Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение

«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО
На заседании педагогического совета
Протокол N2
«02» июля 2021г

УТВЕРЖДАЮ
Директор СПб ГБПОУ «АУГСГиП»
_____А.М. Кривоносов
«02» 07 2021г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 «ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

для специальности 10.02.01 «Организация и технология защиты информации»

среднего профессионального образования

(базовой подготовки)

Санкт-Петербург

2021 г.

ОДОБРЕНЫ
Цикловой комиссией
Общетехнических дисциплин
и компьютерных технологий
Протокол № 9
от «14» мая 2021г.
Председатель ЦК

 Шобарев А.В.

РАССМОТРЕНЫ
Методическим советом
«АУГСГиП»
Протокол № 5
от 25 «июня» 2021 г.

Рабочая программа профессионального модуля ПМ.03 «Программно-аппаратные и технические средства защиты информации» разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.01 «Организация и технология защиты информации»

Разработчик:

Андреев В.В., преподаватель СПб ГБПОУ «Академия управления городской средой, градостроительства и печати»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 «Программно-аппаратные и технические средства защиты информации»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности - «Программно-аппаратные и технические средства защиты информации» и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ОК 10	Применять математический аппарат для решения профессиональных задач.
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах
ПК 3.2	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4	Выявлять и анализировать возможные угрозы информационной безопасности объектов

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– участия в эксплуатации систем и средств защиты информации защищаемых объектов; – применения технических средств защиты информации; – выявления возможных угроз информационной безопасности объектов защиты;
уметь	– работать с техническими средствами защиты информации; – работать с защищенными автоматизированными системами; – передавать информацию по защищенным каналам связи; – фиксировать отказы в работе средств вычислительной техники;
знать	– виды, источники и носители защищаемой информации; – источники опасных сигналов; – структуру, классификацию и основные характеристики технических каналов утечки информации; – классификацию технических разведок и методы противодействия им; – методы и средства технической защиты информации; – методы скрытия информации; – программно-аппаратные средства защиты информации; – структуру подсистемы безопасности операционных систем и выполняемые ею функции; – средства защиты в вычислительных сетях; – средства обеспечения защиты информации в системах управления базами данных; – критерии защищенности компьютерных систем; – методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 705 часов,

из них на освоение МДК 326 часов,

на практики, в том числе учебную 144 часов и производственную 72 часа,

самостоятельная работа – 163 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПМ.03) «Программно-аппаратные и технические средства защиты информации»

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, ак. час.					
			Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа
			Обучение по МДК			Практики		
			Всего	В том числе		Учебная	Производственная	
				Лабораторных и практических занятий	Курсовых работ (проектов)			
1	2	3	4	5	6	7	8	9
ПК 3.1 – ПК 3.4 ОК1-ОК12	Раздел 1. Технические методы и средства, технологии защиты информации	264	176	52	20			88
ПК 3.1 – ПК 3.4 ОК1-ОК12	Раздел 2. Программно-аппаратные средства защиты информации	225	150	38				75
ПК 3.1 – ПК 3.4 ОК1-ОК12	Учебная практика	144	144			144		
ПК 3.1 – ПК 3.4 ОК1-ОК12	Производственная практика (по профилю специальности), часов	72					72	
	Всего:	**705**	**470**	**90**	**20**	**144**	**72**	**163**

2.2. Тематический план и содержание профессионального модуля (ПМ.03)

