**40**
Тема 1.1. Основные меры защиты информации в автоматизированных системах	**Содержание**	
	Изучение нормативно-правовой базы для определения мер защиты информации в автоматизированных информационных системах и требований к ним Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	10
	Содержание	

Тема 1.2. Защита информации в распределенных автоматизированных системах	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	10
Тема 1.3 Администрирование автоматизированных систем	**Содержание**	
	Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Управление, тестирование и эксплуатация автоматизированных систем	10
Тема 1.4 Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	10
Раздел 2. Эксплуатация компьютерных сетей		44
Тема 2.1. Начальная настройка коммутатора	**Содержание**	10
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	
Тема 2.2 Адресация сетевого уровня и маршрутизация	**Содержание**	10
	Основные и расширенные конфигурации маршрутизатора. Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP. Работа с протоколом RIP и OSPF. Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.	
Тема 2.3 Функции управления коммутаторами	**Содержание**	12
	Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	

	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
Тема 2.4 Приоритизация трафика и создание альтернативных маршрутов	**Содержание**	12
	Создание альтернативных маршрутов с использованием статической маршрутизации	
Промежуточная аттестация в форме дифференцированного зачета		
УП 02. ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		66
Раздел 1. Программные и программно-аппаратные средства защиты информации		30
Тема 1.1. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	
	Организация доступа к файлам Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	4
Тема 1.2. Защита программ от изучения	**Содержание**	
	Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям	4
Тема 1.3. Защита программ и данных от несанкционированного копирования	**Содержание**	
		4
Тема 1.4 Системы обнаружения атак и вторжений	**Содержание**	
	Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	6
Тема 1.5 Основы построения защищенных сетей	**Содержание**	
	Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	6
Тема 1.6 Изучение современных программно-аппаратных комплексов.	**Содержание**	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	6
Раздел 2. Криптографические средства защиты информации		18

Тема 2.1 Кодирование информации. Компьютеризация шифрования.	**Содержание**	
	Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII. Изучение современных программных и аппаратных криптографических средств	6
Тема 2.2. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание**	
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	6
Тема 2.3. Защита информации в электронных платежных системах	**Содержание**	
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	6
Промежуточная аттестация в форме дифференцированного зачета		
УП 03. ПМ 03 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		66
Раздел 1. Техническая защита информации		42
Тема 1.1 Методы и средства технической разведки	**Содержание**	10
	Изучение характеристик наземных средств дистанционного съема информации Анализ современных средств перехвата сигналов	
Тема 1.2 Физические процессы при подавлении опасных сигналов	**Содержание**	10
	Изучение пассивных методов подавления опасных сигналов акустоэлектрических преобразователей Изучение активных методов подавления опасных сигналов акустоэлектрических преобразователей	
Тема 1.3. Системы защиты от утечки информации	**Содержание**	10
	Средства акустической разведки Закладные устройства Защита от утечки по виброакустическому каналу Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок.	
Тема 1.4. Эксплуатация технических средств защиты информации	**Содержание**	12
	Установка и настройка технических средств защиты информации	

	Оценка функционирования средств защиты информации от несанкционированного доступа	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		24
Тема 2.1 Применение инженерно-технических средств физической защиты	**Содержание**	12
	Организация пропускного режима на КПП, система автоматического управления Определение путей проникновения злоумышленника на объект информатизации Внутриобъектовый режим. Интегрированные охранные системы	
Тема 2.2 Эксплуатация инженерно-технических средств физической защиты	**Содержание**	12
	Изучение принципов диагностики, устранения отказов и восстановление работоспособности технических средств физической защиты	
Промежуточная аттестация в форме дифференцированного зачета		
УП 04. ПМ 04 Оператор электронно-вычислительных и вычислительных машин		156
Раздел 1 Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		12
Тема 1.1 Работа с программным обеспечением компьютерной системы	**Содержание**	
	Подключение, настройка и подготовка к работе периферийного оборудования Установка и замена расходных материалов для принтеров, ксерокса, сканера Установка прикладных программ	
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах		120
Тема 2.1 Работа в текстовом процессоре	**Содержание**	24
	Форматирование и редактирование шрифтов, абзацев и формул Форматирование и редактирование списков Работа с таблицами в текстовом процессоре Работа с графическими объектами в текстовом процессоре Форматирование документа в целом. Способы вывода документа на печать	
Тема 2.2. Работа в редакторе электронных таблиц	**Содержание**	24
	Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице. Работа со встроенными функциями в электронной таблице.	

