Автономная некоммерческая образовательная организация
профессионального образования
«Санкт-Петербургская академия милиции имени Н.А. Щёлокова»
(АНОО ПО «СПб АМ им. Н.А. Щёлокова»)
ИНН 7801152738/ОГРН 1037800006276
190005, г. Санкт-Петербург, ул. 7-я Красноармейская, д.26, лит. Б
тел. 8 (812) 490-24-85, 8 (812) 316-49-53, 8 (812) 316-03-88
https://police-college.ru/ * e-mail: ipc-info@yandex.ru

Принято на заседании
Педагогического Совета
Протокол № 6 от 28.12.2023г.

Утверждаю
Директор АНОО ПО
«СПб АМ им. Н.А. Щёлокова»
О.В. Ярухин
Приказ №105У от «28» декабря 2023 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

по программе подготовки специалистов среднего звена по специальности

10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

на базе среднего общего образования

Форма обучения: Очная

Санкт-Петербург

2023

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (утв. приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553).

Организация-разработчик: Автономная некоммерческая образовательная организация профессионального образования «Санкт-Петербургская академия милиции имени Н.А. Щёлокова»

С О Д Е Р Ж А Н И Е

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 под- готовки 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 поддержание 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.
ПК 2.7.	*Администрирование компонентов ИТ-инфраструктуры*
ПК 2.8	*Обеспечение мер по информационной безопасности сетевой инфраструктуры и ее компонентов*
ПК 2.9.	*Проведение анализа компонентов ИТ-инфраструктуры на наличие уязвимостей*
ПК 2.10.	*Проведение мониторинга и анализа инцидентов информационной безопасности*

В результате освоения профессионального модуля студент должен:

иметь практический опыт в:	− 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:	− 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;
уметь:	− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − устанавливать и настраивать средства антивирусной защиты в соответствиис 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 − *администрировать веб-сервера, почтовые сервера, прокси.* − *настраивать межсетевые экраны, маршрутизаторы, сетевое оборудование и программное обеспечение.* − *работать с кластерными файловыми системами, организовывать RAID-массивы.* − *настраивать виртуальные частные сети.* − *организовывать удаленный доступ к ресурсам.* − *устанавливать и настраивать безопасную конфигурацию операционной системы, серверов и программного обеспечения с учетом предъявляемых требований.* − *использовать штатные и специальные средства мониторинга безопасности операционных систем* − *работать со сканерами уязвимости* − *осуществлять мониторинг и анализ инцидентов информационной безопасности, в том числе и анализ системных журналов и логов.* − *тестировать информационные системы и сервера на наличие известных и широко распространенных уязвимостей.*

1.3. Количество часов, отводимое на освоение профессионального модуля

№	Вид учебной работы	Объем часов
1.	**Объем работы обучающихся во взаимодействии с преподавателем**	**802**
в том числе:		
теоретическое обучение		**190**
практические занятия		**268**
учебная практика		**108**
производственная практика		**216**
Промежуточная аттестация в форме экзамена		**12**
2.	**Самостоятельная внеаудиторная работа обучающихся**	**64**
Всего по ПМ.02 в рамках образовательной программы		**878**

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	
1	2	3	4	5	6	7	8	9	10
ПК 2.1-ПК 2.6 ОК 1-ОК 10	Раздел 1. Программные и программно-аппаратные средства защиты информации	278	248	154	134	20			30
ПК 2.1-ПК 2.6 ОК 1-ОК 10	Раздел 2. Криптографические средства защиты информации	126	1 08	42	42				18
ПК 7-ПК 10 ОК 1-ОК 10	Раздел 3. Кибербезопасность	138	122	92	92				16
УП.02	Учебная практика	108	108	108			108		
ПП.02	Производственная практика	216	216	216				216	
	Промежуточная аттестация	12		12					
	Итого	878	802	624	266	20	108	216	64