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
ПМ.03 Программно-аппаратные и технические средства защиты информации		**705**	
Раздел 1 Технические методы и средства, технологии защиты информации		**264**	
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала**	**6**	1
	1.1.1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.	2	
	1.1.2. Задачи и требования к способам и средствам защиты информации техническими средствами.	2	
	1.1.3. Нормативно-правовые документы по технической защите информации	2	
Тема 1.2. Информация как объект защиты техническими средствами.	**Содержание учебного материала**	**8**	1
	1.2.1. Информация как объект защиты техническими средствами. Виды, источники и носители защищаемой информации.	2	
	1.2.2. Свойства информации, влияющие на возможности ее защиты техническими средствами.	2	
	1.2.3. Демаскирующие признаки объектов защиты.	2	
	1.2.4. Виды угроз безопасности информации, защищаемой техническими средствами. Источники опасных сигналов.	2	
Тема 1.3. Технические каналы утечки информации	**Содержание учебного материала**	**10**	1
	1.3.1. Технические каналы утечки, классификация	2	
	1.3.2. Каналы утечки речевой информации	2	
	1.3.3. Каналы утечки информации, обрабатываемой ТСПИ	2	
	1.3.4. Каналы утечки информации при ее передаче по каналам связи	2	
	1.3.5. Технические каналы утечки видовой информации	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	Практические занятия	**2**	2
	Практическое занятие № 1. Анализ возможных технических каналов утечки информации, подбор средств и методов их защиты	2	
Тема 1.4. Средства технической разведки	**Содержание учебного материала**	**4**	1
	1.4.1. Классификация технических разведок. Методы и средства защиты от технической разведки	2	
	1.4.2. Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.	2	
	Практические занятия	**6**	2
	Практическое занятие №2. Разработка плана применения технических мер по предотвращению проникновения злоумышленника к источникам информации.	2	
	Практическое занятие № 3. Сравнительный анализ технических средств обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации.	2	
	Практическое занятие № 4. Маскировка объектов наблюдения	2	
Тема 1.5. Защита от утечки информации по акустическому каналу	**Содержание учебного материала**	**16**	1
	1.5.1. Общие сведения о закладных устройствах. Радиозакладки.	2	
	1.5.2. Приемники излучения радиозакладных устройств. Закладные устройства с передачей информации по проводным каналам.	2	
	1.5.3. Микрофон. Акустические антенны. Комбинированные микрофоны. Групповые микрофоны.	2	
	1.5.4 Средства обеспечения скрытности оперативной звукозаписи. Аппаратура звукозаписи.	2	
	1.5.5 Цифровые диктофоны. Обнаружители диктофонов.	2	
	1.5.6. Факторы, влияющие на качество звукозаписи. Выбор типа микрофона и места его установки.	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	1.5.7. Защита от акустического канала утечки информации	2	
	1.5.8. Перехват речевой информации с использованием радиоканала. Оптико-акустическая аппаратура перехвата речевой информации	2	
	Практические занятия	**4**	2
	Практическое занятие № 5. Сравнительный анализ микрофонов.	2	
	Практическое занятие № 6. Сравнительный анализ диктофонов.	2	
Тема 1.6. Защита информации от утечек по материально-вещественному каналу	**Содержание учебного материала**	**4**	1
	1.6.1. Структура вещественных каналов. Методы получения информации с использованием вещественных каналов	2	
	1.6.2. Защита информации от утечки по материально-вещественным каналам	2	
Тема 1.7. Защита от утечки информации по оптическому каналу	**Содержание учебного материала**	**4**	1
	1.7.1. Характеристики оптического канала утечки информации	2	
