Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.03.01 Техническая защита информации

2023

Программу составили:

1. Брехова Виктория Сергеевна

Дисциплина: МДК.03.01 Техническая защита информации

Данные не найдены (ФГОС)

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 №7 от 26.05.2023

Председатель МО Брехова Виктория Сергеевна

Рекомендовано к использованию в учебном процессе Методическим советом

Протокол №7 от 26.05.2023

Председатель МС Шляхова Наталья Ивановна

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 по специальности **Данные не найдены (ФГОС)** . Особое значение дисциплина имеет при формировании и развитии общих компетенций (ОК), профессиональных компетенций (ПК) и личностных результатов (ЛР):

1. ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
2. ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
3. ОК 09. Использовать информационные технологии в профессиональной деятельности.
4. ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
5. ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
6. ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
7. ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
8. ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
9. ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
10. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
11. ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

12. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.
13. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
14. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
15. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

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 07., ОК 10., ОК 09., ОК 08., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01., ПК 3.1., ПК 3.5., ПК 3.4., ПК 3.3., ПК 3.2.	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.; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;; основные понятия криптографии и типовых криптографических методов и средств защиты информации;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объём учебной дисциплины и виды учебной дисциплины

Вид учебной работы	**Объём в часах**
Лекционные занятия	76
Практические занятия	30
Практическая подготовка	48
Промежуточная аттестация	18
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	172
Форма(-ы) контроля: Дифференцированный зачет, Экзамен	