	Создание и работа с диаграммами и графиками. Обмен данными между текстовым процессором и электронной таблицей	
Тема 2.3. Работа в программе подготовки и просмотра презентаций	**Содержание**	24
	Основы работы со слайдом. Работа в презентации со шрифтом и текстом. Понятие темы слайда Добавление в слайды рисунков, звуковых эффектов, таблиц и диаграмм Настройка анимации объектов. Настройка показа и демонстрация результатов работы средствами мультимедиа	
Тема 2.4. Работа в системе управления базами данных	**Содержание**	24
	Ввод данных в таблицы базы данных Создание простых запросов и форм. Создание и форматирование главной кнопочной формы. Создание отчетов.	
Тема 2.5. Работа в графических редакторах	**Содержание**	24
	Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики.	
Раздел 3. Использование ресурсов технологий и сервисов Интернета		
Тема 3.1. Работа с ресурсами Интернета	**Содержание**	24
	Настройка парольной защиты на открытие и запись файла Настройка защиты документа с помощью прав доступа Защита информации в приложениях MS Office.	
Промежуточная аттестация в форме дифференцированного зачета		
УП 05. ПМ 05. Обеспечение комплексной безопасности объекта защиты		12
Раздел 1. Организация и технология работы с конфиденциальной информацией		
Тема 1.1 Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ	**Содержание**	
	Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31 Определение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Анализ приказа № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем	2

	безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» Классификация уязвимостей информационной системы, причины возникновения угроз безопасности Проектирование системы безопасности значимого объекта КИИ Состав системы безопасности значимых объектов.	
Тема 1.2 Организационно-распорядительные документы по обеспечению безопасности объектов в том числе объектов КИИ	**Содержание**	
	Изучение порядка и правил функционирования системы безопасности значимых объектов КИИ Анализ приказа Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» Разработка рабочей и эксплуатационной документации. Определение порядка и правил обеспечения безопасности объектов	4
Раздел 2. Обеспечение системы безопасности объекта защиты		12
Тема 2.1 Состав и структура системы безопасности	**Содержание**	
	Состав и структура системы безопасности. Направления защиты объекта информатизации. Средства и способы защиты. Организации работы в чрезвычайной ситуации. Состав службы безопасности.	2
Тема 2.2 Построение системы защиты информации	**Содержание**	
	Определение угроз информационной безопасности Выделение недостатки существующей КСЗИ. Анализ рисков КСЗИ. Усовершенствование организационного обеспечения и СКУД объекта защиты Усовершенствование инженерно-технического обеспечение комплексной системы защиты информации Усовершенствование программно-аппаратного обеспечения комплексной системы защиты информации Анализ рисков разработанной КСЗИ	4
Промежуточная аттестация в форме дифференцированного зачета		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение учебной практики

Кабинет информационных технологий

Кабинет Вычислительной техники, архитектуры персонального компьютера и периферийных устройств;

Лаборатория Компьютерных систем, сетей и телекоммуникаций»,

Мастерская Кибер-безопасности

Мастерская «Сетевого и системного администрирования»

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.

2. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018 – 336с.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-fed eralnyj-zakon-ot-26-iyulya-2017-g-n-187-fz.

4. Постановление Правительства РФ № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_291398 .

5. Приказ Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://rg.ru/2018/02/13/fstek-prikaz-227-site-dok.html .

6. Давыдова, Е. М. Организация защиты объектов критической информационной инфраструктуры: Учебно-методическое пособие [Электронный ресурс] / Е. М. Давыдова, А. Ю. Якимук. — Томск: ТУСУР, 2022.

— 20 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10003.

3.2.2. Дополнительные источники *(при необходимости)*

1. Котеров Д.В. PHP 5 в подлиннике. – СПб.: БХВ-Петербург, 2018. – 1104 с.

2. Федеральный образовательный портал «Информационно - коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832. Дата обращения 23.07.2022.

3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2019. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

4. Федеральный образовательный портал «Информационно - коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832

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 реализуются в форме практической подготовки и проводятся непрерывно.

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.	Демонстрирует умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 1.2.	Проявляет умения и практический опыт администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 1.3.	Проводит перечень работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 1.4.	Проявляет знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

		(информационных) систем в защищенном исполнении	оценка процесса и результатов выполнения видов работ на практике
УП 02	ПК 2.1.	Демонстрирует умения и навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.2.	Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.3.	Выполняет перечнь работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.4.	Проявляет знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ,

			экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.5.	Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.6.	Проявляет знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
УП 03	ПК 3.1	Демонстрирует умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

	ПК 3.2	Проявляет умения и практический опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.3.	Проводит работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.4	Проводит самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.5	Проявляет знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