	1.7.2. Устройства съема данных. Предотвращение утечки информации по оптическим каналам	2	
Тема 1.8. Защита информации от электрических и электромагнитных каналов утечки информации	**Содержание учебного материала**	**4**	1
	1.8.1. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок	2	
	1.8.2. Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.	2	
	Практические занятия	**6**	2
	Практическое занятие № 7. Определение порядка работы с техническими средствами защиты речевой информации в телефонных линиях	2	
	Практическое занятие № 8. Составление инструкции для работы с техническими средствами защиты от утечек информации по проводным линиям	2	
	Практическое занятие № 9 . Составление инструкции для работы с устройствами защиты от прослушивания проводных телефонных линий.	2	
Тема 1.9. Технические средства добывания	**Содержание учебного материала**	**10**	1
	1.9.1. Технические средства добывания информации. Классификация средств	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
информации	добывания информации		
	1.9.2. Оптическая разведка. Радиоэлектронная разведка	2	
	1.9.3. Акустическая разведка	2	
	1.9.4. Добывание информации без физического проникновении в контролируемую зону	2	
	1.9.5. Специальные технические средства, предназначенные для негласного получения информации. Ответственность, предусмотренная законодательством за их незаконный оборот	2	
Тема 1.10. Средства выявления каналов утечки информации	**Содержание учебного материала**	**12**	
	1.10.1. Индикаторы электромагнитного поля	2	
	1.10.2. Сканирующие радиоприемники	2	
	1.10.3. Анализаторы спектра, радиочастотомеры	2	1
	1.10.4. Многофункциональные комплекты для выявления каналов утечки информации	2	
	1.10.5. Нелинейные локаторы. Комплексы измерения ПЭМИН	2	
	1.10.6. Металлодетекторы. Металлоискатели. Досмотровые эндоскопы	2	
	Практические занятия	**2**	
	Практическое занятие № 10. Обнаружение закладных устройств нелинейным локатором	2	2
Тема 1.11. Технические методы и средства защиты информации	**Содержание учебного материала**	**22**	
	1.11.1. Средства технической защиты информации. Классификация устройств технической защиты информации.	2	
	1.11.2. Концепция и методы инженерно-технической защиты информации	2	
	1.11.3. Экранирование электромагнитных волн. Устройства контроля и защиты слаботочных линий и сети	2	
	1.11.4. Электромагнитное экранирование и развязывающие цепи. Экранированные помещения	2	1
	1.11.5. Фильтрация информационных сигналов. Помехоподавляющие фильтры	2	
	1.11.6. Пространственное и линейное зашумление	2	
	1.11.7. Подавление емкостных паразитных связей. Устройства контроля и защиты проводных линий от утечки информации	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	1.11.8. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам	2	
	1.11.9. Заземление технических средств и подавление информационных сигналов в цепях заземления	2	
	1.11.10. Устройства контроля и защиты слаботочных линий и сети.	2	
	1.11.11. Комплексы радиомониторинга.	2	
	Практические занятия	**24**	2
	Практическое занятие № 11. Решение ситуационных задач. Оценка вероятности утечки речевой информации.	2	
	Практическое занятие № 12. Работа с системой защиты «ГРОМ-ЗИ»	2	
	Практическое занятие № 13. Работа с КАЗ РИ «Орбита-3»	2	
	Практическое занятие № 14. Решение ситуационных задач. Оценка вероятности утечки видовой информации.	2	
	Практическое занятие № 15. Разработка системы инженерно-технической защиты информации	2	
	Практическое занятие № 16. Сравнительный анализ генераторов шума	2	
	Практическое занятие № 17. Сравнительный анализ средств для поиска электромагнитных излучений	2	
	Практическое занятие № 18. Работа с тепловизором	2	
