Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ледович Татьяна Сергеевна
Должность: директор
Дата подписания: 24.09.2023 06:48:32
Уникальный программный ключ:
4ceaf51badb679c2851a28524a4e0d8f56c5a3a6

КОЛЛЕДЖ «СОВРЕМЕННАЯ ШКОЛА БИЗНЕСА»
Частное профессиональное образовательное учреждение

355008, г. Ставрополь, пр-т К. Маркса, 7
+7(8652) 28-49-67
+7(8652) 28-03-46
college09@mail.ru| www.ecmsb.ru

УТВЕРЖДАЮ
Директор ЧПОУ Колледж
«Современная школа бизнеса»
_____ Т.С. Ледович
«23»_____мая_____2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Профессионального учебного цикла
программы подготовки специалистов среднего звена
по специальности 09.02.03 Программирование в компьютерных системах

Ставрополь, 2023

СОДЕРЖАНИЕ

1. **ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4**
2. **СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 7**
3. **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 13**
4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 15**

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.11 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Рабочая программа учебной дисциплины ОП.11 «Основы информационной безопасности» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по СПО 09.02.03 «Программирование в компьютерных системах».

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании в рамках реализации программ переподготовки кадров в учреждениях СПО.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина ОП.11 «Основы информационной безопасности» входит в профессиональный учебный цикл.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Цель дисциплины

- изучение принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

Задачи дисциплины:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;

- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;
- приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

В результате освоения дисциплины обучающийся должен **уметь:**

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации.

В результате освоения учебной дисциплины обучающийся должен **знать**:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

Содержание учебной дисциплины ориентировано на подготовку обучающихся к освоению и овладению следующих компетенций:

ОК 1.Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2.Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3.Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4.Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5.Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникационных технологий.

ОК 6.Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7.Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8.Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9.Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 2.3. Решать вопросы администрирования базы данных.

ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

Максимальная учебная нагрузка обучающегося 108 часов, в том числе:

- обязательная аудиторная учебная нагрузка обучающегося 72 часа;
- самостоятельная работа обучающегося 36 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	**108**
Обязательная аудиторная учебная нагрузка	**72**
в том числе:	
лекционные занятия	36
практические занятия	36
курсовая работа (проект)	не предусмотрено
Самостоятельная работа обучающегося (всего)	**36**
Форма итоговой аттестации – дифференцированный зачет	

2.2. Примерный тематический план и содержание учебной дисциплины Основы информационной безопасности

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) (если предусмотрены)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Информационная безопасность и уровни ее обеспечения		**30**	
Тема 1.1. Понятие "информационная безопасность"	**Введение.**	8	2
	Проблема информационной безопасности общества		
	Самостоятельная работа.		
Тема 1.2. Составляющие информационной безопасности	Доступность информации. Целостность информации	6	3
	Конфиденциальность информации		
Тема 1.3. Система формирования режима информационной безопасности	Задачи информационной безопасности общества	8	2
	Практическая работа. Законодательство РФ в области информационной безопасности.		
	Самостоятельная работа.		
Тема 1.4. Нормативно-правовые основы информационной безопасности в РФ	Правовые основы информационной безопасности общества	8	3
	Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации		
	Ответственность за нарушения в сфере информационной безопасности		
	Практическая работа. Изучение положений о государственном лицензировании деятельности в области защиты информации.		
	Самостоятельная работа.		
Раздел 2. Стандарты информационной безопасности		**42**	
Тема 2.1. Стандарты информационной безопасности: "Общие критерии"	Требования безопасности к информационным системам	12	2
	Принцип иерархии: класс – семейство – компонент – элемент		
	Практическая работа. Изучение положений о сертификации средств защиты		

	информации по требованиям безопасности информации.		
	Практическая работа. Система сертификации средств криптографической защиты информации.		
	Практическая работа. Процедура аутентификации пользователя на основе пароля.		
	Практическая работа. Программная реализация криптографических алгоритмов.		
	Самостоятельная работа.		
Тема 2.2. Стандарты информационной безопасности распределенных систем	Сервисы безопасности в вычислительных сетях	8	2
	Администрирование средств безопасности		
	Самостоятельная работа.		
Тема 2.3. Стандарты информационной безопасности в РФ	Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ	8	3
	Документы по оценке защищенности автоматизированных систем в РФ		
	Самостоятельная работа.		
Тема 2.4. Административный уровень обеспечения информационной безопасности	Цели, задачи и содержание административного уровня	6	2
	Разработка политики информационной безопасности		
Тема 2.5. Классификация угроз "информационной безопасности	Классы угроз информационной безопасности	8	3
	Каналы несанкционированного доступа к информации		
	Практическая работа. Механизмы контроля целостности данных.		
	Самостоятельная работа.		
Раздел 3. Компьютерные вирусы и защита от них		**36**	
Тема 3.1. Вирусы как угроза информационной безопасности	Компьютерные вирусы и информационная безопасность	8	2
	Характерные черты компьютерных вирусов		
Тема 3.2. Классификация компьютерных вирусов	Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям	6	2
Тема 3.3. Характеристика "вирусоподобных" программ	Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы	22	3
	Практическая работа. Алгоритмы поведения вирусных и других вредоносных программ.		