			оценка процесса и результатов выполнения видов работ на практике
УП 04	ПК 4.1.	Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 4.2	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных	
	ПК 4.3	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	
	ПК 4.4	Применение средств защиты информации в компьютерной системе	
УП 05	ПК 5.1	Участвует в оценке качества защиты объекта Управляет защитой информации на объектах информатизации Проводит аудит защищенности информации на объекте информатизации Внедряет организационные меры по защите информации на объекте информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 5.2	Готовит организационные документы, регламентирующие работу по защите информации Ведёт учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации Разрабатывает организационно-распорядительные документы	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

		по защите информации на объектах защиты	
	ПК 5.3	Проводит анализ уязвимостей системы защиты информации Определяет причины возникновения угроз безопасности Находит уязвимости системы защиты информации Разрабатывает модели угроз модели угроз объекта информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПРИЛОЖЕНИЕ 1.1.1.2
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

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

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

ПП.03 ПМ 03 Защита информации техническими средствами

ПП.04 ПМ 04 Оператор электронно-вычислительных и вычислительных машин

ПП.05 ПМ 05 Обеспечение комплексной безопасности объекта защиты

2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

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

Рабочая программа производственной практики (ПП) является частью программы подготовки в соответствии с ФГОС СПО по специальности к ОПОП-П по 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):

ПП 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 защищенном исполнении код и наименование МДК МДК 01.05 Эксплуатация компьютерных сетей
ПП 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
ПП 03 Защита информации техническими средствами	ПМ 03 Защита информации техническими средствами	МДК 03.01 Техническая защита информации МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации
ПП 04 Оператор электронно-вычислительных и вычислительных машин	ПМ 04 Оператор электронно-вычислительных и вычислительных машин	МДК 04.01 Технология создания и обработки цифровой информации
ПП 05 Обеспечение комплексной безопасности объекта защиты	ПМ 05 Обеспечение комплексной безопасности объекта защиты	МДК 05.02 Организация работы с конфиденциальной информацией МДК 05.03 Обеспечение системы безопасности предприятия

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

Код ОК / ПК	Наименование ОК / ПК
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
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.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
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 (ПЭМИН), 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
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 5.1	Участвовать в разработке и внедрении программ и методик организации защиты информации на объекте
ПК 5.2	Осуществлять планирование и организацию выполнения мероприятий по защите информации
ПК 5.3	Выявлять и анализировать возможные угрозы информационной безопасности объектов

Цель производственной практики: приобретение практического опыта в рамках профессиональных модулей данной ОПОП-П по видам деятельности:

ВД 1 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ВД 3 Защита информации техническими средствами

ВД 4 Оператор электронно-вычислительных и вычислительных машин

ВД 5 Обеспечение комплексной безопасности объекта защиты

1.2. Планируемые результаты освоения учебной практики

В результате прохождения производственной практики по видам деятельности, предусмотренным ФГОС СПО и запросам работодателей, обучающийся должен получить практический опыт:

Наименование вида деятельности	Практический опыт / умения
ВД 1 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	Выполнять конфигурирование Настраивать автоматизированные системы в защищенном исполнении Производить компонент систем защиты информации автоматизированных систем Организовывать, конфигурировать, производить монтаж диагностику и устранять неисправности КС Работать с сетевыми протоколами разных уровней Осуществлять конфигурирование Выполнять настройку компонент систем защиты информации автоматизированных систем Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации АС Настраивать неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам Устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам Обеспечивать работоспособность Обнаруживать неисправности Устранять неисправности
ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации Устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации Диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации Применять программные и программно-аппаратные средства для защиты информации в базах данных Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации

	Применять математический аппарат для выполнения криптографических преобразований Использовать типовые программные криптографические средства, в том числе электронную подпись Применять средства гарантированного уничтожения информации Устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
ВД 3 Защита информации техническими средствами	Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Применять технические средства для криптографической защиты информации конфиденциального характера Применять технические средства для уничтожения информации и носителей информации Применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Основные принципы действия и характеристики технических средств физической защиты Основные способы физической защиты объектов информатизации Номенклатуру применяемых средств физической защиты объектов информатизации
ВД 4 Оператор электронно-вычислительных и вычислительных машин	Выполнять требования техники безопасности при работе с вычислительной техникой Производить подключение блоков персонального компьютера и периферийных устройств Производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники Диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники Выполнять инсталляцию системного и прикладного программного обеспечения Создавать и управлять содержимым документов с помощью текстовых процессоров

	Создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц Создавать и управлять содержимым презентаций с помощью редакторов презентаций Использовать мультимедиа проектор для демонстрации презентаций Вводить, редактировать и удалять записи в базе данных Эффективно пользоваться запросами базы данных Создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики Производить сканирование документов и их распознавание Производить распечатку, копирование и тиражирование документов на принтере и других устройствах Управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете Осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера Осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет-сайтов Осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ Осуществлять резервное копирование и восстановление данных
ВД 5 Обеспечение комплексной безопасности объекта защиты	Управлять защитой информации на объектах информатизации Проводить аудит защищенности информации на объекте информатизации Внедрять организационные меры по защите информации на объекте информатизации Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации Разработка организационно-распорядительных документов по защите информации на объектах защиты Находить уязвимости системы защиты информации Разрабатывать модели угроз модели угроз объекта информатизации

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

Код ПП	Код ПК/дополнительные (ПК*, ПКц)	Практический опыт	Наименование темы практики	Объем часов ПП	Обоснование увеличения объема практики
ПП. 01	ПК 1.1- 1.4	Устанавливать компоненты системы защиты информации автоматизированных	Эксплуатация автоматизированных (информац	120	

		(информационных) систем Настраивать компоненты системы защиты информации автоматизированных (информационных) систем Администрировать автоматизированные система в защищенном исполнении Выполнять эксплуатацию компонентов систем защиты информации автоматизированных систем Выполнять диагностику компонентов систем защиты информации автоматизированных систем Устранять отказы работоспособности автоматизированных (информационных) систем в защищенном исполнении Восстанавливать работоспособности автоматизированных (информационных) систем в защищенном исполнении	ионных) систем в защищённом исполнении		
ПП. 02	ПК 2.1- 2.6	Выполнять установку, настройку программных средств защиты информации в автоматизированной	Защита информации в автоматизированных системах программн	156	

		Обеспечивать защиту автономных автоматизированных систем программными и программно-аппаратными средствами Использовать программные и программно-аппаратные средства для защиты информации в сети Тестировать функций, диагностировать работоспособности программных и программно-аппаратных средств защиты информации Устранять отказы и восстанавливать работоспособности программных и программно-аппаратных средств защиты информации Решать задачи защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации Применять электронную подпись, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных	ыми и программно-аппаратными средствами		

		Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности Выполнять работу с подсистемами регистрации событий Выявлять события и инцидентов безопасности в автоматизированной системе			
ПП. 03	ПК 3.1-3.5	Установка, монтаж и настройка технических средств защиты информации Техническое обслуживание технических средств защиты информации Применение основных типов технических средств защиты информации Применять основные типы технических средств защиты информации Выявлять технические каналы утечки информации Участвовать в мониторинге эффективности технических средств защиты информации Диагностировать, устранять отказы и неисправности, восстанавливать работоспособности технических средств защиты информации	Защита информации техническими средствами	168	

		Проводить измерения параметров пэмин, созданные техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации Проводить измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации Выявлять технические каналы утечки информации Устанавливать, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей Восстанавливать работоспособности инженерно-технических средств физической защиты			
ПП. 04	ПК 4.1-4.4	Выполнять требования техники безопасности при работе с	Оператор электронно-вычислите	84	

		вычислительной техникой, Организовывать рабочее места оператора электронно-вычислительных и вычислительных машин, Подготовки оборудования компьютерной системы к работе Инсталлировать, настраивать и обслуживать программное обеспечение компьютерной системы Управлять файлами Применять офисное программное обеспечение в соответствии с прикладной задачей Использовать ресурсы локальной вычислительной сети Использовать ресурсы, технологии и сервисов Интернет Применять средства защиты информации в компьютерной системе	льных и вычислительных машин		
ПП. 05	ПК 5.1-5.3	Внедрять программы и методики защиты на объектах Участвовать в оценке качества защиты объекта Готовить организационные документы, регламентирующие	Обеспечение комплексной безопасности объекта защиты		

		работу по защите информации Вести учет работ и объектов, подлежащих защите Анализировать уязвимости системы защиты информации Определять причины возникновения угроз безопасности			
Объем производственной практики в рамках вариативной части ОПОП-П -_612 ак.ч.					

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

2.1. Трудоемкость освоения производственной практики

Код ПП	**Объем, ак.ч.**	**Форма проведения производственной практики** (концентрированно/ рассредоточено)	**Курс / семестр**
ПП. 01	120	концентрированно	3 курс /4 семестр
ПП. 02	156	концентрированно	3 курс /4 семестр
ПП. 03	168	концентрированно	4 курс /5 семестр
ПП. 04	84	концентрированно	2 курс /2 се естр
ПП. 05	84	концентрированно	4 курс /6 семестр
Всего ПП	612	X	X

2.2. Структура производственной практики

Код ПК	**Наименование разделов профессионального модуля**	**Виды работ**	**Наименование тем учебной практики**	**Объе м часов**
ПП 01. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении				120
ПК 1.1. ПК 1.2. ПК 1.3.	Раздел 1. Эксплуатация автоматизированн ых (информационных)	– участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в	Тема 1.1. Основные меры защиты информации в автоматизиров	20

