Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ
Проректор по учебной и научной работе
Лейфа А.В. Лейфа
« 2 » марта 2024 г.

РАБОЧАЯ ПРОГРАММА
МДК
МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Квалификация выпускника – Техник по защите информации

Год набора – 2024

Курс 2,3 Семестр 3,4,5

Дифференцированный зачет 5 сем

Курсовой проект 5 сем

Общая трудоемкость МДК 310.0 (академ. час)

Составитель О.В. Дорофеева, , Высшая квалификационная категория

Факультет среднего профессионального образования

ЦМК технологических дисциплин

2024

Рабочая программа составлена на основании Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1551

Рабочая программа обсуждена на заседании кафедры технологических дисциплин

09.02.2024 г. , протокол № 6

Заведующий кафедрой Ефремова О.В. Ефремова

СОГЛАСОВАНО
Зам. декана по учебной работе
Кирилюк Н.В. Кирилюк
« 2 » марта 2024 г.

СОГЛАСОВАНО
Выпускающая кафедра
Казакова Т.А. Казакова
« 2 » марта 2024 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
« 2 » марта 2024 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
« 2 » марта 2024 г.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Программа междисциплинарного модуля МДК.02.01 Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных средств защиты является частью образовательной программы в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных системах.

Рабочая программа может быть использована в дополнительном профессиональном образовании.

2. МЕСТО МДК В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Программа междисциплинарного модуля МДК.02.01 Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты входит в профессиональный модуль ПМ.02 Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных (в том числе криптографических) средств защиты читается в 3, 4, 5 семестрах.

На компетенциях, формируемых на профессиональном модуле базируется прохождение производственной практики и производственной практики (преддипломной), а также подготовка и защита дипломного проекта и выполнения демонстрационного экзамена..

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ МДК И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1. Профессиональные компетенции и индикаторы их достижения

Категория (группа) профессиональных компетенций	Код и наименование профессиональных компетенции	Минимальные требования
ПК 2.1.	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	Практический опыт: установки, настройки, испытаний и конфигурирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС; Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно-аппаратных (в том числе

		криптографических) средств защиты информации Знания: способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовых программных и программно- аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС
ПК 2.2.	ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	Практический опыт: поддержания бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить техническое обслуживание и ремонт программно- аппаратных (в том числе криптографических) средств защиты информации Знания: возможных угроз безопасности информации в ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; организации и содержания технического обслуживания и ремонта программно-аппаратных (в

		том числе криптографических) средств защиты информации; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации
ПК 2.3.	ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно–телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	Практический опыт: защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно- аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями Умения: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации Знания: возможных угроз безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовых программных и программно- аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации

4. СТРУКТУРА МДК

Общая трудоемкость МДК составляет 8.61 зачетных единицы, 310.0 академических часов.

1 – № п/п

2 – Тема (раздел) МДК, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

4.10 – У (Уроки)

4.11 – С (Семинарские занятия)

1	2	3	4											5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.10	4.11	4.7	4.8	4.9			
1	Тема 1.1. Обеспечение безопасности операционных систем	3	28		16		16								10	опрос практические/ лабораторные работы
2	Промежуточная аттестация	3														
3	Тема 1.2. Технологии разграничения доступа	4	30		32										5	опрос практические работы
4	Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	4	30		34										5	опрос практические работы
5	Промежуточная аттестация	4														
6	Тема 1.4. Технологии обнаружения вторжений	5	12		18		12									опрос практические/ лаборатор

																ные работы
7	Тема 1.5. Методы управления средствами защиты	5	12		6											опрос практические работы
8	Курсовая работа	5									24	4			16	
9	Промежуточная аттестация	5														
	Итого		112.0		106.0		28.0		0.0	0.0	24.0	4.0	0.0	0.0	36.0	

5. СОДЕРЖАНИЕ МДК

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Тема 1.1. Обеспечение безопасности операционных систем	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. Windows 7. Windows8. Linux. QNX и другие операционные системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации Пароли. PIN- коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи. Программно- аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон – Замок системный администратор. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог.
2	Тема 1.2. Технологии разграничения доступа	Архитектура подсистемы защиты операционной системы Windows Server2016.

		Особенности ОС Windows Server2016. Возможности администратора. Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда. Способы организации. Методы применения. ActiveDirectory. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
3	Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/ IP.Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне.

		Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web- доступ. Протоколы PAP, CHAP,S/ Key, SSO, Kerberos.
4	Тема 1.4. Технологии обнаружения вторжений	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях.Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.
5	Тема 1.5. Методы управления средствами защиты	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.