	Практическая работа. Алгоритмы предупреждения и обнаружения вирусных угроз.		
	Практическая работа. Пакеты антивирусных программ.		
	Самостоятельная работа.		
	Дифференцированный зачет:	**108**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач

2.3 Примерная тематика курсовых работ – не предусмотрены.

2.4 Примерная тематика рефератов

1. Основные алгоритмы шифрования данных: RSA.
2. Основные алгоритмы шифрования данных: DES.
3. Основные алгоритмы шифрования данных: ГОСТ.
4. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
5. Защита данных в автономном компьютере.
6. Защита данных в вычислительных сетях. Разработка сетевых аспектов политики безопасности.
7. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
8. Показатели оценки достоверности передачи данных в сетях.
9. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
10. Парольная защита операционных систем. Парольные взломщики.
11. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
12. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности.
13. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
14. Причины, виды и каналы утечки информации.
15. Методы построения защищенных автоматизированных систем.

2.5 Примерный перечень вопросов к дифференцированному зачету.

1. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
2. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
3. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
4. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.

5. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
6. Реализация методов и средств защиты информации.
7. Средства опознания и разграничения доступа к информации.
8. Криптография. Симметричные криптосистемы.
9. Криптография. Асимметричные криптосистемы.
10. Обзор и классификация методов шифрования информации.
11. Электронно-цифровая подпись.
12. Основные алгоритмы шифрования данных: RSA.
13. Основные алгоритмы шифрования данных: DES.
14. Основные алгоритмы шифрования данных: ГОСТ.
15. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
16. Защита данных в автономном компьютере.
17. Защита данных в вычислительных сетях. Разработка сетевых аспектов политики безопасности.
18. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
19. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
20. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
21. Парольная защита операционных систем. Парольные взломщики.
22. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
23. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности.
24. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
25. Причины, виды и каналы утечки информации.
26. Методы построения защищенных автоматизированных систем.
27. Политика безопасности. Основные типы политики безопасности.
28. Политика безопасности. Модели безопасности.
29. Стандарты информационной безопасности.
30. Правовое обеспечение защиты информации. Нормативные документы.

31. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.
32. Психологические аспекты информационной безопасности организации.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия кабинета стандартизации и сертификации.

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно–наглядных пособий.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением;
- мультимедиапроектор.

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Основы информационной безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - М. : РИОР : ИНФРА-М, 2019. — 202 с. — (Среднее профессионааьное образование). — DOI: https://doi.org/10.29039/01806-4 - Режим доступа: http://znanium.com/catalog/product/1014830
2. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/915902
3. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону: Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Режим доступа: http://znanium.com/catalog/product/997105

Дополнительная литература (в том числе периодические издания):

1. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-627-0 - Режим доступа: http://znanium.com/catalog/product/516806

2. Стандарты информационной безопасности : курс лекций / В.А. Галатенко. — Москва : Интуит НОУ, 2016. — 308 с. — ISBN 978-5-9556-0053-6. — URL: https://book.ru/book/918242
3. Общие вопросы технической защиты информации. Курс лекций / Скрипник Д.А.. — Москва : Интуит Ноу, 2016. — 425 с.— — URL: https://book.ru/book/917804

Информационные справочно-правовые системы:

1. КонсультантПлюс –http://www.consultant.ru/

Интернет ресурсы:

1. http://www.book.ru
2. http://www. znanium.com

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе опроса, проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен **уметь:**	
Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	Результаты выполнения разработки схем (таблиц)
Применять основные правила и документы системы сертификации Российской Федерации;	Результаты выполнения практических занятий
Классифицировать основные угрозы безопасности информации;	Результаты выполнения практических занятий
В результате освоения дисциплины обучающийся должен **знать:**	
Сущность и понятие информационной безопасности, характеристику ее	Результаты выполнения тестирования
Место информационной безопасности в системе национальной безопасности страны;	Результаты выполнения практических занятий
Источники угроз информационной безопасности и меры по их	Результаты выполнения практических занятий
Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;	Результаты выполнения практических занятий
Современные средства и способы обеспечения информационной безопасности.	Результаты выполнения практических занятий