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

2026

Программу составили:

1. Боброва Анастасия Николаевна

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 Информационной безопасности

Протокол №7 от 23.05.2026

Заведующий кафедрой Панова Светлана Александровна

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):

1. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
2. ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
3. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках
4. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
5. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа
6. ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
7. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
8. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
9. 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
10. 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	Умения	Знания
ОК 02., ОК 05., ОК 09., ОК 01., 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	Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.; особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения 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	46
Практические занятия	38
Часы на контроль	18
Практическая подготовка	42
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	144
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, формированию которых способствует элемент программы
Тема 1 Промежуточная аттестация	Содержание учебного материала				ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Часы на контроль** Промежуточная аттестация	18	2	
Тема 2 Практическая подготовка	Содержание учебного материала				ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.1., ПК 2.3., ПК 2.4., ПК 2.2., ПК 2.6.
	1	**Практическая подготовка №1** шифрование методом перестановки	4	2	
	2	**Практическая подготовка №2** Исследование гаммирования при шифровании	4	2	
	3	**Практическая подготовка №3** симметричное шифрование данных с использованием криптографических интерфейсов microsoft cryptoapi и cryptography api: next generation	4	2	
	4	**Практическая подготовка №4** создание криптографических сообщений с использованием интерфейса microsoft cryptoapi и цифровых сертификатов x.509	4	2	
	5	**Практическая подготовка №5** исследование возможностей блочного шифрования на языке программирования java	4	2	
	6	**Практическая подготовка №6** исследование возможностей поточного шифрования на языке программирования java	2	2	
	7	**Практическая подготовка №7** программная реализация шифров на языке программирования java	2	2	
	8	**Практическая подготовка №8** исследование блочного алгоритма шифрования des	2	2	
	9	**Практическая подготовка №9** исследование алгоритма шифрования rsa в ms	2	2	
	10	**Практическая подготовка №10** средства обеспечения безопасности ос семейства windows	2	2	
	11	**Практическая подготовка №11** асимметричная криптография и электронная цифровая подпись на примере системы gnupg	2	2	
	12	**Практическая подготовка №12** аутентификация пользователей web-систем средствами технологии php	2	2	
	13	**Практическая подготовка №13** защита информации с помощью пароля	2	2	
	14	**Практическая подготовка №14** Удостоверяющие центры на основе службы сертификации в операционной системе Windows 2003 Server	2	2	
	15	**Практическая подготовка №15** Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя	2	2	
	16	**Практическая подготовка №16** Защита программ от несанкционированного использования с помощью USB-ключей и средств разработчика	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 3 Практические занятия	Содержание учебного материала				ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Практические занятия №1** Введение в криптографическую защиту информации	2	2	
	2	**Практические занятия №2** Основы криптографической защиты информации	2	2	
	3	**Практические занятия №3** потоковое шифрование данных	2	2	
	4	**Практические занятия №4** исследование методов полиалфавитной подстановки	2	2	
	5	**Практические занятия №5** разработка и исследование криптоалгоритма на основе использования скремблера	4	2	
	6	**Практические занятия №6** алгоритм блочного шифрования данных гост 28147-89	4	2	
	7	**Практические занятия №7** симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 1.	4	2	
	8	**Практические занятия №8** симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 2.	4	2	
	9	**Практические занятия №9** шифрование сообщений с помощью шифров замены криптографическими функциями excel	4	2	
	10	**Практические занятия №10** исследование работы простейших алгоритмов шифрования в среде программирования delphi	6	2	
	11	**Практические занятия №11** исследование функций гаммирования на языке программирования java	4	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 Лекции	Содержание учебного материала				ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.3., ПК 2.4., ПК 2.1., ПК 2.2., ПК 2.6., ПК 2.5.
	1	**Лекционные занятия №1** Криптографические средства с древнего времени	2	1	
	2	**Лекционные занятия №2** Шифр Гая Юлия Цезаря	2	1	
	3	**Лекционные занятия №3** Шифр перестановки Шифр перестановки «сцитала»	2	1	
	4	**Лекционные занятия №4** Диск Энея. Квадрат Полибия	1	1	
	5	**Лекционные занятия №5** Шифр Чейза. Тюремный шифр	1	1	
	6	**Лекционные занятия №6** Шифр Виженера. Шифр Фальконера. Шифр Кеплера и Галилея	2	1	
	7	**Лекционные занятия №7** Основные понятия криптографии	2	1	
	8	**Лекционные занятия №8** Термины и определения в области информационной безопасности	2	1	
	9	**Лекционные занятия №9** Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.	2	1	
	10	**Лекционные занятия №10** Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств	2	1	
	11	**Лекционные занятия №11** Функции, используемые в криптографических системах	2	1	
	12	**Лекционные занятия №12** Однонаправленные функции	2	1	
	13	**Лекционные занятия №13** Имитостойкость	2	1	
	14	**Лекционные занятия №14** Криптографическая стойкость	1	1	
	15	**Лекционные занятия №15** Практическая криптографическая стойкость	1	1	
	16	**Лекционные занятия №16** Классификация поточных шифров	1	1	
	17	**Лекционные занятия №17** Регистр сдвига с линейной обратной связью	1	1	
	18	**Лекционные занятия №18** Линейная сложность	1	1	
	19	**Лекционные занятия №19** Методы и способы криптографической защиты информации.	1	1	
	20	**Лекционные занятия №20** Инфраструктура открытых ключей (ИОК/PKI).	1	1	
	21	**Лекционные занятия №21** Криптосистема	1	1	
	22	**Лекционные занятия №22** Сертификаты	1	1	
	23	**Лекционные занятия №23** Сети и сетевой доступ	1	1	
	24	**Лекционные занятия №24** Способы предотвращения удаленных атак на информационные системы	2	1	
	25	**Лекционные занятия №25** Защита от атак	2	1	
	26	**Лекционные занятия №26** Методы криптографии	2	1	
	27	**Лекционные занятия №27** Межсетевой экран	2	1	
	28	**Лекционные занятия №28** Фильтрация на сетевом уровне	2	1	
	29	**Лекционные занятия №29** Фильтрация на прикладном уровне	1	1	
	30	**Лекционные занятия №30** Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.	1	1	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
	Всего	144		

