Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.02.02 Криптографические средства защиты информации

2023

Программу составили:

1. Брехова Виктория Сергеевна

Дисциплина: МДК.02.02 Криптографические 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 Информационных систем и программирования

Протокол №7 от 26.05.2023

Заведующий кафедрой Брехова Виктория Сергеевна

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.02.02 Криптографические средства защиты информации

(наименование дисциплины)

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина МДК.02.02 Криптографические 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) 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 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

12. ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
13. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
14. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
15. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
16. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

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 2.4., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.6., ПК 2.5.	Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;; Применять математический аппарат для выполнения криптографических преобразований;; Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	основные понятия криптографии и типовых криптографических методов и средств защиты информации;; особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;; Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объём учебной дисциплины и виды учебной дисциплины

Вид учебной работы	**Объём в часах**
Практическая подготовка	42
Лекционные занятия	64
Часы на контроль	18
Практические занятия	22
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	146
Форма(-ы) контроля: Экзамен	

2.2. Тематический план и содержание учебной дисциплины МДК.02.02 Криптографические 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 Лекции	Содержание учебного материала				Данные не найдены (к темам в разделе не привязано компетенций)
	1	**Лекционные занятия №1** Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.	2	1	
	2	**Лекционные занятия №2** Фильтрация на прикладном уровне	2	1	
	3	**Лекционные занятия №3** Фильтрация на сетевом уровне	2	1	
	4	**Лекционные занятия №4** Межсетевой экран	2	1	
	5	**Лекционные занятия №5** Методы криптографии	2	1	
	6	**Лекционные занятия №6** Защита от атак	2	1	
	7	**Лекционные занятия №7** Способы предотвращения удаленных атак на информационные системы	2	1	
	8	**Лекционные занятия №8** Сети и сетевой доступ	2	1	
	9	**Лекционные занятия №9** Сертификаты	2	1	
	10	**Лекционные занятия №10** Криптосистема	2	1	
	11	**Лекционные занятия №11** Криптосистема	2	1	
	12	**Лекционные занятия №12** Криптосистема	2	1	
	13	**Лекционные занятия №13** Инфраструктура открытых ключей (ИОК/PKI).	2	1	
	14	**Лекционные занятия №14** Методы и способы криптографической защиты информации.	2	1	
	15	**Лекционные занятия №15** Линейная сложность	2	1	
	16	**Лекционные занятия №16** Регистр сдвига с линейной обратной связью	2	1	
	17	**Лекционные занятия №17** Классификация поточных шифров	2	1	
	18	**Лекционные занятия №18** Практическая криптографическая стойкость	2	1	
	19	**Лекционные занятия №19** Криптографическая стойкость	2	1	
	20	**Лекционные занятия №20** Имитостойкость	2	1	
	21	**Лекционные занятия №21** Однонаправленные функции	2	1	
	22	**Лекционные занятия №22** Функции, используемые в криптографических системах	2	1	
	23	**Лекционные занятия №23** Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств	2	1	
	24	**Лекционные занятия №24** Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.	2	1	
	25	**Лекционные занятия №25** Термины и определения в области информационной безопасности	2	1	
	26	**Лекционные занятия №26** Основные понятия криптографии	2	1	
	27	**Лекционные занятия №27** Шифр Виженера. Шифр Фальконера. Шифр Кеплера и Галилея	2	1	
	28	**Лекционные занятия №28** Шифр Чейза. Тюремный шифр	2	1	
	29	**Лекционные занятия №29** Диск Энея. Квадрат Полибия	2	1	
	30	**Лекционные занятия №30** Шифр перестановки Шифр перестановки «сцитала»	20	1	
	31	**Лекционные занятия №31** Шифр Гая Юлия Цезаря	2	1	
	32	**Лекционные занятия №32** Криптографические средства с древнего времени	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** исследование функций гаммирования на языке программирования java	2	2	
	2	**Практические занятия №2** исследование работы простейших алгоритмов шифрования в среде программирования delphi	2	2	
	3	**Практические занятия №3** шифрование сообщений с помощью шифров замены криптографическими функциями excel	2	2	
	4	**Практические занятия №4** симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 2.	2	2	
	5	**Практические занятия №5** симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 1.	2	2	
	6	**Практические занятия №6** алгоритм блочного шифрования данных гост 28147-89	2	2	
	7	**Практические занятия №7** разработка и исследование криптоалгоритма на основе использования скремблера	2	2	
	8	**Практические занятия №8** исследование методов полиалфавитной подстановки	2	2	
	9	**Практические занятия №9** потоковое шифрование данных	2	2	
	10	**Практические занятия №10** Основы криптографической защиты информации	2	2	
	11	**Практические занятия №11** Введение в криптографическую защиту информации	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 Практическая подготовка	Содержание учебного материала				Данные не найдены (к темам в разделе не привязано компетенций)
	1	**Практическая подготовка №1** Защита программ от несанкционированного использования с помощью USB-ключей и средств разработчика	2	2	
	2	**Практическая подготовка №2** Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя	2	2	
	3	**Практическая подготовка №3** Удостоверяющие центры на основе службы сертификации в операционной системе Windows 2003 Server	2	2	
	4	**Практическая подготовка №4** защита информации с помощью пароля	2	2	
	5	**Практическая подготовка №5** аутентификация пользователей web-систем средствами технологии php	2	2	
	6	**Практическая подготовка №6** асимметричная криптография и электронная цифровая подпись на примере системы gnupg	2	2	
	7	**Практическая подготовка №7** средства обеспечения безопасности ос семейства windows	2	2	
	8	**Практическая подготовка №8** исследование алгоритма шифрования rsa в ms	2	2	
	9	**Практическая подготовка №9** исследование блочного алгоритма шифрования des	2	2	
	10	**Практическая подготовка №10** программная реализация шифров на языке программирования java	2	2	
	11	**Практическая подготовка №11** исследование возможностей поточного шифрования на языке программирования java	2	2	
	12	**Практическая подготовка №12** исследование возможностей блочного шифрования на языке программирования java	4	2	
	13	**Практическая подготовка №13** создание криптографических сообщений с использованием интерфейса microsoft cryptoapi и цифровых сертификатов x.509	4	2	
	14	**Практическая подготовка №14** симметричное шифрование данных с использованием криптографических интерфейсов microsoft cryptoapi и cryptography api: next generation	4	2	
	15	**Практическая подготовка №15** Исследование гаммирования при шифровании	4	2	
	16	**Практическая подготовка №16** шифрование методом перестановки	4	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	
		Всего	Тематическая и плановая расчасовка не совпадает (146 пл. ч. / 164тем. 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
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.)