ПК 1.4. ПК 1.5	систем в защищённом исполнении	соответствии с требованиями эксплуатационной документации – обслуживание средств защиты информации прикладного и системного программного обеспечения – настройка программного обеспечения с соблюдением требований по защите информации – настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам – настройка встроенных средств защиты информации программного обеспечения – проверка функционирования встроенных средств защиты информации программного обеспечения – своевременное обнаружение признаков наличия вредоносного программного обеспечения – обслуживание средств защиты информации в компьютерных системах и сетях – обслуживание систем защиты информации в автоматизированных системах – участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем	анных системах	
			Тема 1.2. Защита информации в распределенных автоматизированных системах	20
			Тема 1.3 Администрирование автоматизированных систем	20
			Тема 1.4 Эксплуатация средств защиты информации в компьютерных сетях	20
ВСЕГО ПО РАЗДЕЛУ 1				**80**
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	Раздел 2. Эксплуатация компьютерных сетей	– – проверка работоспособности системы защиты информации автоматизированной системы – контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации – контроль стабильности характеристик системы защиты	Тема 2.1. Начальная настройка коммутатора	10
			Тема 2.2 Адресация сетевого уровня и маршрутизация	10

		информации автоматизированной системы – ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем – участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	Тема 2.3 Функции управления коммутаторами	10
			Тема 2.4 Приоритизация трафика и создание альтернативных маршрутов	10
ВСЕГО ПО РАЗДЕЛУ 2				40
ПП 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами				156
ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.	Раздел 1. Программные и программно-аппаратные средства защиты информации	– Участие в установке и настройку отдельных программных, программно-аппаратных средств защиты информации. – Участие в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. – Участие в тестировании функций отдельных программных и программно-аппаратных средств защиты информации. – – Участие в решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации – – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-	Тема 1.1. Принципы программно-аппаратной защиты информации от несанкционированного доступа	20
			Тема 1.2. Защита программ от изучения	20
			Тема 1.3. Защита программ и данных от несанкционированного копирования	20
			Тема 1.4 Системы обнаружения атак и вторжений	20
			Тема 1.5 Основы построения	20

		аппаратных средств обеспечения информационной безопасности.	защищенных сетей	
		– Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики	Тема 1.6 Изучение современных программно-аппаратных комплексов.	20
ВСЕГО ПО РАЗДЕЛУ 1				**120**
ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.	Раздел 2. Криптографические средства защиты информации	– Участие в обработке, хранении и передаче информации ограниченного доступа. – Участие в уничтожении информации и носителей информации с использованием программных и программно-аппаратных средств. Осуществление регистрации основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. – Анализ принципов построения систем информационной защиты производственных подразделений.	Тема 2.1 Кодирование информации. Компьютеризация шифрования.	12
			Тема 2.2. Алгоритмы обмена ключей и протоколы аутентификации	12
			Тема 2.3. Защита информации в электронных платежных системах	12
ВСЕГО ПО РАЗДЕЛУ 2				36
ПП 03. Защита информации в автоматизированных системах программными и программно-аппаратными средствами				168
ПК 3.1. ПК 3.2.	Раздел 1. Техническая защита информации	– Участие в монтаже, настройке, обслуживании и эксплуатации инженерной и технических средств защиты информации;	Тема 1.1 Методы и средства технической разведки	24

ПК 3.3. ПК 3.4. ПК 3.5		– Участие в монтаже, настройке, обслуживании и эксплуатации средств охраны и безопасности; – Участие в монтаже, настройке, обслуживании и эксплуатации систем видеонаблюдения; – Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	Тема 1.2 Физические процессы при подавлении опасных сигналов	24
			Тема 1.3. Системы защиты от утечки информации	24
			Тема 1.4. Эксплуатация технических средств защиты информации	30
ВСЕГО ПО РАЗДЕЛУ 1				102
ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5	Раздел 2. Инженерно-технические средства физической защиты объектов информатизации	– Участвовать в измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа; – Участвовать в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации; – Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами; – Освоение методики выявления возможных угрозы информационной безопасности объектов защиты; – Участие в организации отдельных работ по физической защите объектов информатизации – Разработка предложений по усовершенствованию	Тема 2.1 Применение инженерно-технических средств физической защиты	30
			Тема 2.2 Эксплуатация инженерно-технических средств физической защиты	36

