

Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

на заседании педагогического совета

Протокол № 2

«26» декабря 2023 г.



Директор СПб ГБПОУ «АУТСГиП»

В.М. Кривонос

«26» декабря 2023 г.

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация

Техник по защите информации

Форма обучения

очная

Санкт-Петербург
2023 год

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553.

СОГЛАСОВАНО

ООО «ДЖИ-ТИ ИНВЕСТ»

Генеральный директор

 П.С. Тюганов

«26» декабря 2023 г.



Рабочая программа профессионального модуля рассмотрена на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Рабочая программа профессионального модуля рассмотрена на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С.



СО Д Е Р Ж А Н И Е

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
1.1. Область применения рабочей программы	4
1.2. Цель и планируемые результаты освоения профессионального модуля	4
1.2.1 Перечень общих компетенций	4
Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	4
1.2.2 Перечень профессиональных компетенций	4
Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	5
1.3. Количество часов, отводимое на освоение профессионального модуля.....	7
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	8
2.1. Структура профессионального модуля.....	8
2.2. Тематический план и содержание профессионального модуля (ПМ.01).....	9
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	22
3.1. Материально-техническое обеспечение	22
3.2. Информационное обеспечение обучения	22
3.3. Кадровое обеспечение образовательного процесса.....	23
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	24

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля разработана с целью формирования дополнительных компетенций, умений и знаний, необходимых для обеспечения лучшей подготовки выпускников и возможности продолжения ими образования, в рамках вариативной части программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», с учетом требований ФГОС (утв. приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553).

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и соответствующие ему профессиональные компетенции, общие компетенции.

1.2.1 Перечень общих компетенций

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

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
<i>ПК 2.7.</i>	<i>Администрирование компонентов ИТ-инфраструктуры</i>
<i>ПК 2.8</i>	<i>Обеспечение мер по информационной безопасности сетевой инфраструктуры и ее компонентов</i>
<i>ПК 2.9.</i>	<i>Проведение анализа компонентов ИТ-инфраструктуры на наличие уязвимостей</i>
<i>ПК 2.10.</i>	<i>Проведение мониторинга и анализа инцидентов информационной безопасности</i>

В результате освоения профессионального модуля студент должен:

иметь практический опыт в:	<ul style="list-style-type: none"> — установки, настройки программных средств защиты информации в автоматизированной системе; — обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; — тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ; — решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; — применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; — учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; — выявления событий и инцидентов безопасности в автоматизированной системе.
знать:	<ul style="list-style-type: none"> — особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; — методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; — типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; — основные понятия криптографии и типовых криптографических методов и средств защиты информации; — особенности и способы применения программных и программно-аппаратных

	<p>средств гарантированного уничтожения информации;</p> <ul style="list-style-type: none"> — типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. — <i>принципы виртуализации.</i> — <i>различные методологии поиска уязвимостей информационных ресурсов, компьютерных сетей и приложений.</i> — <i>популярные методы компьютерных атак</i> — <i>основные способы защиты от атак на типовые уязвимости</i> — <i>основные методы сбора информации для расследования инцидента.</i> — <i>принципы функционирования, способы настройки и управления различными операционными системами и серверами.</i> — <i>способы настройки сетевого оборудования и программного обеспечения.</i>
уметь:	<ul style="list-style-type: none"> — устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; — устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; — 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 — <i>администрировать веб-сервера, почтовые сервера, прокси.</i> — <i>настраивать межсетевые экраны, маршрутизаторы, сетевое оборудование и программное обеспечение.</i> — <i>работать с кластерными файловыми системами, организовывать RAID-массивы.</i> — <i>настраивать виртуальные частные сети.</i> — <i>организовывать удаленный доступ к ресурсам.</i> — <i>устанавливать и настраивать безопасную конфигурацию операционной си-</i>

	<p><i>стемы, серверов и программного обеспечения с учетом предъявляемых требований.</i></p> <ul style="list-style-type: none"> – <i>использовать штатные и специальные средства мониторинга безопасности операционных систем</i> – <i>работать со сканерами уязвимости</i> – <i>осуществлять мониторинг и анализ инцидентов информационной безопасности, в том числе и анализ системных журналов и логов.</i>
--	--