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
1	**2**	**3**
Раздел 1. Программные и программно-аппаратные средства защиты информации		**278**
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**248**
Тема 1.1.Общие понятия программно-аппаратных средств защитыинформации	**Содержание учебного материала**	**22**
	1.1.1. Нормативно правовые акты, нормативные методические документы, в состав которых входит требования и рекомендации по защите информации программными и программно-аппаратными средствами	2
	1.1.2. Профили защиты программными и программно-аппаратными средствами	2
	1.1.3. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами	2
	1.1.4. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам.	2
	1.1.5. Вредоносное ПО. Классификация вредоносного ПО. Профилактика заражения.	2
	1.1.6. Бот-неты. Принцип функционирования. Методы обнаружения.	2
	1.1.7. Методы скрытия информации.	2
	1.1.8. Применение средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
	1.1.9. Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Защита от копирования.	2
	1.1.10. Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы ПО Windows	2
	1.1.11. Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации.	2
	Практические занятия	**6**

	Практическое занятие № 1 Обзор продуктов СЗИ от НСД	2
	Практическое занятие № 2 Обзор производителей СЗИ	2
	Практическое занятие № 3 Сравнительный анализ продуктов SIEM	2
Тема 1.2. Защита программ и данных	**Содержание учебного материала**	**8**
	1.2.1. Структура и функции подсистемы безопасности операционных систем	2
	1.2.2. Подсистема безопасности Windows. Подсистема безопасности Linux	2
	1.2.3. Средства обеспечения защиты информации в системах управления базами данных	2
	1.2.4. Критерии защищённости компьютерных систем.	2
Тема 1.3. Защита в компьютерных сетях	**Содержание учебного материала**	**8**
	1.3.1. Средства защиты в вычислительных сетях	2
	1.3.2. Защита информации в VPN-сетях	2
	1.3.3. Защита электронной почты	2
	1.3.4. Защита web-приложений и электронной подписи от мошенничества	2
Тема 1.4. Антивирусная защита данных	**Содержание учебного материала**	**2**
	1.4.1. Современные программные средства для защиты от вредоносных программ	2
	Практические занятия	**2**
	Практическое занятие № 4 Создание загрузочной флешки с антивирусной программой для быстрой проверки	
Тема 1.5. Средства защиты на компьютерах с операционной системой Windows	**Содержание учебного материала**	**6**
	1.5.1. Использование Active Directory и политик безопасности. Понятие домена. Роли контроллера домена	
	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 № 5 Установка серверной версии Windows	
	Практическое занятие № 6 Установка домена Active Directory	
	Практическое занятие № 7 Создание и внесение пользователей и компьютеров в домен	
	Практическое занятие № 8 Создание и применение глобальных политик домена	
	Практическое занятие № 9 Создание и применение локальных политик домена	
	Практическое занятие № 10 Установка сервера безопасности Secret Net Studio	

	Практическое занятие № 11 Установка клиента и программы управления Secret Net Studio	
	Практическое занятие № 12 Настройка централизованной установки клиента Secret Net Studio	
	Практическое занятие № 13 Работа с действующими средствами локальной защиты с помощью Secret Net Studio	
	Практическое занятие № 14 Удаление всех компонентов Secret Net Studio	
	Практическое занятие № 15 Установка Dallas Lock	
	Практическое занятие № 16 Настройка средств администрирования в Dallas Lock	
	Практическое занятие № 17 Настройка подсистем управления доступом в Dallas Lock	
	Практическое занятие № 18 Разграничение доступа к объектам файловой системы в Dallas Lock	
	Практическое занятие № 19 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	
	1.6.6. Принципы мониторинга событий информационной безопасности в DLP-системе Infowatch	
	Практические занятия	**64**
	Практическое занятие № 20 Установка и настройка Traffic monitor	
	Практическое занятие № 21 Установка и настройка Device monitor	
	Практическое занятие № 22 Установка клиента Device monitor	
	Практическое занятие № 23 Установка и настройка Crawler	
	Практическое занятие № 24 Создание правил и проверка их работоспособности в Device monitor	
	Практическое занятие № 25 Создание правил с использованием «белых» и «чёрных» списков в Device monitor	
	Практическое занятие № 26 Работа с Задачами и Журналом в Device monitor	
	Практическое занятие № 27 Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor	
	Практическое занятие № 28 Работа с терминами и списками в Traffic monitor	
	Практическое занятие № 29 Работа с тегами и объектами в Traffic monitor	
	Практическое занятие № 30 Создание политик защиты данных в Traffic monitor	
	Практическое занятие № 31 Создание политик защиты данных на агентах в Traffic monitor	
	Практическое занятие № 32 Создание политик контроля персон в Traffic monitor	

