Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

2025

Программу составили:

1. Кононова Наталия Владимировна

Дисциплина: ОП.01 Основы информационной безопасности

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.01 Основы информационной безопасности

(наименование дисциплины)

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.01 Основы информационной безопасности 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 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
2. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках
3. ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
4. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	Умения	Знания
ОК 06., ОК 09., ОК 03., ПК 2.4.	Классифицировать основные угрозы безопасности информации;; Классифицировать защищаемую информацию по видам тайны и степеням секретности	Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;; Источники угроз безопасности информации и меры по их предотвращению;; Современные средства и способы обеспечения информационной безопасности;; Основные методики анализа угроз и рисков информационной безопасности;; Виды, источники и носители защищаемой информации;; Место информационной безопасности в системе национальной безопасности страны;; Сущность и понятие информационной безопасности, характеристику ее составляющих;; Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объём учебной дисциплины и виды учебной дисциплины

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

2.2. Тематический план и содержание учебной дисциплины ОП.01 Основы информационной безопасности

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 Практические занятия	Содержание учебного материала				ОК 03., ОК 06., ОК 09., ПК 2.4.
	1	**Практические занятия №1** Шифрование информации методом простой подстановки.	2	2	
	2	**Практические занятия №2** Шифрование информации методом усложненной перестановки по таблице .	2	2	
	3	**Практические занятия №3** Шифрование информации методом сложной подстановки.	2	2	
	4	**Практические занятия №4** Шифрование информации методом «Линейного регистра с обратными связями»	2	2	
	5	**Практические занятия №5** Изучение CRC	2	2	
	6	**Практические занятия №6** Изучение алгоритма шифрования RSA	2	2	
	7	**Практические занятия №7** Количественная оценка стойкости парольной защиты Часть 1	2	2	
	8	**Практические занятия №8** Количественная оценка стойкости парольной защиты Часть 2	2	2	
	9	**Практические занятия №9** Шифрование информации методом «Решетки Кардано»	2	2	
Тема 2 Лекции	Содержание учебного материала				ОК 03., ОК 06., ОК 09., ПК 2.4.
	1	**Лекционные занятия №1** Режимы шифрования	2	1	
	2	**Лекционные занятия №2** Уязвимость информации, обрабатываемой в автоматизированных системах. Часть 2	2	1	
	3	**Лекционные занятия №3** Отечественный стандарт на шифрование данных Часть 1	2	1	
	4	**Лекционные занятия №4** Отечественный стандарт на шифрование данных Часть 2	2	1	
	5	**Лекционные занятия №5** Криптографические модели. Часть 1	2	1	
	6	**Лекционные занятия №6** Криптографические модели Часть 2	2	1	
	7	**Лекционные занятия №7** Алгоритмы аутентификации пользователей. Часть 1	2	1	
	8	**Лекционные занятия №8** Алгоритмы аутентификации пользователей. Часть 2	2	1	
	9	**Лекционные занятия №9** Электронная цифровая подпись Часть 1	2	1	
	10	**Лекционные занятия №10** Электронная цифровая подпись Часть 2	2	1	
	11	**Лекционные занятия №11** Защита от удаленных атак через сеть Internet Часть 1	2	1	
	12	**Лекционные занятия №12** Защита от удаленных атак через сеть Internet Часть 2	2	1	
	13	**Лекционные занятия №13** Аппаратно-программные средства защиты компьютерной информации. Часть 1	2	1	
	14	**Лекционные занятия №14** Аппаратно-программные средства защиты компьютерной информации. Часть 2	2	1	
	15	**Лекционные занятия №15** Уязвимость информации, обрабатываемой в автоматизированных системах. Часть 1	2	1	
Всего			48		

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. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2025. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169040

3.2.2. Дополнительные источники

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. - Москва ; Вологда : Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902587

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		
Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	Знать жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	Коллоквиум
Источники угроз безопасности информации и меры по их предотвращению;	Знать источники угроз безопасности информации и меры по их предотвращению;	Коллоквиум
Современные средства и способы обеспечения информационной безопасности;	Знать современные средства и способы обеспечения информационной безопасности;	Коллоквиум
Основные методики анализа угроз и рисков информационной безопасности;	Знать основные методики анализа угроз и рисков информационной безопасности;	Коллоквиум
Виды, источники и носители защищаемой информации;	Знать виды, источники и носители защищаемой информации;	Коллоквиум
Место информационной безопасности в системе национальной безопасности страны;	Знать место информационной безопасности в системе национальной безопасности страны;	Коллоквиум
Сущность и понятие информационной безопасности, характеристику ее составляющих;	Знать сущность и понятие информационной безопасности, характеристику ее составляющих;	Коллоквиум
Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;	Знать факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;	Коллоквиум
Умение		
Классифицировать основные угрозы безопасности информации;	Уметь классифицировать основные угрозы безопасности информации;	Тестирование
Классифицировать защищаемую информацию по видам тайны и степеням секретности	Уметь классифицировать защищаемую информацию по видам тайны и степеням секретности	Тестирование

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		
Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №11-15
Источники угроз безопасности информации и меры по их предотвращению;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №1-5
Современные средства и способы обеспечения информационной безопасности;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №16-20
Основные методики анализа угроз и рисков информационной безопасности;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №21-25
Виды, источники и носители защищаемой информации;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №15-20
Место информационной безопасности в системе национальной безопасности страны;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №35-40
Сущность и понятие информационной безопасности, характеристику ее составляющих;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №25-30
Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №6-10

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		
Классифицировать основные угрозы безопасности информации;	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №31-40
Классифицировать защищаемую информацию по видам тайны и степеням секретности	ПК 2.4., ОК 09., ОК 06., ОК 03.	Вопросы к дифференцированному зачёту №41- 50

Вопросы к практическому занятию указаны в методических указаниях к практическим занятиямпо дисциплине Основы информационной безопасности для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025