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
Лаборатория компьютерной графики:

1. Стол компьютерный (9 шт.)
2. стул (9 шт.)
3. доска (1 шт.)
4. Стенд средства цифровых коммуникационных технологий (3 шт.)
5. плакаты по стратегии продвижения бренда в сети Интернет (3 шт.)
6. плакаты по маркетингу в социальных сетях (2 шт.)
7. плакаты по разработке и размещению рекламного контента (3 шт.)
8. Рабочее место преподавателя, персональный компьютер с подключением к сети «Интернет» (1 шт.)
9. Системный блок (9 шт.)
10. Монитор (9 шт.)
11. Клавиатура (9 шт.)
12. Мультимедийное оборудование (видеопроектор, экран, колонки) (1 шт.)
13. Мышь компьютерная (9 шт.)

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

1. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
2. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов. — Москва : КноРус, 2019. Режим доступа

https://www.book.ru/book/924214

3.2.2. Дополнительные источники

1. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2019. - 432 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-627-0 - Режим доступа: http://znanium.com/catalog/product/516806
2. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. — М. : ИД «ФОРУМ» : ИНФРА-М, 2019. — 542 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/999615

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		
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Коллоквиум
особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	Знать особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	Коллоквиум
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
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
Применять математический аппарат для выполнения криптографических преобразований;	Уметь применять математический аппарат для выполнения криптографических преобразований;	Тестирование
Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Уметь осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Тестирование

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №1-7
особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №8-15
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 №16-24
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 №25-33
Применять математический аппарат для выполнения криптографических преобразований;	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №34-40
Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Данные не найдены (не указаны компетенции)	Вопросы на экзамен №41-50

Вопросы к практической подготовке указаны в методических указаниях к практической подготовке по дисциплине Криптографические средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2023 Вопросы к практическому занятию указаны в методических указаниях к практическим занятиям по дисциплине Криптографические средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2023