	Практическое занятие № 19. Работа с виброакустическим средством Соната	2	
	Практическое занятие № 20. Работа с сетевыми помехоподавляющими фильтрами и генераторами	2	
	Практическое занятие № 21. Методы и средства съема информации с телефонных линий.	2	
	Практическое занятие № 22. Прослушивание помещений высокочастотным навязыванием.	2	
Тема 1.12. Разработка комплекса мер технической защиты информации в	**Содержание учебного материала**	**4**	1
	1.11.1. Структура разработки комплекса мер технической защиты информации в организации	2	
	1.11.2. Подготовка документации по технической защите в организации	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
организации	**Практические занятия**	**8**	2
	Практическое занятие № 23. Анализ деятельности организации, защищаемой информации, средств технической защиты организации	2	
	Практическое занятие № 24. Разработка схемы технической защиты информации организации	2	
	Практическое занятие № 25. Определение вариантов дополнительных мер защиты с оценкой затрат на их обеспечение, выбор рациональных вариантов.	2	
	Практическое занятие № 26. Подготовка технической документации для выбранных средств и методов технической защиты	2	
	Дифференцированный зачет	2	
Самостоятельная работа			
Заполнение рабочей тетради для самостоятельных работ по МДК.03.01 в СДО на платформе Moodle		88	
Раздел 2. Программно-аппаратные средства защиты информации		**150**	
Тема 2.1 Общие понятия программно-аппаратных средств защиты информации	**Содержание учебного материала**	**4**	1
	2.1.1. Виды программно-аппаратных средств защиты информации. Понятие комплексных решений.	2	
	2.1.2. Методы скрытия информации	2	
Тема 2.2. Защита программ и данных	**Содержание учебного материала**	**10**	1
	2.2.1. Структура и функции подсистемы безопасности операционных систем	2	
	2.2.2. Подсистема безопасности Windows.	2	
	2.2.3. Подсистема безопасности Linux	2	
	2.2.4. Средства обеспечения защиты информации в системах управления базами данных	2	
	2.2.5. Критерии защищённости компьютерных систем.	2	
Тема 2.3. Защита в компьютерных сетях	**Содержание учебного материала**	**12**	1
	2.3.1. Методы защиты компьютерных сетей	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	2.3.2. Средства защиты в вычислительных сетях	2	
	2.3.3. Защита информации в VPN-сетях	2	
	2.3.4. Защита электронной почты	2	
	2.3.5. Защита web-приложений от мошенничества	2	
	2.3.6. Защита электронной подписи	2	
Тема 2.4. Антивирусная защита данных	**Содержание учебного материала**	**4**	
	2.4.1. Защита от вредоносного ПО	2	1
	2.4.2. Современные программные средства для защиты от вредоносных программ	2	
Тема 2.5. Криптографические методы и средства обеспечения информационной безопасности	**Содержание учебного материала**	**8**	
	2.5.1. Основные понятия криптографической защиты информации	2	
	2.5.2. Симметричные криптосистемы шифрования	2	1
	2.5.3 Асимметричные криптосистемы шифрования	2	
	2.5.4. Криптографические алгоритмы	2	
Тема 2.6. Средства защиты на компьютерах с операционной системой Windows	**Содержание учебного материала**	**14**	
	2.6.1. Использование Active Directory и политик безопасности. Понятие домена. Роли контроллера домена	2	
	2.6.2. Создание и внесение пользователей и компьютеров в домен	2	
	2.6.3 Локальные политики домена	2	
	2.6.4 Глобальные политики домена	2	1
	2.6.5. Разграничение прав доступа	2	
	2.6.6. Средства защиты информации Dallas Lock. Возможности Dallas Lock. Принцип работы. Параметры установки	2	
	2.6.7. Средство доверенной загрузки Secret Net Studio . Возможности Secret Net Studio. Принцип работы. Параметры установки	2	
	Практические занятия	**6**	2

