

Приложение

К ООП по специальности/профессии

**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ОП.В.13 Безопасность сетей ЭВМ**

2025

Программу составили:

1. Кононова Наталия Владимировна

Дисциплина: ОП.В.13 Безопасность сетей ЭВМ

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.13 Безопасность сетей ЭВМ

(наименование дисциплины)

### 1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.В.13 Безопасность сетей ЭВМ 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 3.5. Организовывать отдельные работы по физической защите объектов информатизации

### 1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	Умения	Знания
ПК 3.5.	настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;;  обеспечивать работоспособность, обнаруживать и устранять неисправности	принципы разработки алгоритмов программ, основных приемов программирования;;  порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;  Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.;  теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

## 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	16
Лабораторные занятия	6
Практические занятия	6
Часы на контроль	18
Практическая подготовка	36
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	82
<b>Форма(-ы) контроля: Экзамен</b>	

## 2.2. Тематический план и содержание учебной дисциплины ОП.В.13 Безопасность сетей ЭВМ

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 Лекции	Содержание учебного материала			ПК 3.5.
	1 Лекционные занятия №1 Обеспечение информационной безопасности	2	1	
	2 Лекционные занятия №2 Управление риском	2	1	
	3 Лекционные занятия №3 Политика	2	1	
	4 Лекционные занятия №4 Юридические вопросы информационной безопасности	2	1	
	5 Лекционные занятия №5 Службы информационной безопасности	2	1	
	6 Лекционные занятия №6 Методы хакеров	2	1	
	7 Лекционные занятия №7 Категории атак	2	1	
	8 Лекционные занятия №8 Определение информационной безопасности	2	1	
Тема 2 Практические занятия	Содержание учебного материала			ПК 3.5.
	1 Практические занятия №1 Необходимость использования СОВ	2	2	
	2 Практические занятия №2 История появления СОВ	2	2	
	3 Практические занятия №3 Нормативно-методические документы по защите информации	2	2	
Тема 3 Лабораторные работы	Содержание учебного материала			ПК 3.5.
	1 Лабораторные занятия №1 Действия при обнаружении атак Пассивные действия при обнаружении атаки	2	2	
	2 Лабораторные занятия №2 Место и роль СОВ в обеспечении защиты	2	2	
	3 Лабораторные занятия №3 Место и роль СОВ в обеспечении защиты	2	2	

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 4 Практическая подготовка	Содержание учебного материала			ПК 3.5.	
	1	Практическая подготовка №1 Слабые и сильные стороны СОВ. Будущее СОВ	2		2
	2	Практическая подготовка №2 Архитектура СОВ	4		2
	3	Практическая подготовка №3 Установка и настройка Защищённого Рабочего Места ViPNet [Клиент] Часть 2 .	2		2
	4	Практическая подготовка №4 Установка и настройка Защищённого Рабочего Места ViPNet [Клиент] Часть 1.	4		2
	5	Практическая подготовка №5 Межсетевое взаимодействие защищенных сетей ViPNet. Часть вторая – АММК	4		2
	6	Практическая подготовка №6 Межсетевое взаимодействие защищенных сетей ViPNet. Часть первая – СММК	4		2
	7	Практическая подготовка №7 Модификация защищенной сети ViPNet. Часть 2	4		2
	8	Практическая подготовка №8 Модификация защищенной сети ViPNet. Часть 1	4		2
	9	Практическая подготовка №9 Первоначальное развертывание защищенной виртуальной сети на базе комплекса ViPNet. Часть 2.	4		2
10	Практическая подготовка №10 Первоначальное развертывание защищенной виртуальной сети на базе комплекса ViPNet. Часть 1.	4	2		
Тема 5 Промежуточная аттестация	Содержание учебного материала			ПК 3.5.	
	1	Часы на контроль Промежуточная аттестация	18		2
		Всего	82		

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:**

Лаборатория сетей и систем передачи информации  
Лаборатория программных и программно-аппаратных средств защиты информации  
Лаборатория технических средств защиты информации:

1. Компьютерный стол (15 шт.)
2. Стул (15 шт.)
3. Доска (1 шт.)
4. Системный блок (15 шт.)
5. Монитор (15 шт.)
6. Клавиатура (15 шт.)
7. Компьютерная мышь (15 шт.)
8. Проектор (1 шт.)

#### **3.2. Информационное обеспечение реализации программы**

##### **3.2.1. Основные печатные издания**

1. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем:
2. Учебное пособие <http://znanium.com/catalog/product/507334> НИЦ ИНФРА-М, 2021,

##### **3.2.2. Дополнительные источники**

1. Пескова, О. Ю. Безопасность сетей ЭВМ : учебное пособие / О. Ю. Пескова, Е. С. Басан ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университет, 2024. - 183 с. - ISBN 978-5-9275-4634-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2180510>

##### **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		
настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;	Уметь настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;	Тестирование
обеспечивать работоспособность, обнаруживать и устранять неисправности	Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности	Тестирование
Знание		
принципы разработки алгоритмов программ, основных приемов программирования;	Знать принципы разработки алгоритмов программ, основных приемов программирования;	Коллоквиум
порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	Знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	Коллоквиум
Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	Коллоквиум
теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	Знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	Коллоквиум

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		
настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;	ПК 3.5.	Вопросы на экзамен №38-45
обеспечивать работоспособность, обнаруживать и устранять неисправности	ПК 3.5.	Вопросы на экзамен №46-52
Знание		
принципы разработки алгоритмов программ, основных приемов программирования;	ПК 3.5.	Вопросы на экзамен №1-9
порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	ПК 3.5.	Вопросы на экзамен №20-28
Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	ПК 3.5.	Вопросы на экзамен №29-37
теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	ПК 3.5.	Вопросы на экзамен №10-19

Вопросы к практическому занятию указаны в методических указаниях к практическим занятиям по дисциплине Безопасность сетей ЭВМ для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025 Вопросы к лабораторной работе

указаны в методических указаниях к лабораторной работе по дисциплине Безопасность сетей ЭВМ для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025

Вопросы к практической подготовке указаны в методических указаниях к практической подготовке по дисциплине Безопасность сетей ЭВМ для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025