		технической защиты информации объекта информатизации.		
ВСЕГО ПО РАЗДЕЛУ 2				66
ПП 04. Оператор электронно-вычислительных и вычислительных машин				84
ПК 4.1 - ПК 4.4	Раздел 1 Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения	– Подготовка оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения.	Тема 1.1 Работа с программным обеспечением компьютерной системы	12
ВСЕГО ПО РАЗДЕЛУ 1				12
ПК 4.1 - ПК 4.4	Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах	– Создание и управление текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах.	Тема 2.1 Работа в текстовом процессоре	10
			Тема 2.2. Работа в редакторе электронных таблиц	10
			Тема 2.3. Работа в программе подготовки и просмотра презентаций	10
			Тема 2.4. Работа в системе управления базами данных	10
			Тема 2.5. Работа в графических редакторах	10
ВСЕГО ПО РАЗДЕЛУ 2				50

ПК 4.1 - ПК 4.4	Раздел 3. Использование ресурсов технологий и сервисов Интернета	– Обеспечение защиты информации в компьютерной системе. – Использование ресурсов локальных вычислительных сетей и Интернета.	Тема 3.1. Работа с ресурсами Интернета	22
ВСЕГО ПО РАЗДЕЛУ 3				22
ПП 05. Обеспечение комплексной безопасности объекта защиты				84
ПК 5.1, ПК 5.2, ПК 5.3	Раздел 1. Организация и технология работы с конфиденциальной информацией	– Разработка нормативных документов необходимых для организации работы с персоналом, имеющим доступ к конфиденциальной информации – Разработка политики информационной безопасности – Разработка модели угроз информационной безопасности	Тема 1.1 Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ	20
			Тема 1.2 Организационно-распорядительные документы по обеспечению безопасности объектов в том числе объектов КИИ	20
ВСЕГО ПО РАЗДЕЛУ 1				40
ПК 5.1, ПК 5.2, ПК 5.3	Раздел 2. Обеспечение системы безопасности объекта защиты	– Анализ структуры организации и информационных процессов – Выявление опасностей и угроз объекта информатизации – Анализ структуры и типов защищаемой информации, по видам тайны и степеням конфиденциальности – Анализ существующей системы защиты объекта – Оценка степени защищенности объекта	Тема 2.1 Состав и структура системы безопасности	20
			Тема 2.2 Построение системы защиты информации	24
ВСЕГО ПО РАЗДЕЛУ 2				**44**

2.3. Содержание производственной практики

Наименование разделов профессионального модуля и тем учебной практики	Содержание работ	Объем, ак.ч.
ПП 01. ПМ 01. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		**120**
Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		**80**
Тема 1.1. Основные меры защиты информации в автоматизированных системах	**Содержание**	
	Изучение нормативно-правовой базы для определения мер защиты информации в автоматизированных информационных системах и требований к ним Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	20
Тема 1.2. Защита информации в распределенных автоматизированных системах	**Содержание**	
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	20
Тема 1.3 Администрирование автоматизированных систем	**Содержание**	
	Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Управление, тестирование и эксплуатация автоматизированных систем	20
Тема 1.4 Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	20
Раздел 2. Эксплуатация компьютерных сетей		40
Тема 2.1. Начальная настройка коммутатора	**Содержание**	10
	Команды обновления программного обеспечения коммутатора и	

	сохранения/восстановления конфигурационных файлов. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	
Тема 2.2 Адресация сетевого уровня и маршрутизация	**Содержание**	10
	Основные и расширенные конфигурации маршрутизатора. Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP. Работа с протоколом RIP и OSPF. Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.	
Тема 2.3 Функции управления коммутаторами	**Содержание**	10
	Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
Тема 2.4 Приоритизация трафика и создание альтернативных маршрутов	**Содержание**	10
	Создание альтернативных маршрутов с использованием статической маршрутизации	
Промежуточная аттестация в форме дифференцированного зачета		
ПП 02. ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		156
Раздел 1. Программные и программно-аппаратные средства защиты информации		120
Тема 1.1. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	
	Организация доступа к файлам Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	20
Тема 1.2. Защита программ от изучения	**Содержание**	
	Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям	20
Тема 1.3. Защита программ и данных от несанкционированного копирования	**Содержание**	
	Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	20
Тема 1.4 Системы обнаружения атак и вторжений	**Содержание**	
	Обнаружение и предотвращение вторжений.	20

	Возможности IDPS. Сильные стороны и ограниченность IDPS.	
Тема 1.5 Основы построения защищенных сетей	**Содержание**	
	Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	20
Тема 1.6 Изучение современных программно-аппаратных комплексов.	**Содержание**	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	20
Раздел 2. Криптографические средства защиты информации		36
Тема 2.1 Кодирование информации. Компьютеризация шифрования.	**Содержание**	
	Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII. Изучение современных программных и аппаратных криптографических средств	12
Тема 2.2. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание**	
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	12
Тема 2.3. Защита информации в электронных платежных системах	**Содержание**	
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	12
Промежуточная аттестация в форме дифференцированного зачета		
ПП 03. ПМ 03 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		168
Раздел 1. Техническая защита информации		102
Тема 1.1 Методы и средства технической разведки	**Содержание**	24
	Изучение характеристик наземных средств дистанционного съема информации Анализ современных средств перехвата сигналов	