1.3. Количество часов, отводимое на освоение профессионального модуля

№	Вид учебной работы	Объем часов
1.	Объем работы обучающихся во взаимодействии с преподавателем	794
в том числе:		
	теоретическое обучение	214
	практические занятия	260
	учебная практика	72
	производственная практика	216
	Промежуточная аттестация в форме экзамена	12
2.	Самостоятельная внеаудиторная работа обучающихся	90
Всего по ПМ.02 в рамках образовательной программы		874

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды ОК, ПК	Наименования разделов профессионального модуля	Общий объем нагрузки, акад. час	Объем профессионального модуля, акад. час						
			Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа
			Всего	в том числе					
				в форме практической подготовки	лабораторные и практические занятия	курсовая работа, проект	учебная практика	производственная практика	
ПК 2.1- ПК 2.6 ОК 1-ОК 10	Раздел 1. Применение программных и программно-аппаратных средств защиты информации	252	222	68	134	20			30
ПК 2.1- ПК 2.6 ОК 1-ОК 10	Раздел 2. Применение криптографических средств защиты информации	94	74	64	10				20
ПК 2.1 - ПК 2.6 ОК 1-ОК 10	Раздел 3. Кибербезопасность	228	198	82	116				30
УП.02	Учебная практика	72	72				72		
ПП.02	Производственная практика	216	216					216	
	Промежуточная аттестация	12							
	Итого	874	782	214	260	20	72	216	80

2.2. Тематический план и содержание профессионального модуля (ПМ.01)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
Раздел 1. Программные и программно-аппаратные средства защиты информации		222
МДК.02.01. Программные и программно-аппаратные средства защиты информации		198
Тема 1.1. Общие понятия программно-аппаратных средств защиты информации	Содержание учебного материала	6
	1.1.1. Виды программно-аппаратных средств защиты информации	
	1.1.2. Понятие комплексных решений SIEM.	
	1.1.3. Методы скрытия информации	
	Практические занятия	
Практическое занятие № 1 Сравнительный анализ продуктов SIEM	2	
Тема 1.2. Защита программ и данных	Содержание учебного материала	6
	1.2.1. Структура и функции подсистемы безопасности операционных систем	
	1.2.2. Подсистема безопасности Windows. Подсистема безопасности Linux	
	1.2.3. Средства обеспечения защиты информации в системах управления базами данных	
Тема 1.3. Защита в компьютерных сетях	Содержание учебного материала	8
	1.3.1. Средства защиты в вычислительных сетях	
	1.3.2. Защита информации в VPN-сетях	
	1.3.3. Защита электронной почты	
	1.3.4. Защита web-приложений и электронной подписи от мошенничества	
Тема 1.4. Антивирусная защита данных	Содержание учебного материала	2
	1.4.1. Современные программные средства для защиты от вредоносных программ	2
	Практические занятия Практическое занятие № 2 Создание загрузочной флешки с антивирусной программой для быстрой проверки	
Тема 1.5. Средства защиты на компьютерах с операционной	Содержание учебного материала 1.5.1. Использование Active Directory и политик безопасности. Понятие домена. Роли контроллера домена	6