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	Практическое занятие № 1 Установка серверной версии Windows. Установка и настройка домена Active Directory	2	
	Практическое занятие № 2 Создание и применение глобальных политик домена	2	
	Практическое занятие № 3 Создание и применение локальных политик домена	2	
Тема 2.7 Методики проверки защищённости объектов информатизации	**Содержание учебного материала**	**4**	1
	2.7.1. Методики проверки защищённости объектов информатизации на соответствие требованиям нормативных правовых актов	2	
	2.7.2. Нормативно-методические документы, регламентирующие порядок проведения аттестации объектов информатизации и содержащие требования к объектам информатизации	2	
	Практические занятия	**2**	1
	Практическое занятие № 4 Работа с требованиями и рекомендациями по технической защите конфиденциальной информации	2	
Тема 2.8. Использование DLP-системы Infowatch для защиты от внутренних утечек информации	**Содержание учебного материала**	**26**	1
	2.8.1. Общая характеристика и принципы функционирования dlp-системы Infowatch	2	
	2.8.2. Виды политик, способы их создания в Traffic monitor	2	
	2.8.3. Принципы построения регулярных выражений для создания политик	2	
	2.8.4. Виды правил и способы создания правил в Device monitor	2	
	2.8.5. Работа с Задачами и Журналом в Device monitor	2	
	2.8.6. Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor	2	
	2.8.7. Работа с терминами и списками в Traffic monitor	2	
	2.8.8. Работа с тегами и объектами в Traffic monitor	2	
	2.8.9. Создание политик контроля персон в Traffic monitor	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	2.8.10. Правила передачи в Traffic monitor	2	
	2.8.11. Правила хранения в Traffic monitor	2	
	2.8.12. Правила копирования в Traffic monitor	2	
	2.8.13. Отчёты в Traffic Monitor	2	
	Практические занятия	**16**	
	Практическое занятие № 5 Установка и настройка Traffic monitor	2	
	Практическое занятие № 6 Установка и настройка Device monitor	2	
	Практическое занятие № 7 Установка клиента Device monitor	2	
	Практическое занятие № 8 Создание правил и проверка их работоспособности в Device monitor	2	2
	Практическое занятие № 9 Создание правил с использованием «белых» и «чёрных» списков в Device monitor	2	
	Практическое занятие № 10 Создание политик защиты данных в Traffic monitor	2	
	Практическое занятие № 11 Создание политик с использованием регулярных выражений в Traffic monitor	2	
	Практическое занятие № 12 Создание и изменение отчётов в Traffic Monitor	2	
Тема 2.9. Использование программно-аппаратных средств для создания защищённой сети	**Содержание учебного материала**	**10**	
	2.9.1.Общая характеристика продуктов ViPNet для создания защищённой сети	2	
	2.9.2. Понятие построения виртуальной защищённой сети	2	
	2.9.3. Компрометация ключей в защищённой сети ViPNet	2	1
	2.9.4. Настройка политик безопасности в VipNet Policy Manager	2	
	2.9.5. Организация межсетевого взаимодействия. Модификация межсетевого взаимодействия в защищённой сети ViPNet	2	
	Практические занятия	**8**	2