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 УЧЕБНОЙДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие помещения:

Лаборатория информационных ресурсов.
Лаборатория информационных технологий, сетей и систем передачи информации, программирования и баз данных
Полигон вычислительной техники:

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. Мультимедийное оборудование (видеопроектор, экран, колонки) (1 шт.)
9. Автоматизированное рабочее место преподавателя, персональный компьютер с подключением к сети «Интернет» (1 шт.)
10. Многофункциональное устройство (1 шт.)

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

1. Лапина, Е. В. Средства криптографической защиты информации : учебное пособие / Е. В. Лапина, В. А. Морозов. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2023. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/400478

3.2.2. Дополнительные источники

1. Введение в теоретико-числовые методы криптографии : учебное пособие для СПО / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 4-е изд., стер. — Санкт-Петербург : Лань, 2026. — 396 с. — ISBN 978-5-507-51289-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/509879

3.2.3. Интернет-ресурсы

1.

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
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
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
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
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Знать основные понятия криптографии и типовых криптографических методов и 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 01., ОК 02., ОК 05., ОК 09., ПК 2.2., ПК 2.6.	Вопросы на экзамен №25-33
Применять математический аппарат для выполнения криптографических преобразований;	ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.3.	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	ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.6., ПК 2.2., ПК 2.3.	Вопросы на экзамен №41-50
Знание		
Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	ПК 2.2., ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.3., ПК 2.6.	Вопросы на экзамен №16-24
особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.5., ПК 2.2.	Вопросы на экзамен №8-15

Результаты обучения	Коды компетенций	Фонды оценочных средств
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	ОК 01., ОК 02., ОК 05., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	Вопросы на экзамен №1-7

Вопросы к практическому занятию указаны в методических указаниях к практическим занятиямпо дисциплине Криптографические средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2026 Вопросы к практической подготовке указаны в методических указаниях к практической подготовкепо дисциплине Криптографические средства защиты информации для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2026