	Практическое занятие № 33 Создание политик с использованием правил передачи в Traffic monitor	
	Практическое занятие № 34 Создание политик с использованием правил копирования в Traffic monitor	
	Практическое занятие № 35 Создание политик с использованием правил хранения в Traffic monitor	
	Практическое занятие № 36 Создание политик с использованием правил работы в приложениях в Traffic monitor	
	Практическое занятие № 37 Создание политик с использованием регулярных выражений в Traffic monitor	
	Практическое занятие № 38 Создание и изменение виджетов в Traffic Monitor	
	Практическое занятие № 39 Создание и изменение отчётов в Traffic Monitor	
Тема 1.7. Методики проверки защищённости объектов информатизации	**Содержание учебного материала**	**4**
	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 № 40 Работа с требованиями и рекомендациями по технической защите конфиденциальной информации	
	Практическое занятие № 41 Работа с нормативно-правовой документацией, регламентирующей порядок проведения аттестации объектов информатизации	
Тема 1.8. Использование программно-аппаратных	**Содержание учебного материала**	**4**
	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 № 42 Развёртывание защищённой сети ViPNet. Учет отказов в работе средств вычислительной техники.	
	Практическое занятие № 43 Создание структуры защищённой сети ViPNet	
	Практическое занятие № 44 Создание защищённой сети ViPNet	
	Практическое занятие № 45 Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet	
	Практическое занятие № 46 Модификация защищённой сети ViPNet	
	Практическое занятие № 47 Компрометация ключей в защищённой сети ViPNet	

	Практическое занятие № 48 Настройка политик безопасности в VipNet Policy Manager	
	Практическое занятие № 49 Организация межсетевого взаимодействия	
	Практическое занятие № 50 Модификация межсетевого взаимодействия в защищённой сети ViPNet	
Тема 1.9. Защита передачи данных через Интернет	**Содержание учебного материала**	**6**
	1.9.1. Понятие https. Технология Secure Socket Layer (SSL)	
	1.9.2. Сертификаты, подписанные центром сертификации (CA).	
	1.9.3. Сертификаты домена. Самозаверяющие сертификаты.	
	Практические занятия	**16**
	Практическое занятие № 51 Установка openssl в centos	
	Практическое занятие № 52 Создание самоподписанного сертификата SSL	
	Практическое занятие № 53 Заполнение анкеты для сертификата	
	Практическое занятие № 54 Применение сертификата	
	Практическое занятие № 55 Перемещение ssl-сертификата с сервера windows на сервер, отличный от window	
	Практическое занятие № 56 Установка Nginx для последующей настройки прокси-сервера	
	Практическое занятие № 57 Настройка прокси-сервера с помощью Nginx	
	Практическое занятие № 58 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	**32**
	Практическое занятие № 59 Установка Астра Смоленск	
	Практическое занятие № 60 Настройка сети Астра Смоленск	
	Практическое занятие № 61 Пользователи Астра Смоленск	
	Практическое занятие № 62 Политики Астра Смоленск	
	Практическое занятие № 63 Настройка удаленного доступа SSH Астра Смоленск	
	Практическое занятие № 64 Поднятие сервера времени Астра Смоленск	
	Практическое занятие № 65 Создание зашифрованного раздела Астра Смоленск	
	Практическое занятие № 66 Установка IDS VipNet	
	Практическое занятие № 67 Активация IDS VipNet	