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	Практическое занятие № 13 Развёртывание защищённой сети ViPNet. Учет отказов в работе средств вычислительной техники.	2	
	Практическое занятие № 14 Создание структуры защищённой сети ViPNet	2	
	Практическое занятие № 15 Создание защищённой сети ViPNet	2	
	Практическое занятие № 16 Модификация защищённой сети ViPNet	2	
Тема 2.10. Защита передачи данных через Интернет	**Содержание учебного материала**	**10**	
	2.10.1. Понятие https. Технология Secure Socket Layer (SSL)	2	
	2.10.2. Сертификаты, подписанные центром сертификации (CA). Сертификаты домена Самозаверяющие сертификаты	2	1
	2.10.3. Установка openssl	2	
	2.10.4. Установка Nginx для последующей настройки прокси-сервера	2	
	2.10.5. Настройка правильной работы ssl	2	
	Практические занятия	**2**	2
	Практическое занятие № 17 Настройка прокси-сервера с помощью Nginx	2	
Тема 2.11 Средства защиты на компьютерах с операционной системой Linux	**Содержание учебного материала**	**8**	
	2.11.1. Средства защиты компьютерных сетей с использованием Samba и политик безопасности на Linux-сервере. Особенности серверов на Linux.	2	
	2.11.2. Программные средства для поднятия контроллера домена на Linux	2	1
	2.11.3. Принципы использования систем обнаружения вторжения	2	
	2.10.4. Синтаксис написания правил для IDS систем	2	
	Практические занятия	**4**	
	Практическое занятие № 18 Установка и настройка VipNet IDS	2	2
	Практическое занятие № 19 Написание правил для VipNet IDS	2	
	Дифференцированный зачет	**2**	
Внеаудиторная (самостоятельная) учебная работа при изучении раздела Заполнение рабочей тетради для самостоятельных работ по МДК.03.02 в СДО на платформе Moodle		**75**	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
Курсовая работа			
Тематика курсовых работ «» по индивидуальным вариантам		20	
	Обязательные аудиторные учебные занятия по курсовой работе: 1. Распределение тем. Выдача задания на курсовую работу. Правила оформления курсовой работы 2. Составление плана теоретической части курсовой работы. Составление Введения 3. Выполнение теоретической части 4. Выполнение практической части 5. Составление Заключения 6. Подготовка доклада для защиты курсовой работы 7. Подготовка презентации для защиты курсовой работы 8. Защита курсовой работы		
Учебная практика		**144**	
	1. Составление номенклатуры необходимых программно-аппаратных средств защиты информации на защищаемом объекте 2. Составление номенклатуры необходимых технических средств защиты информации на защищаемом объекте 3. Разработка системы инженерно-технической защиты информации на защищаемом объекте 4. Разработка схемы технической защиты информации на защищаемом объекте 5. Подготовка технической документации для выбранных средств и методов технической защиты 6. Расчёт стоимости необходимых программно-аппаратных средств защиты информации на защищаемом объекте 7. Расчёт стоимости необходимых технических средств защиты информации на защищаемом объекте 8. Установка домена для последующего использования локальных и глобальных политик безопасности на защищаемом объекте 9. Настройка домена для последующего использования локальных и глобальных политик безопасности на защищаемом объекте 10. Создание и применение локальных и глобальных политик безопасности в сети на защищаемом объекте 11. Создание пользователей домена с различными уровнями прав на защищаемом объекте 12. Установка средств доверенной загрузки ОС на рабочей станции, работающей под ОС Windows с помощью		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	программно-аппаратных комплексов средств защиты информации 13. Настройка средств доверенной загрузки ОС на рабочей станции, работающей под ОС Linux с помощью программно-аппаратных комплексов средств защиты информации 14. Создание индивидуальной для пользователя изолированной рабочей программной среды в ОС Windows с помощью программно-аппаратных комплексов средств защиты информации 15. Проверка корректной работы изолированной рабочей программной среды в ОС Windows 16. Подбор программных средств для защиты от вредоносных программ на защищаемом объекте 17. Установка в сети программных средств для защиты от вредоносных программ на защищаемом объекте 18. Проверка на корректную работу программных средств для защиты от вредоносных программ на защищаемом объекте 19. Установка серверной версии ОС Linux для последующей установки сетевого экрана для защиты информации от внешних атак 20. Установка межсетевого экрана для защиты инфраструктуры защищаемого объекта 21. Настройка межсетевого экрана для защиты инфраструктуры защищаемого объекта 22. Проверка работоспособности межсетевого экрана для защиты инфраструктуры 23. Модификация настроек межсетевого экрана для защиты инфраструктуры защищаемого объекта 24. Установка системы обнаружения вторжений 25. Настройка системы обнаружения вторжений 26. Создание первичных правил для системы обнаружения вторжений 27. Проверка работоспособности правил, написанных для системы обнаружения вторжений 28. Корректировка правил и создание дополнительных правил для системы обнаружения вторжения 29. Установка виртуальной машины для последующей эмуляции вторжений 30. Эмуляция вторжений для анализа информационной безопасности объекта 31. Выявление попыток вторжения с помощью системы обнаружения вторжений 32. Исправление настройки системы обнаружения вторжений после выявления вторжений 33. Применение средств доверенной загрузки ОС на рабочей станции, работающей под ОС Linux с помощью программно-аппаратных комплексов средств защиты информации 34. Создание индивидуальной для пользователя изолированной рабочей программной среды в ОС Linux с помощью