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
системой Windows	1.5.2. Средство защиты информации Secret Net Studio Возможности Secret Net Studio. Принцип работы. Параметры установки	
	1.5.3. Средства защиты информации Dallas Lock Возможности Dallas Lock. Принцип работы. Параметры установки	
	Практические занятия	30
	Практическое занятие № 3 Установка серверной версии Windows	
	Практическое занятие № 4 Установка домена Active Directory	
	Практическое занятие № 5 Создание и внесение пользователей и компьютеров в домен	
	Практическое занятие № 6 Создание и применение глобальных политик домена	
	Практическое занятие № 7 Создание и применение локальных политик домена	
	Практическое занятие № 8 Установка сервера безопасности Secret Net Studio	
	Практическое занятие № 9 Установка клиента и программы управления Secret Net Studio	
	Практическое занятие № 10 Настройка централизованной установки клиента Secret Net Studio	
	Практическое занятие № 11 Работа с действующими средствами локальной защиты с помощью Secret Net Studio	
	Практическое занятие № 12 Удаление всех компонентов Secret Net Studio	
	Практическое занятие № 13 Установка Dallas Lock	
	Практическое занятие № 14 Настройка средств администрирования в Dallas Lock	
	Практическое занятие № 15 Настройка подсистем управления доступом в Dallas Lock	
	Практическое занятие № 16 Разграничение доступа к объектам файловой системы в Dallas Lock	
Практическое занятие № 17 Работа с подсистемой регистрации и учёта в Dallas Lock		
Тема 1.6 Использование DLP-системы Infowatch для защиты от внутренних утечек информации	Содержание учебного материала	12
	1.6.1. Общая характеристика и принципы функционирования dlp-системы Infowatch	
	1.6.2. Виды политик, способы их создания в Traffic monitor	
	1.6.3. Принципы построения регулярных выражений для создания политик	
	1.6.4. Виды правил и способы создания правил в Device monitor	
	1.6.5. Ложные срабатывания политик	

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
	1.6.6. Принципы мониторинга событий информационной безопасности в DLP-системе Infowatch Практические занятия Практическое занятие № 18 Установка и настройка Traffic monitor Практическое занятие № 19 Установка и настройка Device monitor Практическое занятие № 20 Установка клиента Device monitor Практическое занятие № 21 Установка и настройка Crawler Практическое занятие № 22 Создание правил и проверка их работоспособности в Device monitor Практическое занятие № 23 Создание правил с использованием «белых» и «чёрных» списков в Device monitor Практическое занятие № 24 Работа с Задачами и Журналом в Device monitor Практическое занятие № 25 Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor Практическое занятие № 26 Работа с терминами и списками в Traffic monitor Практическое занятие № 27 Работа с тегами и объектами в Traffic monitor Практическое занятие № 28 Создание политик защиты данных в Traffic monitor Практическое занятие № 29 Создание политик защиты данных на агентах в Traffic monitor Практическое занятие № 30 Создание политик контроля персон в Traffic monitor Практическое занятие № 31 Создание политик с использованием правил передачи в Traffic monitor Практическое занятие № 32 Создание политик с использованием правил копирования в Traffic monitor Практическое занятие № 33 Создание политик с использованием правил хранения в Traffic monitor Практическое занятие № 34 Создание политик с использованием правил работы в приложениях в Traffic monitor Практическое занятие № 35 Создание политик с использованием регулярных выражений в Traffic monitor Практическое занятие № 36 Создание и изменение виджетов в Traffic Monitor Практическое занятие № 37 Создание и изменение отчётов в Traffic Monitor	40

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
Тема 1.7. Методики проверки защищённости объектов информатизации	Содержание учебного материала	8
	1.7.1. Методики проверки защищённости объектов информатизации на соответствие требованиям нормативных правовых актов	
	1.7.2. Нормативно-методические документы, регламентирующие порядок проведения аттестации объектов информатизации и содержащие требования к объектам информатизации	
	Практические занятия	2
	Практическое занятие № 38 Работа с требованиями и рекомендациями по технической защите конфиденциальной информации	
Практическое занятие № 39 Работа с нормативно-правовой документацией, регламентирующей порядок проведения аттестации объектов информатизации		
Тема 1.8. Использование программно-аппаратных	Содержание учебного материала	8
	1.8.1. Общая характеристика продуктов ViPNet для создания защищённой сети	
	1.8.2. Понятие построения виртуальной защищённой сети, межсетевой взаимодействие защищённых сетей	
	Практические занятия	18
	Практическое занятие № 40 Развёртывание защищённой сети ViPNet. Учет отказов в работе средств вычислительной техники.	
	Практическое занятие № 41 Создание структуры защищённой сети ViPNet	
	Практическое занятие № 42 Создание защищённой сети ViPNet	
	Практическое занятие № 43 Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet	
	Практическое занятие № 44 Модификация защищённой сети ViPNet	
	Практическое занятие № 45 Компрометация ключей в защищённой сети ViPNet	
Практическое занятие № 46 Настройка политик безопасности в ViPNet Policy Manager		
Практическое занятие № 47 Организация межсетевого взаимодействия		
Практическое занятие № 48 Модификация межсетевого взаимодействия в защищённой сети ViPNet		
Тема 1.9. Защита передачи	Содержание учебного материала	6

