

Приложение

К ООП по специальности/профессии

**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**МДК.03.01 Техническая защита информации**

2024

Программу составили:

1. Хвалько Леонид Александрович

Дисциплина: МДК.03.01 Техническая защита 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 №7 от 26.05.2023

Заведующий кафедрой

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## МДК.03.01 Техническая защита информации

(наименование дисциплины)

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

Учебная дисциплина МДК.03.01 Техническая защита 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) и личностных результатов (ЛР):

1. ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
2. ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
3. ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
4. ОК 09. Использовать информационные технологии в профессиональной деятельности.
5. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
6. ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
7. ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
8. ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
9. ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
10. ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
11. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
12. ПК 3.5. Организовывать отдельные работы по физической защите объектов

информатизации.

13. ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

14. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

15. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

## 1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК, ЛР	Умения	Знания
ОК 02., ОК 03., ОК 05., ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 08., ОК 10., ПК 3.2., ПК 3.5., ПК 3.1., ПК 3.3., ПК 3.4.	проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;;  использовать типовые программные криптографические средства, в том числе электронную подпись;	типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.;  основные понятия криптографии и типовых криптографических методов и средств защиты информации;;  методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

## 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>
Практические занятия	30
Лекционные занятия	76
Часы на контроль	18
Практическая подготовка	48
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	172
<b>Форма(-ы) контроля: Дифференцированный зачет, Экзамен</b>	

## 2.2. Тематический план и содержание учебной дисциплины МДК.03.01 Техническая защита 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
Тема 1 Промежуточная аттестация	Содержание учебного материала			<b>Данные не найдены (к темам в разделе не привязано компетенций)</b>
1	Часы на контроль Промежуточная аттестация	18	2	
Тема 2 Практическая подготовка	Содержание учебного материала			<b>Данные не найдены (к темам в разделе не привязано компетенций)</b>
1	<b>Практическая подготовка №1</b> Настройка аутентификации пользователей с помощью электронного замка «СОБОЛЬ-РСИ. Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	2	
2	<b>Практическая подготовка №2</b> Изучение правовых основ защиты информации и информационной безопасности (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»). Аппаратно-программные средства контроля доступа	2	2	
3	<b>Практическая подготовка №3</b> Моделирование технических каналов утечки информации. Анализ рисков безопасности информации.	4	2	
4	<b>Практическая подготовка №4</b> Защита информации правовыми и организационными методами	4	2	
5	<b>Практическая подготовка №5</b> Организация комплексной системы защиты информации объекта	4	2	
6	<b>Практическая подготовка №6</b> Изучение средств IP-безопасности, обеспечиваемых протоколом Ipsec	4	2	
7	<b>Практическая подготовка №7</b> Исследование протокола IPSec	4	2	
8	<b>Практическая подготовка №8</b> Защита информации от электромагнитных излучений и наводок	4	2	
9	<b>Практическая подготовка №9</b> Методы аутентификации и способы управления доступом	4	2	
10	<b>Практическая подготовка №10</b> Изучение особенностей аттестации помещений по требованиям безопасности информации. Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации	4	2	
11	<b>Практическая подготовка №11</b> Изучение положения о сертификации средств вычислительной техники и связи. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации	4	2	
12	<b>Практическая подготовка №12</b> Система сертификации средств криптографической защиты информации	2	2	
13	<b>Практическая подготовка №13</b> Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	2	2	
14	<b>Практическая подготовка №14</b> Изучение положений о государственном лицензировании деятельности в области защиты информации	2	2	
15	<b>Практическая подготовка №15</b> Законодательство РФ в области информационной безопасности	2	2	