программно-аппаратных комплексов средств защиты информации 35. Проверка корректной работы изолированной рабочей программной среды в ОС Linux 36. Настройка запрета запуска неразрешённых программ и разграничение доступа пользователей к массивам		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	данных и программ с помощью дискреционного контроля доступа 37. Развёртывание DLP-системы (установка Traffic Monitor) для защиты от внутренних угроз 38. Развёртывание DLP-системы (установка Device Monitor) для защиты от внутренних угроз 39. Развёртывание DLP-системы (установка агента на рабочие станции) для защиты от внутренних угроз 40. Первичная проверка работоспособности DLP-системы 41. Установка дополнительного клиента IWDM на отдельную машину и создание нового пользователя – офицера безопасности 42. Устранение неисправностей при развёртывании DLP-системы на защищаемом объекте 43. Планирование защищённой сети VPN 44. Развёртывание защищённой сети на основе технологий VPN 45. Проверка работоспособности защищённой сети на основе технологии VPN 46. Модификация защищённой сети на основе технологий VPN 47. Применение защищённой сети для отправки деловой почты по защищённому каналу 48. Применение защищённой сети для отправки документов по защищённому каналу 49. Эмуляция компрометации ключей в защищённой сети 50. Отработка действий в случае компрометации ключей в защищённой сети на основе технологий VPN 51. Поднятие защищённой сети после компрометации ключей 52. Настройка политик безопасности в защищённой сети на основе технологий VPN 53. Первичная настройка межсетевого взаимодействия в защищённой сети на основе технологий VPN 54. Модификация межсетевого взаимодействия в защищённой сети на основе технологий VPN 55. Исправление ошибок после модификации межсетевого взаимодействия в защищённой сети 56. Настройка межсетевого взаимодействия с применением асимметричного межсетевого мастер ключа 57. Настройка туннелирования незащищённых узлов в защищённой сети на основе технологии VPN 58. Добавление дополнительных незащищённых узлов при туннелировании в защищённой сети на основе технологии VPN 59. Настройка фильтрации трафика в защищённой сети на основе технологии VPN 60. Применение фильтрации трафика в защищённой сети на основе технологии VPN 61. Применение DLP-системы для написания правил безопасности для применения на рабочих станциях 62. Проверка работоспособности правил, выявление некорректной работы правил 63. Корректировка агентских правил безопасности в DLP-системе 64. Применение DLP-системы для написания простых политик безопасности для применения на рабочих		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
станциях 65. Проверка работоспособности простых политик безопасности, выявление некорректной работы политик безопасности 66. Корректировка простых политик безопасности в DLP-системе 67. Применение DLP-системы для защиты документов и печати защищаемого объекта 68. Проверка работоспособности DLP-системы для защиты документов и печати защищаемого объекта 69. Применение DLP-системы для написания сложных политик безопасности с лингвистическим разбором на защищаемом объекте 70. Проверка работоспособности DLP-системы для написания сложных политик безопасности с лингвистическим разбором на защищаемом объекте 71. Составление отчёта по событиям домена 72. Фиксирование отказов средств защиты на основе отчёта по событиям домена на защищаемом объекте 73. Составление отчёта по событиям системы на рабочей станции 74. Ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса с помощью программно-аппаратных средств защиты информации 75. Составление сводок по работе DLP-системы и выявление отказов средств защиты 76. Составление виджетов по работе DLP-системы и выявление отказов средств защиты 77. Составление отчётов по работе DLP-системы и выявление отказов средств защиты 78. Составление на основе сводок, виджетом и отчётов по работе DLP-системы плана проведения работ по устранению отказов средств защиты 79. Анализ возможных технических каналов утечки информации после проведённых работ по защите объекта 80. Подбор дополнительных средств и методов защиты на защищаемом объекте 81. Составление инструкции для работы с техническими средствами защиты от утечек информации по проводным линиям 82. Разработка плана применения технических мер по предотвращению проникновения злоумышленника к источникам информации 83. Составление списка возможных угроз информационной безопасности объекта 84. Анализ внешних угроз информационной безопасности объекта 85. Анализ внутренних угроз информационной безопасности объекта 86. Расчёт эффективности применения средств защиты информации 87. Сравнительный анализ продуктов SIEM		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
88. Подбор и расчёт стоимости продукта SIEM			
Производственная практика		**72**	
1.1. Ознакомление с основной деятельностью организации 1.2. Определение информационных активов организации 1.3. Ознакомление с используемыми техническими и инженерно-техническими средствами защиты информации в организации 1.4. Ознакомление с используемыми программно-аппаратными средствами защиты информации в организации 2.1. Выявление утечек информации по техническим каналам 2.2. Выявление утечек информации при эксплуатации программно-аппаратных средств 3.1. Фиксирование отказов средств защиты по техническим каналам 3.2. Фиксирование отказов средств защиты при эксплуатации программно-аппаратных средств		**72**	
Всего по ПМ.03		**705**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально- техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета «Ведение домашнего хозяйства», мастерской «Технологии уборочных работ».