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
данных через Интернет	1.9.1. Понятие https. Технология Secure Socket Layer (SSL)	16
	1.9.2. Сертификаты, подписанные центром сертификации (CA).	
	1.9.3. Сертификаты домена. Самозаверяющие сертификаты.	
	Практические занятия	
	Практическое занятие № 49 Установка openssl в centos	
	Практическое занятие № 50 Создание самоподписанного сертификата SSL	
	Практическое занятие № 51 Заполнение анкеты для сертификата	
	Практическое занятие № 52 Применение сертификата	
	Практическое занятие № 53 Перемещение ssl-сертификата с сервера windows на сервер, отличный от window	
	Практическое занятие № 54 Установка Nginx для последующей настройки прокси-сервера	
	Практическое занятие № 55 Настройка прокси-сервера с помощью Nginx	
	Практическое занятие № 56 Настройка правильной работы ssl при использовании Nginx	
Тема 1.10 Средства защиты на компьютерах с операционной системой Linux	Содержание учебного материала	6
	1.10.1. Средства защиты компьютерных сетей с использованием Samba и политик безопасности на Linux-сервере. Особенности серверов на Linux. Программные средства для поднятия контроллера домена на Linux	
	1.10.2. Принципы использования систем обнаружения вторжения	
	1.10.3. Синтаксис написания правил для IDS систем	
	Практические занятия	22
	Практическое занятие № 57 Установка серверной версии Ubuntu	
	Практическое занятие № 58 Установка Samba	
	Практическое занятие № 59 Настройка Samba	
	Практическое занятие № 60 Конфигурирование BIND9 на контроллере домена Ubuntu Server	
	Практическое занятие № 61 Установка системы обнаружения и предотвращения вторжения Snort	
Практическое занятие № 62 Настройка системы обнаружения и предотвращения вторжения Snort		
Практическое занятие № 63 Настройка записи предупреждений о вторжениях в базу данных		

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
	Практическое занятие № 64 Установка пакетов для веб-интерфейса IDS Snort Практическое занятие № 65 Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort Практическое занятие № 66 Применение правил для IDS Snort. Синтаксис правил Практическое занятие № 67 Проверка настроенных правил в IDS Snort с помощью сканирования портов	
Самостоятельная работа	Заполнение рабочей тетради для самостоятельных работ по МДК.02.01	30
Раздел 2. Криптографические средства защиты информации		114
МДК.02.02. Криптографические средства защиты информации		94
Тема 2.1. Основные термины и определения	Содержание учебного материала 2.1.1 Основные термины и определения в криптографии 2.2.2 Основные требования, предъявляемые к криптосистемам	4
Тема 2.2. Классификация шифров	Содержание учебного материала 2.2.1. Шифры замены. Основы шифрования. Шифры однозначной замены. Полиграммные шифры. 2.2.2. Шифры перестановки. Шифры гаммирования. Шифры одинарной перестановки. Шифры множественной перестановки. Генерация гаммы. RC4. 2.2.3. Шифрование с открытым ключом. Алгоритм RSA. Алгоритм на основе задачи об укладке ранца. 2.2.4. Вероятностное шифрование. Алгоритм шифрования Эль-Гамала. Алгоритм на основе эллиптических кривых. 2.2.5. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений. 2.2.6. DES-алгоритм. Усложнения DES-алгоритма. Шифр AES. Российский стандарт шифрования ГОСТ-28147.	12
	Практические занятия Практическое занятие № 1 Алгоритмизация шифра Цезаря	4

