

Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В.11 Управление информационной безопасностью

2024

Программу составили:

1. Сивирский Сергей Михайлович

Дисциплина: ОП.В.11 Управление информационной безопасностью

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 №9 от 27.05.2024

Заведующий кафедрой Цыбань Илья Константинович

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В.11 Управление информационной безопасностью

(наименование дисциплины)

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.В.11 Управление информационной безопасностью 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. ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
2. ЛР 1 Осознающий себя гражданином и защитником великой страны
3. 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
4. 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»
5. ЛР 7 Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
6. ЛР 16 Выработавший умения и навыки трудовой деятельности, проявляющий основы трудовой культуры по отношению к коллегам, контрагентам и клиентам Компании
7. 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 | Умения | Знания |
|---|---|--|
| ПК 2.1., ЛР 1, ЛР 3, ЛР 4, ЛР 7, ЛР 16, ЛР 22 | <p>анализировать и оценивать угрозы информационной безопасности объекта;</p> <p>применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях;</p> <p>применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации;</p> <p>выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования;</p> <p>анализировать информационную безопасность многопользовательских систем;</p> <p>использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации</p> | <p>организационные, технические программные методы защиты информации в информационных системах;</p> <p>методы идентификации пользователей;</p> <p>архитектуру основных стандартов защиты информации;</p> <p>организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности;</p> <p>правовые основы защиты компьютерной информации;</p> <p>основные методы противодействия «внутренним» угрозам информационной безопасности организации</p> |

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной дисциплины

| Вид учебной работы | Объем в часах |
|---|----------------------|
| Лекционные занятия | 16 |
| Лабораторные занятия | 6 |
| Практическая подготовка | 20 |
| Практические занятия | 6 |
| 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.В.11 Управление информационной безопасностью

| 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 Лабораторные работы | Содержание учебного материала | | | ПК 2.1., ЛР 1, ЛР 3, ЛР 7, ЛР 16, ЛР 22 |
| | 1 Лабораторные занятия №1 Реализация дискреционной модели политики безопасности Часть 2 | 2 | 2 | |
| | 2 Лабораторные занятия №2 Реализация дискреционной модели политики безопасности Часть 1 | 2 | 2 | |
| | 3 Лабораторные занятия №3 Аудит методов и средств обеспечения информационной безопасности организации | 2 | 2 | |
| Тема 2 Лекции | Содержание учебного материала | | | ЛР 1, ПК 2.1., ЛР 3, ЛР 7, ЛР 16, ЛР 22 |
| | 1 Лекционные занятия №1 Аудит методов и средств обеспечения информационной безопасности организации | 2 | 1 | |
| | 2 Лекционные занятия №2 Планирование деятельности по обработке рисков обеспечения информационной безопасности организации | 2 | 1 | |
| | 3 Лекционные занятия №3 Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации | 2 | 1 | |
| | 4 Лекционные занятия №4 Социальные аспекты системы управления информационной безопасностью бизнеса | 2 | 1 | |
| | 5 Лекционные занятия №5 Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса | 2 | 1 | |
| | 6 Лекционные занятия №6 Система управления информационной безопасностью бизнеса | 2 | 1 | |
| | 7 Лекционные занятия №7 Обеспечение информационной безопасности бизнеса | 2 | 1 | |
| | 8 Лекционные занятия №8 Основы построения систем обеспечения информационной безопасности на предприятии. | 2 | 1 | |
| Тема 3 Практические занятия | Содержание учебного материала | | | ЛР 1, ПК 2.1., ЛР 3, ЛР 7, ЛР 16, ЛР 22 |
| | 1 Практические занятия №1 Безопасность персонала | 2 | 2 | |
| | 2 Практические занятия №2 Классификация ресурсов и их контроль | 2 | 2 | |
| | 3 Практические занятия №3 Организация защиты | 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 4 | Содержание учебного материала | | | ЛР 1, ПК 2.1., ЛР 3, ЛР 7, ЛР 16, ЛР 22 |
| Практическая подготовка | 1 Практическая подготовка №1 Разработка и сопровождение информационных систем. Планирование бесперебойной работы организации | 2 | 2 | |
| | 2 Практическая подготовка №2 Управление доступом к системам | 2 | 2 | |
| | 3 Практическая подготовка №3 Администрирование компьютерных систем и вычислительных сетей | 2 | 2 | |
| | 4 Практическая подготовка №4 Физическая безопасность и безопасность окружающей среды | 2 | 2 | |
| | 5 Практическая подготовка №5 Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра Часть 2 | 2 | 2 | |
| | 6 Практическая подготовка №6 Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра Часть 1 | 2 | 2 | |
| | 7 Практическая подготовка №7 Ассиметричные алгоритмы шифрования данных | 4 | 2 | |
| | 8 Практическая подготовка №8 Количественная оценка стойкости парольной защиты Часть 2 | 2 | 2 | |
| | 9 Практическая подготовка №9 Количественная оценка стойкости парольной защиты Часть 1 | 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
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.)