	Практическое занятие № 68 Настройка сетевого адаптера для сети	
	Практическое занятие № 69 Веб-интерфейс IDS VipNet	
	Практическое занятие № 70 Создание правил для сканирования портов	
	Практическое занятие № 71 Установка Kali Linux	
	Практическое занятие № 72 Проведение атаки на порты с использованием Kali Linux	
	Практическое занятие № 73 Создание собственных правил IDS VipNet	
	Практическое занятие № 74 Имитация атаки на собственные правила IDS VipNet	
Самостоятельная работа Заполнение рабочей тетради для самостоятельных работ по МДК.02.01		**30**
Раздел 2. Криптографические средства защиты информации		**126**
МДК.02.02. Криптографические средства защиты информации		**108**
Тема 2.1. Основные термины и определения	**Содержание учебного материала**	**4**
	2.1.1 Основные термины и определения в криптографии. Основные требования, предъявляемые к криптосистемам	
	2.2.2 Основные алгоритмические структуры, применяемые в криптографии. Делимость чисел. Алгоритм Евклида нахождения НОД двух чисел.	
Тема 2.2. Классификация шифров	**Содержание учебного материала**	**16**
	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-Гамаля. Алгоритм на основе эллиптических кривых.	
	2.2.5. Математические модели открытых сообщений. Критерии на открытый текст.	
	2.2.6. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений.	
	2.2.7. DES-алгоритм. Усложнения DES-алгоритма. Шифр AES	
	2.2.8. Российский стандарт шифрования ГОСТ-28147.	
	Практические занятия	**4**
	Практическое занятие № 1 Алгоритмизация шифра Цезаря	
	Практическое занятие №2 Декодирование моноалфавитного подстановочного шифра частотным методом	

Тема 2.3. Криптографические протоколы	**Содержание учебного материала**	**32**
	2.3.1. Понятие криптографических протоколов. Классификация.	
	2.3.2. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана-Меркла	
	2.3.3. Протоколы аутентификации	
	2.3.4. Протоколы идентификации	
	2.3.5. Протоколы электронной цифровой подписи. Протокол на базе алгоритма RSA. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.	
	2.3.6. Протокол взаимоблокировки. Протокол Ву-Лама	
	2.3.7. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля	
	2.3.8. Протоколы обмена ключами	
	2.3.9. Протокол Kerberos	
	2.3.10. Ключевые функции хеширования. Бесключевые функции хеширования	
	2.3.11. Хеш-функции. MD5. Применение шифрования для получения хеш-образа.	
	2.3.12. Протоколы защиты данных в сети Internet	
	2.3.13. Протоколы IPSec, AH, ESP, ISAKMP, Oakley. Протокол SSL	
	2.3.14. Протоколы электронных платежей. Цифровые деньги	
	2.3.15. Протоколы голосования	
	2.3.16. Теория алгоритмов и чисел	
	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**	**16**
	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	
	2.4.4. Дифференциальный криптоанализ	
	2.4.5. Методы криптоанализа блочных шифров. Атаки на блочные шифры.	
	2.4.6. Методы криптоанализа. Частотный анализ. Метод полного перебора	
	2.4.7. Методы взлома шифров сложной замены	
	2.4.8. Кодирование информации. Общедоступные кодовые системы. Секретные кодовые системы.	
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	**2**
	Практическое занятие № 5 Анализ графических изображений на наличие скрытой информации.	
Тема 2.6. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**6**
	2.6.1. Аутентификация данных. Электронная подпись. Хэш-функция.	
	2.6.2. Стандарты на электронную подпись	
	2.6.3. Электронная подпись на базе шифра Эль-Гамаля	
	Практические занятия	**8**
	Практическое занятие №6. Применение различных функций хэширования, анализ особенностей хешей	
	Практическое занятие №7. Генерация и проверка ЭП RSA	
	Практическое занятие №8. Применение криптографических атак на хеш-функции	
	Практическое занятие №9. Применение стандартов на электронную подпись	
Самостоятельная работа Заполнение рабочей тетради для самостоятельных работ по МДК.02.02		**18**
Раздел 3. Кибербезопасность		**138**
МДК.02.03. Кибербезопасность		**122**
Тема 3.1. Установка и настройка Windows Server 2019	**Содержание темы**	**4**
	3.1.1. Обзор Windows Server 2019. Развертывание и управление Windows Server 2019.Доменные сервисы Службы Каталога. Введение в AD DS. AD DS. Обзор функций контроллера домена. Установка контроллера домена	
	3.1.2. Настройка удаленного управления в Windows Server 2019 Групповые политики в Windows Server 2019. Серверы времени и лицензирования. Центр сертификации.	
	Практические занятия	**6**
	Практическое занятие № 1. Установка и настройка Windows Server 2019.Установка ролей сервера Windows Server 2019	
	Практическое занятие № 2. Подключение сетевых периферийных устройств через ГП	