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
	Практическое занятие №2 Декодирование моноалфавитного подстановочного шифра частотным методом	
Тема 2.3. Криптографические протоколы	Содержание учебного материала	20
	2.3.1. Понятие криптографических протоколов. Классификация.	
	2.3.2. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана-Меркла	
	2.3.3. Протоколы аутентификации. Протоколы идентификации	
	2.3.4. Протоколы электронной цифровой подписи. Протокол на базе алгоритма RSA. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.	
	2.3.5. Протокол взаимоблокировки. Протокол Ву-Лама	
	2.3.6. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамала	
	2.3.7. Протоколы обмена ключами. Протокол Kerberos	
	2.3.8. Ключевые функции хеширования. Бесключевые функции хеширования. Хеш-функции. MD5. Применение шифрования для получения хеш-образа.	
	2.3.9. Протоколы защиты данных в сети Internet. Протоколы IPSec, AH, ESP, ISAKMP, Oakley. Протокол SSL	
2.3.10. Протоколы электронных платежей. Цифровые деньги		
	Практические занятия	4
	Практическое занятие № 3 Метод шифрования с открытым ключом RSA	
	Практическое занятие № 4 Разработка хэш-функции	
Тема 2.4. Основы криптоанализа	Содержание учебного материала	12
	2.4.1. временные симметричные криптосистемы. Принцип итерирования. Конструкция Фейтстеля.	
	2.4.2. Угрозы безопасности при использовании криптографии. Общие сведения о криптоанализе.	
	2.4.3. Линейный криптоанализ. Дифференциальный криптоанализ	
	2.4.4. Методы криптоанализа блочных шифров. Атаки на блочные шифры. Частотный анализ. Метод полного перебора	
	2.4.5. Методы взлома шифров сложной замены	
	2.4.6. Кодирование информации. Общедоступные кодовые системы. Секретные кодовые системы.	

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
Тема 2.5. Стеганография	Содержание учебного материала	16
	2.5.1. Классическая стеганография	
	2.5.2. Цифровая стеганография	
	2.5.3. Стеганографические протоколы.	
	2.5.4. Стеганография с открытым ключом	
	2.5.5. Стегосистемы: методы, требования, ограничения.	
	2.5.6. Методы сокрытия и обнаружения информации в изображениях	
	2.5.7. Методы сокрытия и обнаружения информации в аудиофайлах	
	2.5.8. Методы сокрытия и обнаружения информации в видеофайлах	
	Практические занятия Практическое занятие № 5 Анализ графических изображений на наличие скрытой информации.	
Самостоятельная работа Заполнение рабочей тетради для самостоятельных работ по МДК.02.02		20
Раздел 3. Кибербезопасность		202
МДК.02.03. Кибербезопасность		202
Тема 3.1. Установка и настройка Windows Server 2019	Содержание темы	12
	3.1.1. Обзор Windows Server 2019. Развертывание и управление Windows Server 2019	
	3.1.2. Доменные сервисы Службы Каталога. Введение в AD DS.	
	3.1.3. AD DS. Обзор функций контроллера домена. Установка контроллера домена	
	3.1.4. Настройка удаленного управления в Windows Server 2019	
	3.1.5. Групповые политики в Windows Server 2019	
	3.1.6. Серверы времени и лицензирования. Центр сертификации.	
	Практические занятия	14
	Практическое занятие № 1. Установка и настройка Windows Server 2019	
	Практическое занятие № 2. Установка контроллера домена. Использование Windows PowerShell для	

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
	администрирования AD DS. Практическое занятие № 3. Установка ролей сервера Windows Server 2019 Практическое занятие № 4. Подключение сетевых периферийных устройств через ГП Практическое занятие № 5. Установка и настройка сервера времени и сервера лицензирования Практическое занятие № 6. Управление пользовательским рабочим столом через ГП Практическое занятие № 7. Установка, настройка и устранение неполадок роли сервер	
Тема 3.2. Администрирование Windows Server 2019	Содержание темы 3.2.1. Управление службой DNS и устранение неполадок 3.2.2. Настройка DHCP в Windows Server 2019 3.2.3. Защита доступа к сети. Настройка NAP 3.2.4. Реализация безопасности клиентских систем. 3.2.5. Внедрение управления обновлениями. Обзор WSUS. Развертывание обновлений посредством WSUS 3.2.6. Создание общих файлов в домене	12
	Практические занятия Практическое занятие № 8. Применение технологии DirectAccess с помощью мастера начальной настройки Практическое занятие № 9. Развертывание расширенной инфраструктуры DirectAccess Практическое занятие № 10. Внедрение VPN Практическое занятие № 11. Настройка шифрования и расширенного аудита Практическое занятие № 12. Использование службы развертывания Практическое занятие № 13. Внедрение управления обновлениями. Практическое занятие № 14. Настройка файлового сервера Практическое занятие № 15. Настройка DHCP Практическое занятие № 16. Настройка центра сертификации Практическое занятие № 17. Настройка групповых политик Практическое занятие № 18. Добавление рабочих станций в домен	22

