

Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

2023

Программу составили:

1. Хвалько Леонид Александрович

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 на заседании методического объединения Укрупненных групп специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность»

Протокол №6 от 26.05.2023

Председатель МО Хвалько Леонид Александрович

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

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 по специальности «10.02.05 Обеспечение информационной безопасности автоматизированных систем». Особое значение дисциплина имеет при формировании и развитии общих компетенций (ОК), профессиональных компетенций (ПК) и личностных результатов (ЛР):

1. ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
2. ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
3. ОК 09. Использовать информационные технологии в профессиональной деятельности.
4. ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
5. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.
6. ЛР 1 Осознающий себя гражданином и защитником великой страны
7. ЛР 3 Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
8. ЛР 4 Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа»
9. ЛР 7 Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
10. ЛР 16 Выработавший умения и навыки трудовой деятельности, проявляющий основы трудовой культуры по отношению к коллегам, контрагентам и клиентам Компании

11. ЛР 22 Выработавший принципы экологически целесообразного поведения, бережного отношения к своей жизни, жизни других людей, природы, планеты в целом

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 10., ОК 06., ОК 09., ОК 03., ПК 2.4., ЛР 1, ЛР 3, ЛР 4, ЛР 7, ЛР 16, ЛР 22	<p>Классифицировать защищаемую информацию по видам тайны и степеням секретности;</p> <p>Классифицировать основные угрозы безопасности информации;</p>	<p>Источники угроз безопасности информации и меры по их предотвращению;;</p> <p>Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;;</p> <p>Современные средства и способы обеспечения информационной безопасности;;</p> <p>Основные методики анализа угроз и рисков информационной безопасности;;</p> <p>Виды, источники и носители защищаемой информации;;</p> <p>Место информационной безопасности в системе национальной безопасности страны;;</p> <p>Сущность и понятие информационной безопасности, характеристику ее составляющих;;</p> <p>Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</p>

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной дисциплины

Вид учебной работы	Объем в часах
Лекционные занятия	30
Практические занятия	18
Общий объем 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 и личностных результатов, формированию которых способствует элемент программы	
Тема 1 Лекции	Содержание учебного материала			ЛР 1, ЛР 3, ЛР 4, ЛР 7, ЛР 16, ЛР 22, ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	
	1	Лекционные занятия №1 Режимы шифрования	2		1
	2	Лекционные занятия №2 Уязвимость информации, обрабатываемой в автоматизированных системах. Часть 1	2		1
	3	Лекционные занятия №3 Уязвимость информации, обрабатываемой в автоматизированных системах. Часть 2	2		1
	4	Лекционные занятия №4 Отечественный стандарт на шифрование данных Часть 1	2		1
	5	Лекционные занятия №5 Отечественный стандарт на шифрование данных Часть 2	2		1
	6	Лекционные занятия №6 Криптографические модели. Часть 1	2		1
	7	Лекционные занятия №7 Криптографические модели Часть 2	2		1
	8	Лекционные занятия №8 Алгоритмы аутентификации пользователей. Часть 1	2		1
	9	Лекционные занятия №9 Алгоритмы аутентификации пользователей. Часть 2	2		1
	10	Лекционные занятия №10 Электронная цифровая подпись Часть 1	2		1
	11	Лекционные занятия №11 Электронная цифровая подпись Часть 2	2		1
	12	Лекционные занятия №12 Защита от удаленных атак через сеть Internet Часть 1	2		1
	13	Лекционные занятия №13 Защита от удаленных атак через сеть Internet Часть 2	2		1
	14	Лекционные занятия №14 Аппаратно-программные средства защиты компьютерной информации. Часть 1	2		1
15	Лекционные занятия №15 Аппаратно-программные средства защиты компьютерной информации. Часть 2	2	1		
Тема 2 Практические занятия	Содержание учебного материала			ЛР 1, ЛР 3, ЛР 4, ЛР 7, ЛР 16, ЛР 22, ОК 10., ОК 06., ОК 09., ОК 03., 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 «Решетки Кардано»	2		2
	4	Практические занятия №4 Шифрование информации методом сложной подстановки.	2		2
	5	Практические занятия №5 Шифрование информации методом «Линейного регистра с обратными связями»	2		2
	6	Практические занятия №6 Изучение CRC	2		2
	7	Практические занятия №7 Изучение алгоритма шифрования RSA	2		2
	8	Практические занятия №8 Количественная оценка стойкости парольной защиты Часть 1	2		2
9	Практические занятия №9 Количественная оценка стойкости парольной защиты Часть 2	2	2		
		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:

Кабинет информационных систем в профессиональной деятельности
Кабинет информатики и математики
Кабинет компьютерного дизайна
Лаборатория информационных технологий в профессиональной деятельности
Лаборатория информационных технологий
Лаборатория компьютерного дизайна
Лаборатория разработки веб-приложений
Студия инженерной и компьютерной графики
Студия разработки дизайна веб-приложений
Кабинет для самостоятельной работы:

1. Системный блок (9 шт.)
2. Монитор (9 шт.)
3. Мышь компьютерная (9 шт.)
4. Стенды (1 шт.)
5. Клавиатура (9 шт.)
6. Плакаты (34 шт.)

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.)

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:

1. Монитор (9 шт.)
2. Мышь компьютерная (9 шт.)
3. Системный блок (9 шт.)
4. Стенды (3 шт.)
5. Клавиатура (9 шт.)

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

1. А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин Основы информационной безопасности: учеб. для студ ИЦ «Академия», 2019,
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие
3. <http://znanium.com/catalog/product/549989>
4. НИЦ ИНФРА-М, 2016,

3.2.2. Дополнительные источники

1. Т.Л. Партыка, И.И. Попов Информационная безопасность: Учебное пособие М. : ФОРУМ : ИНФРА-М, 2018, <http://znanium.com/catalog/product/915902>

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		
Источники угроз безопасности информации и меры по их предотвращению;	Знать источники угроз безопасности информации и меры по их предотвращению;	Коллоквиум
Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	Знать жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	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 защищаемую информацию по видам тайны и степеням секретности	Уметь классифицировать защищаемую информацию по видам тайны и степеням секретности	Тестирование
Классифицировать основные угрозы безопасности информации;	Уметь классифицировать основные угрозы безопасности информации;	Тестирование

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		
Источники угроз безопасности информации и меры по их предотвращению;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №1-5
Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №11-15
Современные средства и способы обеспечения информационной безопасности;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №16-20
Основные методики анализа угроз и рисков информационной безопасности;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №21-25
Виды, источники и носители защищаемой информации;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №15-20
Место информационной безопасности в системе национальной безопасности страны;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №35-40

Результаты обучения	Коды компетенций	Фонды оценочных средств
Сущность и понятие информационной безопасности, характеристику ее составляющих;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №25-30
Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №6-10
Умение		
Классифицировать защищаемую информацию по видам тайны и степеням секретности	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №41- 50
Классифицировать основные угрозы безопасности информации;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ЛР 4, ЛР 7, ОК 03., ОК 06., ОК 09., ОК 10., ПК 2.4.	Вопросы к дифференцированному зачёту №31-40

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