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 3	Содержание учебного материала			<b>Данные не найдены</b>
Практические занятия	1 <b>Практические занятия №1</b> Электронно-цифровая подпись	2	2	<b>(к темам в разделе не привязано компетенций)</b>
	2 <b>Практические занятия №2</b> Разработка моделей объектов защиты	2	2	
	3 <b>Практические занятия №3</b> Специфика персонала предприятия как объекта защиты	2	2	
	4 <b>Практические занятия №4</b> Основные этапы проектирования системы защиты информации	2	2	
	5 <b>Практические занятия №5</b> Защита информации от случайных угроз	2	2	
	6 <b>Практические занятия №6</b> Защита информации от традиционного шпионажа и диверсий	2	2	
	7 <b>Практические занятия №7</b> Угрозы безопасности информации на предприятии	2	2	
	8 <b>Практические занятия №8</b> Адаптер записи с телефонной линии ICON TRX1	2	2	
	9 <b>Практические занятия №9</b> Беспроводная IP-камера для помещений Link 128 МИНИ	2	2	
	10 <b>Практические занятия №10</b> Подавитель диктофонов Бубен-ультра	2	2	
	11 <b>Практические занятия №11</b> Видеорегистратор LawMate PV-550SE с камерой 618CA	2	2	
	12 <b>Практические занятия №12</b> Микрофон усиливающий «Супер Ухо SD»	2	2	
	13 <b>Практические занятия №13</b> Видеозондоскоп MaxiVideo MV208	2	2	
	14 <b>Практические занятия №14</b> Видеоглазок беспроводной Radio DVR	2	2	
	15 <b>Практические занятия №15</b> Автономный регистратор сотовых разговоров SpRecord SpGate MR	2	2	

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 4 Лекции	Содержание учебного материала			Данные не найдены
	1 Лекционные занятия №1 Настройка средств защиты информации сервера	2	1	(к темам в разделе не привязано компетенций)
	2 Лекционные занятия №2 Настройка средств криптографической защиты сетевого трафика стандартного протокола IPsec	2	1	
	3 Лекционные занятия №3 Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	1	
	4 Лекционные занятия №4 правовые основы защиты информации и информационной безопасности (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»)	2	1	
	5 Лекционные занятия №5 Система технической защиты информации. Часть 2	2	1	
	6 Лекционные занятия №6 Способы и средства оценки эффективности инженерно-технической защиты информации. Часть 1.	2	1	
	7 Лекционные занятия №7 Лицензирование деятельности и сертификация средств защиты информации. Часть 2.	2	1	
	8 Лекционные занятия №8 Лицензирование деятельности и сертификация средств защиты информации. Часть 1.	2	1	
	9 Лекционные занятия №9 Характеристика каналов утечки информации от средств связи и ПЭМИН. Средства технической защиты для этих каналов. Часть 2.	2	1	
	10 Лекционные занятия №10 Характеристика каналов утечки информации от средств связи и ПЭМИН. Средства технической защиты для этих каналов. Часть 1.	2	1	
	11 Лекционные занятия №11 Управление средствами информационной безопасности сервера	2	1	
	12 Лекционные занятия №12 Изменение политики контроля устройств	2	1	
	13 Лекционные занятия №13 Настройка аутентификации пользователей с помощью электронного замка	2	1	
	14 Лекционные занятия №14 Аппаратно-программные средства контроля доступа	2	1	
	15 Лекционные занятия №15 Система технической защиты информации. Часть 1	2	1	
	16 Лекционные занятия №16 Способы и средства оценки эффективности инженерно-технической защиты информации. Часть 2.	2	1	
	17 Лекционные занятия №17 Технические средства защиты от наблюдения и линий связи от утечки конфиденциальной информации. Часть 2.	2	1	
	18 Лекционные занятия №18 Технические средства защиты от наблюдения и линий связи от утечки конфиденциальной информации. Часть 1.	2	1	
	19 Лекционные занятия №19 Технические средства защиты информации в акустических и вибрационных полях.	2	1	
	20 Лекционные занятия №20 Технические каналы утечки акустической (речевой) и видовой информации.	2	1	
	21 Лекционные занятия №21 Технические каналы утечки информации с СВТ и ИС.	2	1	
	22 Лекционные занятия №22 Цели и задачи защиты информации от утечки информации по техническим каналам	2	1	
	23 Лекционные занятия №23 Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Часть 2	2	1	
	24 Лекционные занятия №24 Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Часть 1	2	1	
	25 Лекционные занятия №25 Основные механизмы защиты информации	2	1	
	26 Лекционные занятия №26 Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации	2	1	
	27 Лекционные занятия №27 Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации	2	1	
	28 Лекционные занятия №28 Анализ существующих методик определения требований к защите информации	2	1	
	29 Лекционные занятия №29 Каналы и методы несанкционированного доступа к информации. Уязвимости	2	1	
	30 Лекционные занятия №30 Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации	2	1	
	31 Лекционные занятия №31 Цели и задачи защиты информации. Основные понятия в области защиты информации	2	1	
	32 Лекционные занятия №32 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Часть 1	2	1	
	33 Лекционные занятия №33 Целостность, доступность и конфиденциальность информации	2	1	
	34 Лекционные занятия №34 Понятие информации и информационной безопасности	2	1	
	35 Лекционные занятия №35 Организационная структура системы защиты информации. Законодательные акты в области защиты информации	2	1	
	36 Лекционные занятия №36 Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации	2	1	
	37 Лекционные занятия №37 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Часть 2	2	1	
	38 Лекционные занятия №38 Понятие «угроза информации». Понятие «риска информационной безопасности»	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	172	