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
Тема 3.3. Установка и администрирование Linux	Содержание темы	10
	3.3.1. Администрирование ОС на базе Linux	
	3.3.2. Развертывание веб-серверов Linux	
	3.3.3. Лог-файлы и мониторинг. Атрибуты файлов и права доступа	
	3.3.4. Управление пакетами при помощи RPM и yum Управление системными сервисами	
	3.3.5 Аутентификация LDAP	36
	Практические занятия	
	Практическое занятие № 19. Установка сервера Debian.	
	Практическое занятие № 20. Настройка web-сервера в ОС Debian.	
	Практическое занятие № 21. Настройка сервера DNS в ОС Debian.	
	Практическое занятие № 22. Настройка сервера DHCP в ОС Debian.	
	Практическое занятие № 23. Настройка файловых серверов в ОС Debian	
	Практическое занятие № 24. Настройка контейнеров Docker.	
	Практическое занятие № 25. Установка сервера CentOS.	
	Практическое занятие № 26. Настройка web-сервера в CentOS.	
	Практическое занятие № 27. Настройка сервера DNS в CentOS.	
	Практическое занятие № 28. Настройка сервера DHCP в CentOS.	
	Практическое занятие №29. Установка и настройка OpenVPN	
	Практическое занятие №30. Применение протокола IPsec и SSH.	
	Практическое занятие №31. Настройка регистрации действий	
Практическое занятие № 32. Установка и настройка OpenLDAP		
Практическое занятие № 33. Установка и настройка IPtables		
Практическое занятие № 34. Установка и базовая настройка Kali Linux		
Практическое занятие № 35. Администрирование Kali Linux		
Практическое занятие №36. Установка и настройка утилит в Kali Linux		
Тема 3.4. Основы кибербезопасности	Содержание темы 3.4.1. Основные проблемы обеспечения кибербезопасности	10

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего	
	Практическое занятие № 49. Анализ уязвимостей серверов		
	Практическое занятие № 50. Поиск и устранение неисправностей сети с помощью MegaPing		
Тема 3.6. Защита информационной инфраструктуры	Содержание темы	10	
	3.6.1. Методы защиты информационной инфраструктуры		
	3.6.2. Использование межсетевых экранов		
	3.6.3. Безопасность операционных систем		
	3.6.4. Основные способы защиты информационных систем		
	3.6.5. Повышение уровня защищенности ИИ		
	Практические занятия		
Тема 3.7. Расследование инцидентов	Практическое занятие № 51. Настройка межсетевого экрана	6	
	Практическое занятие № 52. Настройка параметров безопасности Windows.		
	Практическое занятие № 53. Составление рекомендаций по повышению уровня защищенности информационной инфраструктуры		
		Содержание темы	10
		3.7.1. Понятие и виды компьютерных преступлений. Основные стадии компьютерного преступления	
		3.7.2. Идентификация нападающего. Мотивация нарушителей.	
		3.7.3. Анализ технических аспектов нападения.	
3.7.4. Типовые действия, выполняемые в рамках процесса управления инцидентами. Идентификация инцидента. Реагирование на инцидент ИБ. Восстановление после инцидента ИБ.			
3.7.5. Оценка ущерба от произошедшего нарушения информационной безопасности. Устранение негативных последствий инцидентов			
	Практические занятия	4	
	Практическое занятие № 54. Выявление предпосылок и обстоятельств, приведших к возникновению компьютерного инцидента.		
	Практическое занятие № 55. Обнаружение события информационной безопасности. Оценка события информационной безопасности		

