

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**

2022

Программу составили:

1. Хвалько Леонид Александрович

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 на заседании методического объединения Укрупненных групп специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность»

Протокол №6 от 26.05.2022

Председатель МО Харченко Ирина Владимировна

**Данные не найдены (РПД не рекомендовано)**

# **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 по специальности «10.02.05 Обеспечение информационной безопасности автоматизированных систем». Особое значение дисциплина имеет при формировании и развитии общих компетенций (ОК), профессиональных компетенций (ПК) и личностных результатов (ЛР):

1. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
2. ЛР 2 Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
3. ЛР 3 Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
4. ЛР 7 Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
5. ЛР 16 Выработавший умения и навыки трудовой деятельности, проявляющий основы трудовой культуры по отношению к коллегам, контрагентам и клиентам Компании
6. ЛР 22 Выработавший принципы экологически целесообразного поведения, бережного отношения к своей жизни, жизни других людей, природы, планеты в целом

### **1.2. Цель и планируемые результаты освоения дисциплины**

В рамках программы учебной дисциплины обучающимися осваиваются

умения и знания

Код ОК, ПК, ЛР	Умения	Знания
ПК 2.2., ЛР 2, ЛР 3, ЛР 7, ЛР 16, ЛР 22	<p>Применять инженерно-технические средства физической защиты объектов информатизации.;</p> <p>Применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных.;</p> <p>Применять технические средства для криптографической защиты информации конфиденциального характера.;</p> <p>Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом.;</p>	<p>Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.;</p> <p>Методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации.;</p> <p>Основные способы физической защиты объектов информатизации.;</p> <p>Основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации.;</p> <p>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.;</p> <p>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.;</p>

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объём учебной дисциплины и виды учебной дисциплины

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

## **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 и личностных результатов, формированию которых способствует элемент программы
-----------------------------	--	---------------	------------------	--

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 1 Новый раздел	Содержание учебного материала			ЛР 2, ЛР 3, ЛР 7, ЛР 16, ЛР 22
	1 <b>Лекционные занятия №1</b> Ретроспективный анализ развития подходов к разработке средств криптографической защиты информации.	2	1	
	2 <b>Практические занятия №1</b> Угрозы безопасности информации на предприятии	2	2	
	3 <b>Лекционные занятия №2</b> 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 <b>Практические занятия №2</b> Защита информации от традиционного шпионажа и диверсий	2	2	
	5 <b>Лекционные занятия №3</b> Модели сетевой безопасности и безопасности информационной системы. Информация как объект защиты.	2	1	
	6 <b>Практические занятия №3</b> Защита информации от случайных угроз	2	2	
	7 <b>Лекционные занятия №4</b> Основные задачи обеспечения криптографической защиты информации.	2	1	
	8 <b>Практическая подготовка №1</b> Основные этапы проектирования системы защиты информации	4	2	
	9 <b>Лекционные занятия №5</b> Основные методы и средства защиты информации в информационных системах. Анализ угроз информационной безопасности; классификация угроз.	2	1	
	10 <b>Практическая подготовка №2</b> Специфика персонала предприятия как объекта защиты	4	2	
	11 <b>Лекционные занятия №6</b> 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 <b>Лабораторные занятия №1</b> Формирование и изучение свойств модели Белла–ЛаПадула	2	2	
	13 <b>Практическая подготовка №3</b> Разработка моделей объектов защиты	4	2	
	14 <b>Лекционные занятия №7</b> Стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем; особенности применения криптографических методов; способы реализации криптографической подсистемы;	2	1	
	15 <b>Лабораторные занятия №2</b> Модель доменов и типов для шпих-систем	2	2	
	16 <b>Практическая подготовка №4</b> Электронная цифровая подпись (ЭЦП)	4	2	
	17 <b>Лекционные занятия №8</b> 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 <b>Лабораторные занятия №3</b> Изучение программной системы защиты	2	2	
	19 <b>Практическая подготовка №5</b> Методы аутентификации и способы управления доступом	4	2	
	20 <b>Лекционные занятия №9</b> 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 Р 34.10–94. Стандарт ЭЦП Р 34.10– 2001	2	1	
	21 <b>Практическая подготовка №6</b> Защита информации от электромагнитного излучения, наводок	4	2	
	22 <b>Лекционные занятия №10</b> 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 <b>Практическая подготовка №7</b> Исследование протокола IPsec	4	2	
	24 <b>Лекционные занятия №11</b> 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 <b>Практическая подготовка №8</b> Изучение средств IP-безопасности, обеспечиваемых протоколом IPsec	4	2	
	26 <b>Лекционные занятия №12</b> 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 <b>Практическая подготовка №9</b> Организация комплексной системы защиты информации объекта	2	2	
	28 <b>Лекционные занятия №13</b> Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. Программно- аппаратные средства защиты ПЭВМ	2	1	
	29 <b>Практическая подготовка №10</b> Защита информации правовыми и организационными методами (ПР)	4	2	
	30 <b>Лекционные занятия №14</b> Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Постановка задач оптимизации систем защиты информации.	2	1	
	31 <b>Практическая подготовка №11</b> Моделирование технических каналов утечки информации	4	2	
	32 <b>Лекционные занятия №15</b> Защита компьютерных сетей от удаленных атак	2	1	
	33 <b>Практическая подготовка №12</b> Анализ рисков безопасности информации	4	2	
	34 <b>Лекционные занятия №16</b> 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 и личностных результатов, 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:**