*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  
Лаборатория информационных технологий:

1. Стол компьютерный (16 шт.)
2. стол (3 шт.)
3. стул (16 шт.)
4. доска (1 шт.)
5. Расширенный дверной проем (1 шт.)
6. Плакаты по информационным технологиям в профессиональной деятельности (12 шт.)
7. плакаты по стратегическому и тактическому планированию рекламных мероприятий (5 шт.)
8. стенды информационные технологии в профессиональной деятельности (4 шт.)
9. плакаты по стратегическому и тактическому планированию коммуникационных кампаний (7 шт.)
10. Рабочее место преподавателя, персональный компьютер с подключением к сети «Интернет» (1 шт.)
11. Системный блок (16 шт.)
12. Монитор (16 шт.)
13. Клавиатура (16 шт.)
14. Мышь компьютерная (16 шт.)
15. Robobuilder RQ – HUNO (Многофункциональный робот-андроид) (1 шт.)

16. Телевизор (1 шт.)
17. Специализированная мебель (1 шт.)
18. Матрешка – Z (набор – конструктор) (5 шт.)

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

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

1. Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1359091>

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

1. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189337> (дата обращения: 18.09.2022).

#### **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		
проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Тестирование
использовать типовые программные криптографические средства, в том числе электронную подпись;	Уметь использовать типовые программные криптографические средства, в том числе электронную подпись;	Тестирование
Знание		
типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Коллоквиум
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Коллоквиум
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Коллоквиум

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		
проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 02., ОК 03., ОК 05., ОК 08., ОК 10., ПК 3.2., ПК 3.5., ПК 3.1., ПК 3.3., ПК 3.4.	Вопросы на экзамен №40-50
использовать типовые программные криптографические средства, в том числе электронную подпись;	ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 02., ОК 03., ОК 05., ОК 08., ОК 10., ПК 3.2., ПК 3.5., ПК 3.1., ПК 3.3., ПК 3.4.	Вопросы на экзамен №30-39
Знание		
типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 02., ОК 03., ОК 05., ОК 08., ОК 10., ПК 3.2., ПК 3.5., ПК 3.1., ПК 3.3., ПК 3.4.	Вопросы на экзамен №20-29
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 02., ОК 03., ОК 05., ОК 08., ОК 10., ПК 3.2., ПК 3.5., ПК 3.1., ПК 3.3., ПК 3.4.	Вопросы на экзамен №10-19
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 02., ОК 03., ОК 05., ОК 08., ОК 10., ПК 3.2., ПК 3.5., ПК 3.1., ПК 3.3., ПК 3.4.	Вопросы на экзамен №1-9

Вопросы к практической подготовке указаны в методических указаниях к практической подготовке по дисциплине Техническая защита информации для

обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2021 Вопросы к практическому занятию указаны в методических указаниях к практическим занятиям по дисциплине Техническая защита информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2021 Вопросы к практическому занятию указаны в методических указаниях к практическим занятиям по дисциплине Техническая защита информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2021 Вопросы к практической подготовке указаны в методических указаниях к практической подготовке по дисциплине Техническая защита информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2021