Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В.18 Методы и средства защиты информации

2025

Программу составили:

1. Кононова Наталия Владимировна

Дисциплина: ОП.В.18 Методы и средства защиты информации

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утверждённым приказом Минобрнауки России от 09.12.2016 г. №1553.

Рабочая программа учебной дисциплины составлена на основании учебного плана по специальности «10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Визирование РПД для исполнения в очередном учебном году

Рассмотрено и рекомендовано на заседании кафедры Информационной безопасности

Протокол №10 от 12.05.2025

Заведующий кафедрой Кононова Наталия Владимировна

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В.18 Методы и средства защиты информации

(наименование дисциплины)

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.В.18 Методы и средства защиты информации является обязательной частью обязательной частью цикла основной образовательной программы в соответствии ФГОС «10.02.05 Обеспечение информационной безопасности автоматизированных систем»по специальности . Особое значение дисциплина имеет при формировании и развитии общих компетенций (ОК), профессиональных компетенций (ПК):

1. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами

1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	Умения	Знания
ПК 2.2.	Применять технические средства для криптографической защиты информации конфиденциального характера;; Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;; Применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;; Применять инженерно-технические средства физической защиты объектов информатизации.	Номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;; Основные способы физической защиты объектов информатизации;; Физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;; Основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;; Методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;; Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объём учебной дисциплины и виды учебной дисциплины

Вид учебной работы	**Объём в часах**
Практические занятия	6
Лабораторные занятия	6
Лекционные занятия	32
Практическая подготовка	46
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	90
Форма(-ы) контроля: Дифференцированный зачет	

2.2. Тематический план и содержание учебной дисциплины ОП.В.18 Методы и средства защиты информации

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы

Наименование разделов и тем		Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 1 Новый раздел	Содержание учебного материала				ПК 2.2.
	1	**Лекционные занятия №1** Ретроспективный анализ развития подходов к разработке средств криптографической защиты информации.	2	1	
	2	**Лабораторные занятия №1** Угрозы безопасности информации на предприятии	2	2	
	3	**Лекционные занятия №2** Информация общедоступная и ограниченного доступа. Категории ценности информации. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак.	2	1	
	4	**Лабораторные занятия №2** Защита информации от традиционного шпионажа и диверсий	2	2	
	5	**Лекционные занятия №3** Модели сетевой безопасности и безопасности информационной системы. Информация как объект защиты.	2	1	
	6	**Лабораторные занятия №3** Защита информации от случайных угроз	2	2	
	7	**Лекционные занятия №4** Основные задачи обеспечения криптографической защиты информации.	2	1	
	8	**Практическая подготовка №1** Основные этапы проектирования системы защиты информации	4	2	
	9	**Лекционные занятия №5** Основные методы и средства защиты информации в информационных системах. Анализ угроз информационной безопасности; классификация угроз.	2	1	
	10	**Практическая подготовка №2** Специфика персонала предприятия как объекта защиты	4	2	
	11	**Лекционные занятия №6** Архитектура электронных систем обработки данных; формальные модели; модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем;	2	1	
	12	**Лабораторные занятия №4** Формирование и изучение свойств модели Белла–ЛаПадула	2	2	
	13	**Практическая подготовка №3** Разработка моделей объектов защиты	4	2	
	14	**Лекционные занятия №7** Стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем; особенности применения криптографических методов; способы реализации криптографической подсистемы;	2	1	
	15	**Лабораторные занятия №5** Модель доменов и типов для unix-систем	2	2	
	16	**Практическая подготовка №4** Электронная цифровая подпись (ЭЦП)	4	2	
	17	**Лекционные занятия №8** Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости.	2	1	
	18	**Лабораторные занятия №6** Изучение программной системы защиты	2	2	
	19	**Практическая подготовка №5** Методы аутентификации и способы управления доступом	4	2	
	20	**Лекционные занятия №9** Общие сведения об электронной цифровой подписи (ЭЦП). Алгоритм ЭЦП в симметричной криптосистеме. Алгоритм ЭЦП в асимметричной криптосистеме. Проблема обмена открытыми ключами при ЭЦП. Сложные математические задачи и алгоритмы ЭЦП с открытыми ключами. Алгоритм DSA. Алгоритм ГОСТ Р34.10–94. Стандарт ЭЦП Р34.10– 2001	2	1	
	21	**Практическая подготовка №6** Защита информации от электомагнитного излучения, наводок	4	2	
	22	**Лекционные занятия №10** Функции хэширования. Классификация. Функции хэширования без ключа (MDC) и с ключом (MAC). Принципы построения. Функции хэширования Ривеста: MD2, MD4, MD5. Американский стандарт функции хэширования (SHS) и его изменения. Российский стандарт функции хэширования (ГОСТ Р 34.11-94). Применение функции хэширования в схемах цифровой подписи и при построении криптосистем. Сильные хэш- функции SHA-1, SHA-2 и ГОСТ 34.11-94. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш- функций и алгоритма HMAC. Контроль целостности данных. Идентификация и аутентификация	2	1	
	23	**Практическая подготовка №7** Исследование протокола IPSec	4	2	
	24	**Лекционные занятия №11** Программно-аппаратные средства защиты ПЭВМ и сетей; методы средства ограничения доступа к компонентам сети; методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям: методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности	2	1	
	25	**Практическая подготовка №8** Изучение средств IP-безопасности, обеспечиваемых протоколом IPsec	4	2	
	26	**Лекционные занятия №12** Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды	2	1	
	27	**Практическая подготовка №9** Организация комплексной системы защиты информации объекта	2	2	
	28	**Лекционные занятия №13** Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. Программно- аппаратные средства защиты ПЭВМ	2	1	
	29	**Практическая подготовка №10** Защита информации правовыми и организационными методами (ПР)	4	2	
	30	**Лекционные занятия №14** Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Постановка задач оптимизации систем защиты информации.	2	1	
	31	**Практическая подготовка №11** Моделирование технических каналов утечки информации	4	2	
	32	**Лекционные занятия №15** Защита компьютерных сетей от удаленных атак	2	1	
	33	**Практическая подготовка №12** Анализ рисков безопасности информации	4	2	
	34	**Лекционные занятия №16** Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. Перспективы КЗИ: защищенные информационные технологии (ЛК)	2	1	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
	Всего	90		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (ознакомление с ранее изученными объектами, свойствами);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие помещения:

Лекционная аудитория:

1. Проектор (1 шт.)

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

1. Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. Защита информации в персональном компьютере: учебное пособие /— 2-е изд. —— 368 с. — (Среднее профессиональное образование). URL: https://znanium.com/catalog/product/1189325 Москва : ФОРУМ : ИНФРА-М, 2021.

3.2.2. Дополнительные источники

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие —— 201 с. — (Среднее профессиональное образование).. - URL: https://znanium.com/catalog/product/1191479 Москва : ИНФРА-М, 2021.

3.2.3. Интернет-ресурсы

1. Электронно-библиотечная система Znanium.com
2. Электронно- библиотечная система BOOK.RU

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Образовательные результаты освоения образовательной программы учебной дисциплины, подлежащие проверке

Результаты обучения	Критерии оценки	Методы оценки
Знание		
Номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;	Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;	Коллоквиум
Основные способы физической защиты объектов информатизации;	Знать основные способы физической защиты объектов информатизации;	Коллоквиум
Физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;	Знать физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;	Коллоквиум
Основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;	Знать основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;	Коллоквиум
Методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	Знать методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	Коллоквиум
Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.	Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.	Коллоквиум
Умение		
Применять технические средства для криптографической защиты информации конфиденциального характера;	Уметь применять технические средства для криптографической защиты информации конфиденциального характера;	Тестирование
Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	Уметь применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	Тестирование
Применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Уметь применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Тестирование
Применять инженерно-технические средства физической защиты объектов информатизации.	Уметь применять инженерно-технические средства физической защиты объектов информатизации.	Тестирование

4.2. Матрица соответствия контрольно-оценочных средств образовательным результатам учебной дисциплины

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		

Результаты обучения	Коды компетенций	Фонды оценочных средств
Номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;	ПК 2.2.	Вопросы к дифференцированному зачёту №6-10
Основные способы физической защиты объектов информатизации;	ПК 2.2.	Вопросы к дифференцированному зачёту №16-20
Физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;	ПК 2.2.	Вопросы к дифференцированному зачёту №1-5
Основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;	ПК 2.2.	Вопросы к дифференцированному зачёту №11-15
Методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	ПК 2.2.	Вопросы к дифференцированному зачёту №21-25
Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.	ПК 2.2.	Вопросы к дифференцированному зачёту №26-30
Умение		
Применять технические средства для криптографической защиты информации конфиденциального характера;	ПК 2.2.	Вопросы к дифференцированному зачёту №36-40
Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	ПК 2.2.	Вопросы к дифференцированному зачёту №31-35
Применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	ПК 2.2.	Вопросы к дифференцированному зачёту №41-45
Применять инженерно-технические средства физической защиты объектов информатизации.	ПК 2.2.	Вопросы к дифференцированному зачёту №46-50

Вопросы к лабораторной работе указаны в методических указаниях к лабораторной работепо дисциплине Методы и средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025 Вопросы к практической подготовке указаны в методических указаниях к практической подготовкепо дисциплине Методы и средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025 Вопросы к практическому занятию указаны в методических указаниях к практическим занятиямпо дисциплине Методы и средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025