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

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 Лекции	Содержание учебного материала				Данные не найдены (к темам в разделе не привязано компетенций)
	1	**Лекционные занятия №1** Понятие информации и информационной безопасности	2	1	
	2	**Лекционные занятия №2** Понятие «угроза информации». Понятие «риска информационной безопасности»	2	1	
	3	**Лекционные занятия №3** Целостность, доступность и конфиденциальность информации	20	1	
	4	**Лекционные занятия №4** Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Часть 1	2	1	
	5	**Лекционные занятия №5** Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Часть 2	2	1	
	6	**Лекционные занятия №6** Цели и задачи защиты информации. Основные понятия в области защиты информации	2	1	
	7	**Лекционные занятия №7** Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации	2	1	
	8	**Лекционные занятия №8** Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации	2	1	
	9	**Лекционные занятия №9** Каналы и методы несанкционированного доступа к информации. Уязвимости	2	1	
	10	**Лекционные занятия №10** Анализ существующих методик определения требований к защите информации	2	1	
	11	**Лекционные занятия №11** Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации	2	1	
	12	**Лекционные занятия №12** Организационная структура системы защиты информации. Законодательные акты в области защиты информации	2	1	
	13	**Лекционные занятия №13** Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации	2	1	
	14	**Лекционные занятия №14** Основные механизмы защиты информации	2	1	
	15	**Лекционные занятия №15** Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Часть 1	2	1	
	16	**Лекционные занятия №16** Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Часть 2	2	1	
	17	**Лекционные занятия №17** Цели и задачи защиты информации от утечки информации по техническим каналам	2	1	
	18	**Лекционные занятия №18** Технические каналы утечки информации с СВТ и ИС.	2	1	
	19	**Лекционные занятия №19** Технические каналы утечки акустической (речевой) и видовой информации.	2	1	
	20	**Лекционные занятия №20** Технические средства защиты информации в акустических и вибрационных полях.	2	1	
	21	**Лекционные занятия №21** Характеристика каналов утечки информации от средств связи и ПЭМИН. Средства технической защиты для этих каналов. Часть 1.	2	1	
	22	**Лекционные занятия №22** Характеристика каналов утечки информации от средств связи и ПЭМИН. Средства технической защиты для этих каналов. Часть 2.	2	1	
	23	**Лекционные занятия №23** Технические средства защиты от наблюдения и линий связи от утечки конфиденциальной информации. Часть 1.	2	1	
	24	**Лекционные занятия №24** Технические средства защиты от наблюдения и линий связи от утечки конфиденциальной информации. Часть 2.	2	1	
	25	**Лекционные занятия №25** Лицензирование деятельности и сертификация средств защиты информации. Часть 1.	2	1	
	26	**Лекционные занятия №26** Лицензирование деятельности и сертификация средств защиты информации. Часть 2.	2	1	
	27	**Лекционные занятия №27** Способы и средства оценки эффективности инженерно-технической защиты информации. Часть 1.	2	1	
	28	**Лекционные занятия №28** Способы и средства оценки эффективности инженерно-технической защиты информации. Часть 2.	2	1	
	29	**Лекционные занятия №29** Система технической защиты информации. Часть 1	2	1	
	30	**Лекционные занятия №30** Система технической защиты информации. Часть 2	2	1	
	31	**Лекционные занятия №31** правовые основы защиты информации и информационной безопасности (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»)	2	1	
	32	**Лекционные занятия №32** Аппаратно-программные средства контроля доступа	2	1	
	33	**Лекционные занятия №33** Настройка аутентификации пользователей с помощью электронного замка	2	1	
	34	**Лекционные занятия №34** Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	1	
	35	**Лекционные занятия №35** Изменение политики контроля устройств	2	1	
	36	**Лекционные занятия №36** Настройка средств криптографической защиты сетевого трафика стандартного протокола IPSec	2	1	
	37	**Лекционные занятия №37** Управление средствами информационной безопасности сервера	2	1	
	38	**Лекционные занятия №38** Настройка средств защиты информации сервера	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
Тема 2 Практические занятия	Содержание учебного материала				Данные не найдены (к темам в разделе не привязано компетенций)
	1	**Практические занятия №1** Автономный регистратор сотовых разговоров SpRecord SpGate MR	2	2	
	2	**Практические занятия №2** Видеоглазок беспроводной Radio DVR	2	2	
	3	**Практические занятия №3** Видеоэндоскоп MaxiVideo MV208	2	2	
	4	**Практические занятия №4** Видеоэндоскоп MaxiVideo MV208	2	2	
	5	**Практические занятия №5** Видеорегистратор LawMate PV-550SE с камерой 618CA	2	2	
	6	**Практические занятия №6** Подавитель диктофонов Бубен-ультра	2	2	
	7	**Практические занятия №7** Беспроводная IP-камера для помещений Link 128 МИНИ	2	2	
	8	**Практические занятия №8** Адаптер записи с телефонной линии ICON TRX1	2	2	
	9	**Практические занятия №9** Угрозы безопасности информации на предприятии	2	2	
	10	**Практические занятия №10** Защита информации от традиционного шпионажа и диверсий	2	2	
	11	**Практические занятия №11** Защита информации от случайных угроз	2	2	
	12	**Практические занятия №12** Основные этапы проектирования системы защиты информации	2	2	
	13	**Практические занятия №13** Специфика персонала предприятия как объекта защиты	2	2	
	14	**Практические занятия №14** Разработка моделей объектов защиты	2	2	
	15	**Практические занятия №15** Электронно-цифровая подпись	2	2	
Тема 3 Практическая подготовка	Содержание учебного материала				Данные не найдены (к темам в разделе не привязано компетенций)
	1	**Практическая подготовка №1** Законодательство РФ в области информационной безопасности	2	2	
	2	**Практическая подготовка №2** Изучение положений о государственном лицензировании деятельности в области защиты информации	2	2	
	3	**Практическая подготовка №3** Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	2	2	
	4	**Практическая подготовка №4** Система сертификации средств криптографической защиты информации	2	2	
	5	**Практическая подготовка №5** Изучение положения о сертификации средств вычислительной техники и связи. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации	4	2	
	6	**Практическая подготовка №6** 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	
	7	**Практическая подготовка №7** Методы аутентификации и способы управления доступом	4	2	
	8	**Практическая подготовка №8** Защита информации от электромагнитных излучений и наводок	4	2	
	9	**Практическая подготовка №9** Исследование протокола IPSec	4	2	
	10	**Практическая подготовка №10** Изучение средств IP-безопасности, обеспечиваемых протоколом Ipsec	4	2	
	11	**Практическая подготовка №11** Организация комплексной системы защиты информации объекта	4	2	
	12	**Практическая подготовка №12** Защита информации правовыми и организационными методами	4	2	
	13	**Практическая подготовка №13** Моделирование технических каналов утечки информации. Анализ рисков безопасности информации.	4	2	
	14	**Практическая подготовка №14** 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	
	15	**Практическая подготовка №15** Настройка аутентификации пользователейс помощью электронного замка «СОБОЛЬ-PCI. Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	2	
Тема 4 Промежуточная аттестация	Содержание учебного материала				Данные не найдены (к темам в разделе не привязано компетенций)
	1	Данные не найдены (не указан вид занятия) Промежуточная аттестация	18	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
	Всего	**Тематическая и плановая расчасовка не совпадает (172 пл. ч. / 190тем. ч.)**		

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.)

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
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
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	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
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

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		
типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №20-29
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №1-9
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №10-19
Умение		
проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №40-50
использовать типовые программные криптографические средства, в том числе электронную подпись;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №30-39

Задания к практическим работам представлены в методических указаниях к практическим работам по дисциплине " Техническая защита информации" для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Ставрополь, 2023. Методические указания к практическим занятиям по дисциплине «Техническая защита информации» для

студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Ставрополь, 2023.