	Практическое занятие № 3. Установка и настройка сервера времени и сервера лицензирования. Управление пользовательским рабочим столом через ГП	
Тема 3.2. Администрирование Windows Server2019	**Содержание темы**	**4**
	3.2.1. Управление службой DNS и устранение неполадок. Настройка DHCP в Windows Server 2019	
	3.2.2. Защита доступа к сети. Настройка NAP. Реализация безопасности клиентских систем. Внедрение управления обновлениями. Обзор WSUS. Развертывание обновлений посредством WSUS. Создание общих файлов в домене	
	Практические занятия	**14**
	Практическое занятие № 4.Применение технологии DirectAccess с помощью мастера начальной настройки	
	Практическое занятие № 5.Развертывание расширенной инфраструктуры DirectAccess	
	Практическое занятие № 6.Внедрение VPN	
	Практическое занятие № 7.Настройка шифрования и расширенного аудита	
	Практическое занятие № 8. Использование службы развертывания	
	Практическое занятие № 9. Внедрение управления обновлениями.	
	Практическое занятие №10. Настройка файлового сервера	
	Практическое занятие № 11. Настройка DHCP	
	Практическое занятие № 12. Настройка центра сертификации	
	Практическое занятие № 13. Настройка групповых политик	
	Практическое занятие № 14. Добавление рабочих станций в домен	
Тема 3.3. Установка и администрирование Linux	**Содержание темы**	**4**
	3.3.1. Администрирование ОС на базе Linux. Развертывание веб-серверов Linux. Лог-файлы и мониторинг. Атрибуты файлов и права доступа	
	3.3.2. Управление пакетами при помощи RPM и yum Управление системными сервисами. Аутентификация LDAP	
	Практические занятия	**18**
	Практическое занятие № 15. Установка сервера Debian.	
	Практическое занятие № 16. Настройка web-сервера в ОС Debian.	
	Практическое занятие № 17. Настройка сервера DNS в ОС Debian.	
	Практическое занятие № 18. Настройка сервера DHCP в ОС Debian.	
	Практическое занятие № 19. Настройка файловых серверов в ОС Debian	
	Практическое занятие № 20. Настройка контейнеров Docker.	
	Практическое занятие № 21. Установка сервера CentOS.	

	Практическое занятие № 22. Настройка web-сервера в CentOS.	
	Практическое занятие № 23. Настройка сервера DNS в CentOS.	
	Практическое занятие № 24. Настройка сервера DHCP в CentOS.	
	Практическое занятие №25. Установка и настройка OpenVPN	
	Практическое занятие №26. Применение протокола IPsec и SSH.	
	Практическое занятие №27. Настройка регистрации действий	
	Практическое занятие № 28. Установка и настройка OpenLDAP	
	Практическое занятие № 29. Установка и настройка IPtables	
	Практическое занятие № 30. Установка и базовая настройка Kali Linux	
	Практическое занятие № 31. Администрирование Kali Linux	
	Практическое занятие №32. Установка и настройка утилит в Kali Linux	
Тема 3.4. Основы кибербезопасности	**Содержание темы**	**4**
	3.4.1. Основные проблемы обеспечения кибербезопасности. Классификация угроз информационной безопасности	
	3.4.2. Защита информации от компьютерных вирусов	
	3.4.3 Повышение защищенности веб-серверов	
	3.4.4. Рекомендации по повышению защищенности веб-приложений	
	Практические занятия	**8**
	Практическое занятие № 33. Поиск уязвимостей информационных систем	
	Практическое занятие № 34. Применение антивирусной защиты	
	Практическое занятие № 35. Настройка безопасности веб-браузеров	
	Практическое занятие № 36. Оценка рисков информационной безопасности с использованием классификации веб-угроз	
Тема 3.5. Поиск уязвимостей	**Содержание темы**	**4**
	3.5.1. Уязвимости сети. Обнаружение уязвимостей сайтов. Уязвимости веб-приложений. Обнаружение уязвимостей веб-приложений.	
	3.5.2. SQL-инъекции. XSS-уязвимости. Уязвимости CSRF. IDOR. Атака типа clickjacking. Подделка межсайтового запроса.	
	3.5.3. Проблемы аутентификации и проверки сессий. Проблемы контроля доступа.	
	3.5.4. Методы сканирования сети. Обзор популярных сканеров уязвимостей	
	Практические занятия	**20**
	Практическое занятие № 37. Сканирование системы с помощью IP-сканера	
	Практическое занятие № 38. Сканирование системы с помощью CFI LanGuard	