5.2. Практические занятия

Наименование темы	Содержание темы
Практическая работа № 1	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав

	пользователя
Практическая работа № 2	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита
Практическая работа № 3	Настройка изолированной среды
Практическая работа № 4	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды
Практическая работа № 5	Программы надежного удаления информации
Практическая работа № 6	Архивирование информации
Практическая работа № 7	Программные средства резервного копирования. Настройка RAID-массивов
Практическая работа № 8	Инсайдерская информация. Программы сбора информации о ПК
Практическая работа № 9	Настройка межсетевого экрана.
Практическая работа №10	Основные действия с виртуальной машиной
Практическая работа №11	Работа с контрольными точками
Практическая работа №12	Использование внешних устройств
Практическая работа №13	Работа с локальным хранилищем сертификатов в ОС WINDOWS
Практическая работа №14	Установка и настройка ПО
Практическая работа №15	Настройка ПО с помощью групповых политик
Практическая работа №16	Развертывание TMS в среде Active Directory
Практическая работа №17	Настройка TMS в среде Active Directory
Практическая работа №18	Настройка политик TMS
Практическая работа №19	Настройка использования виртуального токена
Практическая работа № 20	Использование токена на рабочем месте администратора

Практическая работа № 21	Установка и настройка драйверов
Практическая работа № 22	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP
Практическая работа № 23	Применение DallasLock
Практическая работа № 24	Применение MaxPatrolEducation
Практическая работа № 25	Изучение основных возможностей ПО
Практическая работа № 26	Изучение настроек ПО
Практическая работа № 26	Изучение возможностей ПО Деловая почта
Практическая работа № 28	Изучение средств обнаружения атак
Практическая работа № 29	Программные средства проведения аудита безопасности.

5.3. Лабораторные занятия

Наименование темы	Содержание темы
Лабораторная работа № 1	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация
Лабораторная работа № 2	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование
Лабораторная работа № 3	Восстановление информации типовыми средствами Программы восстановление информации
Лабораторная работа № 4	Изучение антивирусных продуктов

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Тема 1.1. Обеспечение безопасности операционных систем	Презентация по теме: "Проблемы обеспечения безопасности операционных системWindowsXP. Windows 7. Windows8. Linux. QNX". Самостоятельное изучение вопроса: Методы аутентификации Подготовка к практическим/ лабораторным работам	10
2	Тема 1.2. Технологии разграничения доступа	подготовить презентацию по теме: "Схемы защиты на базе межсетевых экранов".	5

		Подготовка к практическим работам	
3	Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Подготовка к практическим/ лабораторным работам	5
4	Курсовая работа	Самостоятельная работа по теме курсовой работы	16

Результаты освоения МДК достигаются за счет использования в процессе обучения современных инструментальных средств: лекции с применением мультимедийных технологий, практические занятия с использованием соответствующего оборудования. При проведении занятий используются активные и интерактивные формы. В таблице приведено описание образовательных технологий, используемых в данном модуле.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Примерные вопросы к промежуточной аттестации:

3 семестр:

1. Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. Windows 7. Windows8. Linux. QNX и другие операционные системы.
2. Технологии аутентификации.
3. Аутентификация, авторизация и администрирование действий пользователя.
4. Методы аутентификации
5. Пароли. PIN-коды. Методы надежного составления паролей.
6. Строгая аутентификация.
7. Односторонняя аутентификация. Двухсторонняя аутентификация
8. Аппаратно-программные средства идентификации и аутентификации.
9. Токены. Смарт-карты. Виртуальные ключи.
10. Программно-аппаратные модули доверенной загрузки.
11. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ.
12. АПМДЗ Криптон –Замок системный администратор.
13. Изучение настроек системного администратора АПМДЗ.
14. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ.
15. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ
16. Сектор НЖМД. Область памяти. Файл, папка, каталог.

4 семестр:

1. Архитектура подсистемы защиты операционной системы Windows Server2016.
2. Особенности ОС Windows Server2016. Возможности администратора.
3. Разграничение доступа к объектам операционной системы.
4. Модели доступа. Дискреционная модель. Мандатная модель. Роли.
5. Локальная политика безопасности.
6. Настройка локальной политики безопасности. Администрирование системы.
7. Изолированная программная среда.
8. Способы организации. Методы применения.ActiveDirectory.
9. Комплексная система организации управления доступом. Инсталяция. Настройка.
10. Аудит безопасности операционной системы.