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. Николаев, Н.С., Управление информационной безопасностью : учебник / Н.С. Николаев. — Москва : КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL:<https://book.ru/book/939841> (дата обращения: 15.10.2022). — Текст : электронный.

3.2.2. Дополнительные источники

1. Фисун, В.В., Искусственный интеллект управления информационной безопасностью объектов критической информационной инфраструктуры : монография / В.В. Фисун. — Москва : Русайнс, 2020. — 357 с. — ISBN 978-5-4365-6315-2. — URL:<https://book.ru/book/939472> (дата обращения: 15.10.2022). — Текст : электронный.

3.2.3. Интернет-ресурсы

1. Электронно-библиотечная система Znaniium.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 |
|--|--|---------------|
| Умение | | |
| анализировать и оценивать угрозы информационной безопасности объекта | уметь анализировать и оценивать угрозы информационной безопасности объекта | Тестирование |
| применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях | уметь применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях | Тестирование |
| применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации | уметь применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации | Тестирование |
| выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования | уметь выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования | Тестирование |
| анализировать информационную безопасность многопользовательских систем | уметь анализировать информационную безопасность многопользовательских систем | Тестирование |
| использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации | уметь использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации | Тестирование |
| Знание | | |
| организационные, технические программные методы защиты информации в информационных системах | знать организационные, технические программные методы защиты информации в информационных системах | Коллоквиум |
| методы идентификации пользователей | знать методы идентификации пользователей | Коллоквиум |
| архитектуру основных стандартов защиты информации | знать архитектуру основных стандартов защиты информации | Коллоквиум |
| организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности | знать организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности | Коллоквиум |
| правовые основы защиты компьютерной информации | знать правовые основы защиты компьютерной информации | Коллоквиум |
| основные методы противодействия «внутренним» угрозам информационной безопасности организации | знать основные методы противодействия «внутренним» угрозам информационной безопасности организации | Коллоквиум |

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

| Результаты обучения | Коды компетенций | Фонды оценочных средств |
|---|---|---|
| Умение | | |
| анализировать и оценивать угрозы информационной безопасности объекта | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №25-28 |
| применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №29-32 |
| применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №33-35 |

| Результаты обучения | Коды компетенций | Фонды оценочных средств |
|--|---|---|
| выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №36-42 |
| анализировать информационную безопасность многопользовательских систем | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №47-50 |
| использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №43-46 |
| Знание | | |
| организационные, технические программные методы защиты информации в информационных системах | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №11-14 |
| методы идентификации пользователей | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №15-19 |
| архитектуру основных стандартов защиты информации | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №20-24 |
| организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №9-10 |
| правовые основы защиты компьютерной информации | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №1-3 |
| основные методы противодействия «внутренним» угрозам информационной безопасности организации | ЛР 1, ПК 2.1., ЛР 22, ЛР 3, ЛР 4, ЛР 7, ЛР 16 | Вопросы к дифференцированному зачёту №4-8 |

Вопросы к практическому занятию указаны в методических указаниях к практическим занятиям по дисциплине Управление информационной безопасностью для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2024

Вопросы к лабораторной работе указаны в методических указаниях к лабораторной работе по дисциплине Управление информационной безопасностью для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2024

Вопросы к практической подготовке указаны в методических указаниях к практической подготовке по дисциплине Управление информационной безопасностью для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2024