Тема 1.2 Физические процессы при подавлении опасных сигналов	**Содержание**	24
	Изучение пассивных методов подавления опасных сигналов акустоэлектрических преобразователей Изучение активных методов подавления опасных сигналов акустоэлектрических преобразователей	
Тема 1.3. Системы защиты от утечки информации	**Содержание**	24
	Средства акустической разведки Закладные устройства Защита от утечки по виброакустическому каналу Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок.	
Тема 1.4. Эксплуатация технических средств защиты информации	**Содержание**	30
	Установка и настройка технических средств защиты информации Оценка функционирования средств защиты информации от несанкционированного доступа	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		66
Тема 2.1 Применение инженерно-технических средств физической защиты	**Содержание**	30
	Организация пропускного режима на КПП, система автоматического управления Определение путей проникновения злоумышленника на объект информатизации Внутриобъектовый режим. Интегрированные охранные системы	
Тема 2.2 Эксплуатация инженерно-технических средств физической защиты	**Содержание**	36
	Изучение принципов диагностики, устранения отказов и восстановление работоспособности технических средств физической защиты	
Промежуточная аттестация в форме дифференцированного зачета		
ПП 04. ПМ 04 Оператор электронно-вычислительных и вычислительных машин		84
Раздел 1 Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		12
Тема 1.1 Работа с программным обеспечением компьютерной системы	**Содержание**	
	Подключение, настройка и подготовка к работе периферийного оборудования Установка и замена расходных материалов для принтеров, ксерокса, сканера Установка прикладных программ	12

Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах		50
Тема 2.1 Работа в текстовом процессоре	**Содержание**	10
	Форматирование и редактирование шрифтов, абзацев и формул Форматирование и редактирование списков Работа с таблицами в текстовом процессоре Работа с графическими объектами в текстовом процессоре Форматирование документа в целом. Способы вывода документа на печать	
Тема 2.2. Работа в редакторе электронных таблиц	**Содержание**	10
	Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице. Работа со встроенными функциями в электронной таблице. Создание и работа с диаграммами и графиками. Обмен данными между текстовым процессором и электронной таблицей	
Тема 2.3. Работа в программе подготовки и просмотра презентаций	**Содержание**	10
	Основы работы со слайдом. Работа в презентации со шрифтом и текстом. Понятие темы слайда Добавление в слайды рисунков, звуковых эффектов, таблиц и диаграмм Настройка анимации объектов. Настройка показа и демонстрация результатов работы средствами мультимедиа	
Тема 2.4. Работа в системе управления базами данных	**Содержание**	10
	Ввод данных в таблицы базы данных Создание простых запросов и форм. Создание и форматирование главной кнопочной формы. Создание отчетов.	
Тема 2.5. Работа в графических редакторах	**Содержание**	10
	Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики.	
Раздел 3. Использование ресурсов технологий и сервисов Интернета		22
Тема 3.1. Работа с ресурсами Интернета	**Содержание**	22
	Настройка парольной защиты на открытие и запись файла	

	Настройка защиты документа с помощью прав доступа Защита информации в приложениях MS Office.	
Промежуточная аттестация в форме дифференцированного зачета		
УП 05. ПМ 05. Обеспечение комплексной безопасности объекта защиты		84
Раздел 1. Организация и технология работы с конфиденциальной информацией		40
Тема 1.1 Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ	**Содержание**	
	Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31 Определение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Анализ приказа № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» Классификация уязвимостей информационной системы, причины возникновения угроз безопасности Проектирование системы безопасности значимого объекта КИИ Состав системы безопасности значимых объектов.	20
Тема 1.2 Организационно-распорядительные документы по обеспечению безопасности объектов в том числе объектов КИИ	**Содержание**	
	Изучение порядка и правил функционирования системы безопасности значимых объектов КИИ Анализ приказа Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» Разработка рабочей и эксплуатационной документации. Определение порядка и правил обеспечения безопасности объектов	20
Раздел 2. Обеспечение системы безопасности объекта защиты		44
Тема 2.1 Состав и структура системы безопасности	**Содержание**	
	Состав и структура системы безопасности. Направления защиты объекта информатизации.	22

	Средства и способы защиты. Организации работы в чрезвычайной ситуации. Состав службы безопасности.	
Тема 2.2 Построение системы защиты информации	**Содержание**	
	Определение угроз информационной безопасности Выделение недостатки существующей КСЗИ. Анализ рисков КСЗИ. Усовершенствование организационного обеспечения и СКУД объекта защиты Усовершенствование инженерно-технического обеспечение комплексной системы защиты информации Усовершенствование программно-аппаратного обеспечения комплексной системы защиты информации Анализ рисков разработанной КСЗИ	24
Промежуточная аттестация в форме дифференцированного зачета		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение производственной практики

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся (далее – Профильные организации).