11. Методы проведения контрольных проверочных мероприятий. Программные средства аудита.
12. Функции межсетевых экранов.
13. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.
14. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.
15. Особенности функционирования межсетевых экранов.
16. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня.
17. Схемы защиты на базе межсетевых экранов.
18. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ.
19. Тестирование межсетевых экранов.
20. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
21. Проблемы информационной безопасности сетей.
22. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/ OSI и стек протоколов TCP/ IP.Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях
23. Концепция построения виртуальных защищенных сетей.
24. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование.
25. VPN – решения для построения защищенных сетей.
26. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация.
27. Защита на канальном уровне.
28. Протоколы PPTP, L2F, L2TP.
29. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.\
30. Защита на сетевом уровне.
31. Архитектура средств безопасности IPSec, AH, ESP.Защита на прикладном уровне.
32. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web- доступ. Протоколы PAP, CHAP,S/ Key, SSO, Kerberos.

5 семестр (дифференцированный зачет):
1. Технология обнаружения атак.
2. Концепция адаптивного управления безопасностью. Технология анализа защищенности.
3. Средства анализа защищенности сетевых протоколов и сервисов.
4. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.
5. Средства обнаружения сетевых атак.
6. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях.Методы реагирования на сетевые атаки.
7. Обзор современных средств обнаружения атак.
8. Технологии защиты от вирусов.
9. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусовЖизненный цикл вирусов. Основные каналы распространения

вирусов и других вредоносных программ.
10. Методы управления средствами сетевой защиты.
11. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты.
12. Аудит безопасности информационной системы.
13. Мониторинг безопасности системы. Программные средства проведения аудита безопасности.
14. Обзор современных систем управления сетевой защитой.
15. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.

Примерная тематика курсовых работ :
1. Модель угроз НСД на предприятии
2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии
3. Проведение классификации ПО по требованиям ФСТЭК на предприятии
4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии
5. Построение модели нарушителя по требованиям ФСТЭК на предприятии
6. Построение модели нарушителя по требованиям ФСБ на предприятии
7. Модель угроз безопасности ИС персональных данных на предприятии
8. Комплексная модель защиты информации на предприятии.
9. Оценка эффективности существующих программных и программно- аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
10. Обзор и анализ современных программно- аппаратных средств защиты информации (индивидуальное задание)
11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
13. Проблема защиты информации в облачных хранилищах данных и ЦОДах
14. Защита сред виртуализации.

Результаты (освоенные профессиональные компетенции)	Формы и методы контроля и оценки
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно- аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	опрос практические работы лабораторные работы курсрсовой проект
ПК 2.2. Поддерживать бесперебойную работу программных и программно- аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	опрос практические работы лабораторные работы курсрсовой проект
ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно– телекоммуникационных системах и сетях с использованием программных и программно-	опрос практические работы лабораторные работы курсрсовой проект

аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	

8. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ МДК

а) литература

Основная литература

Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 464 с. — (Профессиональное образование). — ISBN 978-5-534-17310-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/bcode/542157

Казарин, О. В. Программно- аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/bcode/543631

Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3- е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340

Дополнительная литература

Солонская, О. И. Средства защиты информации : учебное пособие для СПО / О. И. Солонская. — Саратов : Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/125578.html

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, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/bcode/542339

Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Саратов : Профобразование, 2024. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/139767.html (дата обращения: 10.07.2024). — Режим доступа: для авторизир. пользователей

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2024. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537691

Защита персональных данных : учебное пособие для СПО / О. М. Голембиовская, М. Ю. Рытов, Ю. Ю. Громов [и др.]. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. — 156 с. — ISBN 978-5-4488-1753-3, 978-5-4497-2662-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/135612.html

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Google Chrome	Бесплатное распространение по лицензии google chromium http:// code.google.com/ intl/ ru/ chromium/ terms.html на условиях https:// www.google.com/ chrome/ browser/privacy/eula_text.html.
2	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
3	VirtualBox	Бесплатное распространение по лицензии GNU GPL https://www.virtualbox.org/wiki/GPL

в) профессиональные базы данных и информационные справочные системы

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ МДК

Занятия по МДК.02.01 проводятся в учебной аудитории, компьютерном классе, лаборатории информационно- телекоммуникационных систем и сетей, лаборатории защиты информации от утечки по техническим каналам, лаборатории программных и программно- аппаратных средств защиты информации, кабинете метрологии и стандартизации

Оснащения кабинета: Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, доска, мультимедиа-проектор, проекционный экран, ПК.

Оснащение лаборатории: Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, ПК, лабораторное оборудование.