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов всего
Тема 3.8. Поиск информации по открытым источникам	Содержание темы	4
	3.8.1. Методы социальной инженерии	
	3.8.2. Исследование на основе открытых источников. Инструменты OSINT	
	Практические занятия	6
	Практическое занятие № 56. Исследование открытой информации в поисковых системах	
	Практическое занятие № 57. Поиск информации в социальных сетях	
Практическое занятие № 58. Поиск информации с помощью утилит		
Курсовая работа		20
Тематика курсовых работ «Организация защиты от внутренних угроз в организации с использованием DLP-системы» по индивидуальным вариантам		20
Учебная практика		108
Производственная практика		180
Промежуточная аттестация		18
Всего		1112

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Реализация программы профессионального модуля требует лаборатории «Технических средств защиты информации, программно-аппаратных средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочие столы и стулья по количеству обучающихся;
- компьютеры с лицензионным программным обеспечением и мультимедиапроектор, экран.

Оборудование полигона подразделение защиты информации:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий, в т.ч. на электронных носителях.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением на каждом посадочном месте обучающихся и на рабочем месте преподавателя

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Шишов, О. В. Современные технологии и технические средства информатизации : учебник / О.В. Шишов. — Москва : ИНФРА-М, 2021. — 462 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011776-8. - Текст : электронный. – Режим доступа: сетевой доступ URL: <https://znanium.com/catalog/product/1215864> (дата обращения: 24.02.2022).

Дополнительная литература

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Режим доступа: сетевой доступ URL: <https://urait.ru/bcode/495524> (дата обращения: 24.02.2022).
2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образова-

тельная платформа Юрайт [сайт]. Режим доступа: сетевой доступ URL: <https://urait.ru/bcode/496741> (дата обращения: 24.02.2022).

3. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мещатунян. — Москва : ФОРУМ : ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. Режим доступа: сетевой доступ: <https://znanium.com/catalog/product/1189337> (дата обращения: 24.02.2022).
4. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Режим доступа: сетевой

3.3. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарным курсам: высшее педагогическое или высшее техническое образование.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: высшее педагогическое или высшее техническое образование.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
<p>Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.</p>	<p>установка и настройка отдельных программных, программно-аппаратных средств защиты информации.</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
<p>Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.</p>	<p>защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
<p>Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.</p>	<p>тестирование функций отдельных программных и программно-аппаратных средств защиты информации.</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики</p>

		Экзамен по ПМ.
Осуществлять обработку, хранение и передачу информации ограниченного доступа.	обработка, хранение и передача информации ограниченного доступа.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Уничтожение информации и носителей информации с использованием программных и программно-аппаратных средств.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
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.	регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Администрирование компонентов ИТ-инфраструктуры	Администрирование компонентов ИТ-инфраструктуры	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения само-

		<p>стоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
Обеспечение мер по информационной безопасности сетевой инфраструктуры и ее компонентов	меры по информационной безопасности сетевой инфраструктуры и ее компонентов	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
Проведение анализа компонентов ИТ-инфраструктуры на наличие уязвимостей	анализ компонентов ИТ-инфраструктуры на наличие уязвимостей	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
Проведение мониторинга и анализа инцидентов информационной безопасности	мониторинг и анализ инцидентов информационной безопасности	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Наблюдения при выполнении практических работ и</p>

		наблюдение в процессе практики Экзамен по ПМ.
Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области; собственная оценка эффективности и качества выполнения заданий.	Проверка качества выполнения практических работ, проверка отчетной документации по практике
Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	эффективный поиск необходимой информации; использование различных источников, включая электронные	Анализ результатов практических работ
Планировать и реализовывать собственное профессиональное и личностное развитие	Эффективное планирование профессионального и личного развития	Анализ результатов практических работ
Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	взаимодействие с обучающимися, преподавателями в ходе обучения работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	взаимодействие с обучающимися, преподавателями в ходе обучения	Анализ результатов практических работ
Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности	Соблюдение режима труда и отдыха, здоровьесберегающих технологий в процессе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

сти и поддержания необходимого уровня физической подготовленности		
Использовать информационные технологии в профессиональной деятельности	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ
Пользоваться профессиональной документацией на государственном и иностранном языках	работа с различными источниками информации	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Анализ результатов практических работ
Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	Использование приемов предпринимательской деятельности в процессе решения профессиональных задач	Анализ результатов практических работ