	Практическое занятие № 39. Поиск открытых портов	
	Практическое занятие № 40. Сканирование сети с помощью NetScan	
	Практическое занятие № 41. «Сканирование сети с помощью Nessus Tool	
	Практическое занятие № 42. Сканирование сети с помощью Colasoft Packet Builder	
	Практическое занятие № 43. Сканирование устройства в сети с помощью Dude»	
	Практическое занятие № 44. Отображение сети с помощью Friendly Pinger	
	Практическое занятие № 45. Анализ уязвимостей серверов	
	Практическое занятие № 46. Поиск и устранение неисправностей сети с помощью MegaPing	
Тема 3.6. Защита информационной инфраструктуры	**Содержание темы**	
	3.6.1. Методы защиты информационной инфраструктуры. Использование межсетевых экранов	**4**
	3.6.2. Безопасность операционных систем. Основные способы защиты информационных систем. Повышение уровня защищенности ИИ	
	Практические занятия	
	Практическое занятие № 47. Настройка межсетевого экрана	
	Практическое занятие № 48. Настройка параметров безопасности Windows.	**6**
	Практическое занятие № 49. Составление рекомендаций по повышению уровня защищенности информационной инфраструктуры	
Тема 3.7. Расследование инцидентов	**Содержание темы**	
	3.7.1. Понятие и виды компьютерных преступлений. Основные стадии компьютерного преступления. Идентификация нападающего. Мотивация нарушителей. Анализ технических аспектов нападения.	
	3.7.2. Типовые действия, выполняемые в рамках процесса управления инцидентами. Идентификация инцидента. Реагирование на инцидент ИБ. Восстановление после инцидента ИБ. Оценка ущерба от произошедшего нарушения информационной безопасности. Устранение негативных последствий инцидентов	**4**
	Практические занятия	
	Практическое занятие № 54. Выявление предпосылок и обстоятельств, приведших к возникновению компьютерного инцидента.	**2**
	Практическое занятие № 55. Обнаружение события информационной безопасности. Оценка события информационной безопасности	
Тема 3.8. Поиск информации по открытым источникам	**Содержание темы**	
	3.8.1. Методы социальной инженерии. Исследование на основе открытых источников. Инструменты OSINT	**2**

	Практические занятия	**4**
	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		216
Промежуточная аттестация		12
Всего		878

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 мультимедиа проектор, 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 // Образовательная платформа Юрайт [сайт].

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**
Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	установка и настройка отдельных программных, программно-аппаратных средств защиты информации.	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 процессепрактики Экзамен по ПМ.
Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	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 процессепрактики Экзамен по ПМ.

Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	тестирование функций отдельных программных и программно-аппаратных средств защиты информации. 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 процессепрактики
		Экзамен по ПМ.
		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 процессепрактики Экзамен по ПМ.
Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения,	регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программныхипрограммно-аппаратных средств обнаружения, предупреждения и	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при

предупреждения и ликвидации последствий компьютерных атак.	ликвидации последствий компьютерных атак	выполнении практических работ и наблюдение в процессепрактики 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 самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Обеспечение мер по информационной безопасности сетевой инфраструктуры и ее компонентов	меры по информационной безопасности сетевой инфраструктуры и ее компонентов	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 процессепрактики Экзамен по ПМ.
Проведение анализа компонентов ИТ-инфраструктуры на наличие уязвимостей	анализ компонентов ИТ-инфраструктуры на наличие уязвимостей	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 процессепрактики Экзамен по ПМ.
Проведение мониторинга и анализа инцидентов информационной безопасности	мониторинг и анализ инцидентов информационной безопасности	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.
Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	выбор и применение эффективных методов и способов решения профессиональныхзадач в профессиональнойобласти; 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 государственномязыке 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,	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью

ресурсосбережению, эффективно действовать в чрезвычайных ситуациях		обучающегося в процессе освоения образовательной программы
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Соблюдение режима труда и отдыха, здоровье сберегающих технологий в процессе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы -
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