База прохождения производственной практики должна быть укомплектована оборудованием, техническими средствами обучения в объеме, позволяющем выполнять определенные виды работ, связанные с будущей профессиональной деятельностью обучающихся. База практики должна обеспечивать безопасные условия труда для обучающихся.

При определении мест производственной практики (по профилю специальности) для лиц с ограниченными возможностями здоровья учитываются рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации, относительно рекомендованных условий и видов труда.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Наименование.

Разработчики рабочей программы выбирают не менее одного издания из приведенного в ПОП-П перечня печатных и/или электронных образовательных изданий для использования в образовательном процессе. Электронные ресурсы (не учебные издания) указываются в дополнительных источниках. Список может быть дополнен другими изданиями.

*Списки литературы оформляются **в алфавитном порядке** в соответствии с ГОСТ Р 7.0.100–2018 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления» (утв. приказом № 1050-ст Федерального агентства по техническому регулированию и метрологии (Росстандартом) от 03 декабря 2018 года).*

3.2.2. Дополнительные источники *(при необходимости)*

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.

2. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018 – 336с.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-fed eralnyj-zakon-ot-26-iyulya-2017-g-n-187-fz.

4. Постановление Правительства РФ № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_291398 .

5. Приказ Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://rg.ru/2018/02/13/fstek-prikaz-227-site-dok.html .

6. Давыдова, Е. М. Организация защиты объектов критической информационной инфраструктуры: Учебно-методическое пособие [Электронный ресурс] / Е. М. Давыдова, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 20 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10003.

3.2.2. Дополнительные источники (при необходимости)

1. Котеров Д.В. PHP 5 в подлиннике. – СПб.: БХВ-Петербург, 2018. – 1104 с.

2. Федеральный образовательный портал «Информационно - коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832. Дата обращения 23.07.2022.

3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2019. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

4. Федеральный образовательный портал «Информационно - коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832

3.3. Общие требования к организации производственной практики

Производственная практика проводится в профильных организациях на основе договоров, заключаемых между образовательным организацией СПО и профильными организациями.

В период прохождения производственной практики обучающиеся могут зачисляться на вакантные должности, если работа соответствует требованиям программы производственной практики.

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

Производственная практика реализуются в форме практической подготовки и проводится непрерывно.

3.4 Кадровое обеспечение процесса производственной практики

Организацию и руководство производственной практикой осуществляют руководители практики от образовательной организации и от профильной организации.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Индекс УП	Код ПК, ОК	Основные показатели оценки результата	Формы и методы контроля и оценки
УП 01	ПК 1.1.	Демонстрирует умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 1.2.	Проявляет умения и практический опыт администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 1.3.	Проводит перечень работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 1.4.	Проявляет 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	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

УП 02	ПК 2.1.	Демонстрирует умения и навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.2.	Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.3.	Выполняет перечнь работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.4.	Проявляет знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ,

			оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.5.	Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 2.6.	Проявляет знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
УП 03	ПК 3.1	Демонстрирует умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.2	Проявляет умения и практический опыта в эксплуатации технических средств защиты информации в	Тестирование, экзамен квалификационный,

		соответствии с требованиями эксплуатационной документации	экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.3.	Проводит работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.4	Проводит самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 3.5	Проявляет знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

УП 04	ПК 4.1.	Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 4.2	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных	
	ПК 4.3	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	
	ПК 4.4	Применение средств защиты информации в компьютерной системе	
УП 05	ПК 5.1	Участвует в оценке качества защиты объекта Управляет защитой информации на объектах информатизации Проводит аудит защищенности информации на объекте информатизации Внедряет организационные меры по защите информации на объекте информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 5.2	Готовит организационные документы, регламентирующие работу по защите информации Ведёт учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации Разрабатывает организационно-распорядительные документы по защите информации на объектах защиты	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
	ПК 5.3	Проводит анализ уязвимостей системы защиты информации	Тестирование, экзамен квалификационный,

		Определяет причины возникновения угроз безопасности Находит уязвимости системы защиты информации Разрабатывает модели угроз модели угроз объекта информатизации	экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике