Министерство образования Ставропольского края Государственное бюджетное профессиональное образовательное учреждение «Ставропольский региональный многопрофильный колледж»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 98 D1 56 74 19 8C 56 17 96 D5
Владелец: Бледных Евгений Викторович
Действителен: с 03.09.2020 по 03.09.2025

УТВЕРЖДАЮ
Директор ГБПОУ СРМК
_____ Е.В.Бледных
«01» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.16 Информационная безопасность
Специальность 09.02.07 Информационные системы и программирование

Ставрополь 2022

ОДОБРЕНА
Кафедрой «Программное обеспечение
и информационные технологии»

Протокол №10 от 24.05.2022 г.
Зав. кафедрой
_____ Т.М. Белянская

Согласовано:
Методист
_____О.С. Сизинцова

Разработчик:
Безпалько Е.Л-А., преподаватель ГБПОУ СРМК

Рекомендована Экспертным советом государственного бюджетного профессионального образовательного учреждения «Ставропольский региональный многопрофильный колледж»

Заключение Экспертного совета №13 от 27 мая 2022 г.

Рабочая программа учебной дисциплины разработана за счет часов вариативной части Федерального государственного образовательного стандарта по специальности программы подготовки специалистов среднего звена государственного бюджетного профессионального образовательного учреждения «Ставропольский региональный многопрофильный колледж» по специальности **09.02.07 «Информационные системы и программирование»**, входящей в укрупненную группу направлений подготовки и специальностей **09.00.00 Информатика и вычислительная техника**

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение «Ставропольский региональный многопрофильный колледж»

Разработчики:
Есауленко Н.А, преподаватель

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа учебной дисциплины разработана за счет часов вариативной части Федерального государственного образовательного стандарта по специальности среднего профессионального образования **09.02.06 Сетевое и системное администрирование** (базовой подготовки), укрупненной группы специальностей **09.00.00 Информатика и вычислительная техника**

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: дисциплина относится к дисциплинам общепрофессионального цикла.

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

Цель рабочей программы учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен уметь:

- формулировать тему, проблему, ставить цель и задачи,
- обосновывать актуальность проблемы, определять гипотезу, доказывать или опровергать ее,
- создавать продукт исследовательской деятельности,
- составлять содержание работы и план своих действий на каждом этапе,
- составлять структуру своего исследования,
- проводить исследование и делать вывод по его результатам,
- работать с различными источниками информации, используя разные формы защиты информации,
- выявлять вирусы,
- использовать современные средства защиты информации.

В результате освоения учебной дисциплины обучающийся должен знать:

- современные методы защиты информации;•
- основные виды угроз;
- виды продуктов вирусов;
- формы защиты информации в сети ЭВМ;
- требования к защите информации, критерии оценки угроз.

В результате освоения дисциплины формируются компоненты следующих общих и профессиональных компетенций

ОК 02: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК..06. Проявлять гражданско- патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК.07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК.09. Использовать информационные технологии в профессиональной деятельности
ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.

1.4. Количество часов на освоение программы дисциплины:
максимальной учебной нагрузки обучающегося 60 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 50 часов;
самостоятельной работы обучающегося 10 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	60
Обязательная аудиторная учебная нагрузка (всего)	50
в том числе:	
лекции	30
лабораторные занятия (не предусмотрена)	-
практические занятия	20
контрольные работы	-
курсовая работа (проект) (не предусмотрена)	-
Самостоятельная работа обучающегося (всего)	10
Итоговая аттестация в форме дифференцированного зачета	

2.2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.16 Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лекции и практические занятия, самостоятельная работа обучающихся.	Объем часов	Коды компетенций
1	2	3	4
Раздел 1.	**Общие вопросы информационной безопасности.**	**16**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4, ПК.11.6
Тема 1.1. Международные стандарты информационного обмена	**Содержание учебного материала**	**4**	
	1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. 2. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность защиты информации: инструментальная, структурная,		
	Практические занятия: Защита документооборота в вычислительных системах	**2**	
	Самостоятельная работа обучающихся:1. Проведение анализа информационной системы. 2. Доклад на тему «Защита информации, тайна»	**1**	
Тема 1.2 Понятия и угрозы.	**Содержание учебного материала**	**4**	
	1. Основные понятия. Механизмы безопасности. Классы безопасности. 2. Основные определения и критерии классификации угроз		
	Практическая работа Криптографические методы защиты	**2**	
	Самостоятельная работа обучающихся:1. Выявление угроз и уязвимостей, каналов утечки информации 2. Презентация по теме «Основные угрозы»	**1**	

Раздел 2.	**Государственная система информационной безопасности**	**10**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4, ПК.11.
Тема 2.1	**Содержание учебного материала**	**4**	
Информационная безопасность в условиях функционирования в России глобальных сетей.	1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации 2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.	**4**	
	Практические занятия: Шифрование методом IDEA	**4**	
	Самостоятельная работа обучающихся:1. Краткий конспект по теме «Концепция информационной безопасности.» 2. Исследовательская работа	**2**	
Раздел 3.	**Угрозы безопасности**	**8**	
Тема 3.1 Угрозы безопасности.	**Содержание учебного материала**	**2**	
	1. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения 2. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного		
	Практические занятия: Шифрование методом RC6	**4**	
	Самостоятельная работа обучающегося: 1. Виды противников или «нарушителей». Понятие о видах вируса	**2**	

Раздел 4.	**Теоретические основы методов защиты информационных систем**	**8**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4,
Тема 4.1 Теоретические основы методов защиты информационных систем	**Содержание учебного материала**	**4**	
	1. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности 2. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения		
	Практические занятия: Шифрование методом SAFER K-64	**2**	
	Самостоятельная работа обучающегося: 1. Три вида возможных нарушений информационной системы. 2. Доклад по теме «Права доступа Take-Grant»	**1**	
Раздел 5.	**Методы защиты средств вычислительной техники**	**10**	
Тема 5.1 Методы защиты средств вычислительной техники	**Содержание учебного материала**	**4**	
	1. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. 2. Средства операционной системы. Средства резервирования данных. Проверка		
	Практические занятия: Криптосистема Эль-Гамаля	**2**	
	Самостоятельная работа обучающегося 1. Виды защиты 2. Выявление угроз и уязвимостей	**2**	
Раздел 6.	**Основы криптографии**	**8**	
Тема 6.1	**Содержание учебного материала**	**4**	
Основы криптографии	1. Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. 2. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы.		

	Практические занятия Шифрование методом Вернам	**2**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4, ПК.11. ПК.11.
	Самостоятельная работа обучающегося: 1. Презентация по теме «Криптоанализ»	**1**	
Раздел 7.	**Архитектура защитных экономических систем**	**4**	
Тема 7.1 Архитектура защитных экономических систем	**Содержание учебного материала**	**4**	
	1. Основные технологии построения защищенных экономических информационных		
	2.Функции защиты информации. Классы задач защиты информации. Архитектура систем		
	защиты информации		
	Самостоятельная работа обучающегося	**-**	
	Промежуточная аттестация –дифференцированный зачет	**2**	
	Всего	**60 час.** -	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины предполагает наличие кабинета Информатики, библиотеки, читального зала с выходом в сеть Интернет.

Кабинет информатики и информационных технологий

рабочие места по количеству обучающихся;
доска ученическая
12 ПК (ПЭВМ СПК 910);
мультимедийный проектор (Ben Q MX528),
- экран настенный.
Программное обеспечение:
•Антивирус Kaspersky
•Kerio control
• Windows 7 Professional
•WindowsServer 2008 R2standart
• Windows 8.1 Enterprise Инструментальная среда адаптивного тестирования "АСТ-тест"
• СПС Консультант +
• УМК дисциплины.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основной источник литературы

1. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — Саратов:, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/86938.html (дата обращения: 22.11.2019).

Дополнительная литература

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/87992.html (дата обращения: 15.10.2019).
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/87995.html (дата обращения: 27.11.2019).
3. Информационная безопасность: лабораторный практикум / составители Т.

Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь: Пермский государственный гуманитарно-педагогический университет, 2018. — 86 с. — ISBN 978-5-85219-007-9. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/86357.html (дата обращения: 22.11.2019).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Программа составлена в соответствии с требованиями ФГОС СПО для специальностей технического профиля

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов я**
1. выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	Выполнение и защита заданий по практическим работам.
2. осуществлять диагностику и поиск неисправностей технических средств;	Выполнение и защита заданий по практическим работам.
3. тестировать кабели и коммуникационные устройства;	Выполнение и защита заданий по практическим работам.
4. правильно оформлять техническую документацию;	Выполнение и защита заданий по практическим работам.
5. наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	Выполнение и защита заданий по практическим работам.
6. устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	Выполнение и защита заданий по практическим работам.

Результаты (освоенные общие компетенции)	**Формы и методы контроля**
ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами. ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.	Экспертное оценивание выполнения практических работ и самостоятельной работы