

Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

2024

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 и рекомендовано на заседании кафедры Информационной безопасности

Протокол №9 от 27.05.2024

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 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
2. 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;
3. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.
4. 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;
5. 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 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	<p>Применять полученные знания к различным предметным областям;;</p> <p>Ориентироваться в особенностях применяемых средств защиты компьютерной информации;;</p> <p>Применять средства антивирусной защиты.</p>	<p>Криптографические методы защиты компьютерной информации;</p> <p>Пути практической реализации концепции комплексной защиты информации.;</p> <p>Историю, состояние и перспективы развития методов и средств защиты информации;;</p> <p>Основные способы защиты информации в компьютерных сетях;;</p> <p>Источники угроз безопасности компьютерной информации;</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, формированию которых способствует элемент программы	
Тема 1 Практические занятия	Содержание учебного материала			ОК 10., ОК 09., ОК 06., ОК 03., ПК 2.4.	
	1	Практические занятия №1 Количественная оценка стойкости парольной защиты Часть 2	2		2
	2	Практические занятия №2 Количественная оценка стойкости парольной защиты Часть 1	2		2
	3	Практические занятия №3 Изучение алгоритма шифрования RSA	2		2
	4	Практические занятия №4 Изучение CRC	2		2
	5	Практические занятия №5 Шифрование информации методом «Линейного регистра с обратными связями»	2		2
	6	Практические занятия №6 Шифрование информации методом сложной подстановки.	2		2
	7	Практические занятия №7 Шифрование информации методом «Решетки Кардано»	2		2
	8	Практические занятия №8 Шифрование информации методом усложненной перестановки по таблице .	2		2
	9	Практические занятия №9 Шифрование информации методом простой подстановки.	2		2
Тема 2 Лекции	Содержание учебного материала			ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	
	1	Лекционные занятия №1 Аппаратно-программные средства защиты компьютерной информации. Часть 2	2		1
	2	Лекционные занятия №2 Аппаратно-программные средства защиты компьютерной информации. Часть 1	2		1
	3	Лекционные занятия №3 Защита от удаленных атак через сеть Internet Часть 2	2		1
	4	Лекционные занятия №4 Защита от удаленных атак через сеть Internet Часть 1	2		1
	5	Лекционные занятия №5 Электронная цифровая подпись Часть 2	2		1
	6	Лекционные занятия №6 Электронная цифровая подпись Часть 1	2		1
	7	Лекционные занятия №7 Алгоритмы аутентификации пользователей. Часть 2	2		1
	8	Лекционные занятия №8 Алгоритмы аутентификации пользователей. Часть 1	2		1
	9	Лекционные занятия №9 Криптографические модели Часть 2	2		1
	10	Лекционные занятия №10 Криптографические модели. Часть 1	2		1
	11	Лекционные занятия №11 Отечественный стандарт на шифрование данных Часть 2	2		1
	12	Лекционные занятия №12 Отечественный стандарт на шифрование данных Часть 1	2		1
	13	Лекционные занятия №13 Уязвимость информации, обрабатываемой в автоматизированных системах. Часть 2	2		1
	14	Лекционные занятия №14 Уязвимость информации, обрабатываемой в автоматизированных системах. Часть 1	2		1
15	Лекционные занятия №15 Режимы шифрования	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:

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
Лаборатория фотостудии
Лаборатория цифровых коммуникационных технологий:

1. Стол компьютерный (9 шт.)
2. стул (9 шт.)
3. доска (1 шт.)
4. Стенды по интернет-маркетингу (2 шт.)
5. плакаты по контент-маркетингу (3 шт.)
6. плакаты по интернет-маркетингу (6 шт.)
7. плакаты по PR-коммуникации в digital (5 шт.)
8. плакаты по исследованию рекламных и коммуникационных кампаний (5 шт.)
9. Рабочее место преподавателя, персональный компьютер с подключением к сети «Интернет» (1 шт.)
10. Системный блок (9 шт.)
11. Монитор (9 шт.)
12. Клавиатура (9 шт.)
13. Мышь компьютерная (9 шт.)
14. Мультимедийное оборудование (видеопроектор, экран, колонки) (1 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

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. 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 НИЦ ИНФРА-М, 2019, <http://znanium.com/catalog/product/549989>

3.2.2. Дополнительные источники

1. Т.Л. Партыка, И.И. Попов Информационная безопасность: Учебное пособие М. : ФОРУМ : ИНФРА-М, 2019, <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		
Криптографические методы защиты компьютерной информации	Знать криптографические методы защиты компьютерной информации	Коллоквиум
Пути практической реализации концепции комплексной защиты информации.	Знать пути практической реализации концепции комплексной защиты информации.	Коллоквиум
Историю, состояние и перспективы развития методов и средств защиты информации;	Знать историю, состояние и перспективы развития методов и средств защиты информации;	Коллоквиум
Основные способы защиты информации в компьютерных сетях;	Знать основные способы защиты информации в компьютерных сетях;	Коллоквиум
Источники угроз безопасности компьютерной информации;	Знать источники угроз безопасности компьютерной информации;	Коллоквиум
Умение		
Применять полученные знания к различным предметным областям;	Уметь применять полученные знания к различным предметным областям;	Тестирование
Ориентироваться в особенностях применяемых средств защиты компьютерной информации;	Уметь ориентироваться в особенностях применяемых средств защиты компьютерной информации;	Тестирование
Применять средства антивирусной защиты.	Уметь применять средства антивирусной защиты.	Тестирование

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		
Криптографические методы защиты компьютерной информации	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №16-20
Пути практической реализации концепции комплексной защиты информации.	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №21-25
Историю, состояние и перспективы развития методов и средств защиты информации;	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №1-5
Основные способы защиты информации в компьютерных сетях;	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №6-10
Источники угроз безопасности компьютерной информации;	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №11-15
Умение		
Применять полученные знания к различным предметным областям;	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №26-30
Ориентироваться в особенностях применяемых средств защиты компьютерной информации;	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №31-40
Применять средства антивирусной защиты.	ОК 10., ОК 06., ОК 09., ОК 03., ПК 2.4.	Вопросы к дифференцированному зачёту №41-50

Вопросы к практическому занятию указаны в методических указаниях к практическим занятиям по дисциплине Основы информационной безопасности для обучающихся специальности "Обеспечение информационной безопасности

автоматизированных систем". Ставрополь, 2024