Компьютерный класс  
Кабинет информатики  
Лаборатория технологии разработки баз данных  
Лаборатория системного и прикладного программирования  
Лаборатория информационно-коммуникационных систем  
Лаборатория управления проектной деятельностью  
Лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств  
Лаборатория программного обеспечения и сопровождения компьютерных систем  
Лаборатория программирования и баз данных  
Лаборатория организации и принципов построения информационных систем  
Лаборатория информационных ресурсов:

1. Клавиатура (16 шт.)
2. Матрешка – Z (набор – конструктор) (5 шт.)
3. Robobuilder RQ – HUNO (Многофункциональный робот-андроид) (1 шт.)
4. Монитор (16 шт.)
5. Мышь компьютерная (16 шт.)
6. Плакаты (32 шт.)
7. Системный блок (16 шт.)
8. Стенды (4 шт.)

Лаборатория сетей и систем передачи информации  
Лаборатория электроники и схемотехники  
Лаборатория программных и программно-аппаратных средств защиты информации  
Лаборатория технических средств защиты информации  
Полигон вычислительной техники  
Полигон учебных баз практик  
Методический кабинет  
Кабинет для самостоятельной работы:

1. Монитор (9 шт.)
2. Мышь компьютерная (9 шт.)
3. Системный блок (9 шт.)

4. Стенды (3 шт.)
5. Клавиатура (9 шт.)

Кабинет информационных систем в профессиональной деятельности

Кабинет информатики и математики

Кабинет компьютерного дизайна

Лаборатория информационных технологий в профессиональной деятельности

Лаборатория информационных технологий

Лаборатория компьютерного дизайна

Лаборатория разработки веб-приложений

Студия инженерной и компьютерной графики

Студия разработки дизайна веб-приложений

Кабинет для самостоятельной работы:

1. Системный блок (9 шт.)
2. Монитор (9 шт.)
3. Мышь компьютерная (9 шт.)
4. Стенды (1 шт.)
5. Клавиатура (9 шт.)
6. Плакаты (34 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
Умение		
Применять инженерно-технические средства физической защиты объектов информатизации.	Уметь применять инженерно-технические средства физической защиты объектов информатизации.	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 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
Знание		
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
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
Основные способы физической защиты объектов информатизации;	Знать основные способы физической защиты объектов информатизации;	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
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
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

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		
Применять инженерно-технические средства физической защиты объектов информатизации.	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №46-50

Результаты обучения	Коды компетенций	Фонды оценочных средств
Применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №41-45
Применять технические средства для криптографической защиты информации конфиденциального характера;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №36-40
Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №31-35
<b>Знание</b>		
Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №26-30
Методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №21-25
Основные способы физической защиты объектов информатизации;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №16-20
Основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №11-15
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;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №1-5
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;	ЛР 16, ЛР 2, ЛР 22, ЛР 3, ЛР 7, ПК 2.2.	Вопросы к дифференцированному зачёту №6-10

Вопросы к диф. зачету, Задание к лабораторной и практической работе, находятся в МЕТОДИЧЕСКИХ УКАЗАНИЯХ к лабораторным работам и практическим занятиям для студентов специальности 10.02.05 "Обеспечение информационной безопасности автоматизированных систем". Ставрополь. 2022. Методические указания к лабораторным работам, практическим занятиям и практическим подготовкам для обучающихся специальности 10.02.05 "Обеспечение информационной безопасности автоматизированных систем". Ставрополь. 2022.