Оборудование учебного кабинета:

-посадочные места по количеству обучающихся;

- рабочее место преподавателя;
- комплект учебно - наглядных пособий;
- стенд «Умный дом»;
- сантехнический комплекс;
- предметы сервировки стола;
- стенд энергоснабжения.

Технические средства обучения: компьютер, проектор, интерактивная доска, программное обеспечение.

Оборудование мастерской:

- поломоечные машины;
- однодисковые машины;
- подметальные машины;
- пылесосы;
- пылеводососы;
- экстракционная машина и пенный экстрактор для чистки ковров.

Реализация программы профессионального модуля (ПМ.01) «Обеспечение работ по ведению домашнего хозяйства» предполагает обязательную учебную и производственную практику.

Учебная практика реализуется в мастерской «Технологии уборочных работ». Производственная практика реализуется в организациях профиля ЖКХ и домашнего хозяйства, обеспечивающих деятельность обучающихся по овладению видом профессиональной деятельности (ВД 1) Обеспечение работ по ведению домашнего хозяйства» и соответствующими ему профессиональными компетенциями.

3.2. Информационное обеспечение реализации программы

МДК 03.01 ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА, ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Основная литература

Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 3-е изд. – Москва : РИОР : ИНФРА-М, 2023. — 400 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для СПО/ О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Дополнительная литература

Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ИД ФОРУМ : НИЦ ИНФРА-М, 2023. — 416 с.: ил. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Ищейнов В. Я. Основные положения информационной безопасности : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян – Москва : Форум, НИЦ ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Партыка Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Внуков А. А. Основы информационной безопасности: защита информации : учебное пособие для СПО / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

МДК 03.02 ПРОГРАММНО – АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Основная литература

Мельников В.П. Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов. — Москва : КноРус, 2022. — 267 с. — (Среднее профессиональное образование). — URL: https://www.book.ru. — Режим доступа: по подписке.

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Хорев П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 2-е изд., испр. и доп. – Москва : Форум : НИЦ ИНФРА-М, 2021. — 352 с.: ил. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для СПО / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Дополнительная литература

Ищейнов В. Я. Основные положения информационной безопасности : учебное пособие / В. Я.Ищейнов, М. В. Мецатунян – Москва : Форум, НИЦ ИНФРА-М, 2021. - 208 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Партыка Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 3-е изд. – Москва : РИОР : ИНФРА-М, 2023. — 400 с. — URL: http://znanium.com. — Режим доступа: по подписке.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ 03

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах	Использование программно-аппаратных и технических средств защиты информации на защищаемых объектах	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Экзамен по ПМ.
Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.	Формирование и применение политик и правил безопасности	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Экзамен по ПМ.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
Проводить регламентные работы и фиксировать отказы средств защиты.	Проведение регламентных работ, подготовка соответствующей отчетной документации	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.
Выявлять и анализировать возможные угрозы информационной безопасности объектов	Выявление возможных угроз информационной безопасности объектов	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
		практических работ и наблюдение в процессе практики Экзамен по ПМ.
Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	проявление интереса к будущей профессии в процессе теоретического обучения, производственной практики	Проверка качества выполнения практических работ, проверка отчетной документации по практике
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области; собственная оценка эффективности и качества выполнения заданий.	Анализ результатов практических работ
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	решение стандартных и нестандартных профессиональных задач	Анализ результатов практических работ
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	эффективный поиск необходимой информации; использование различных источников, включая электронные	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Использовать информационно-коммуникационные технологии в	работа с различными прикладными программами	Анализ результатов практических работ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
профессиональной деятельности		
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ
Применять математический аппарат для решения профессиональных задач.	Применение математических расчетов в ходе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Анализ результатов практических работ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
Оценивать значимость документов, применяемых в профессиональной деятельности.	работа с различными источниками информации нормативно-правой информации	Анализ результатов практических работ
Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	работа с различными источниками информации нормативно-правой информации	Анализ результатов практических работ