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» июня 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.16 Информационная безопасность

Технологический профиль

Специальность 09.02.07 Информационные системы и программирование

Курс 2,3

Группа П-23, П-31, П-32, П-34

Ставрополь 2023

ОДОБРЕНА
Кафедрой «Программное обеспечение
и информационные технологии»
Протокол №10 от 15. 05.2023 г.
Зав. кафедрой
_____ Т.М. Белянская

Согласовано:
Методист
_____О.С. Сизинцова

Разработчик:
Мамутов Е.В. , преподаватель

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

Заключение Экспертного совета № 14 от 24мая 2023 г.

Рабочая программа разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование, укрупненной группы специальностей 09.00.00 Информатика и вычислительная техника

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

СОДЕРЖАНИЕ

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

1.1. Область применения программы

Рабочая программа учебной дисциплиныразработана 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**

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 защитыинформации,
- 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 следующихобщих 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 60часов, 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.16Информационная безопасность»

Наименование разделовитем	Содержаниеучебногоматериала,лекцииипрактическиезанятия,самостоятельнаяработаобучающихся.	Объем часов	Коды компетенций
1	2	3	4
Раздел1.	**Общиевопросыинформационнойбезопасности.**	**16**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4, ПК.11.6
Тема1.1. Международные стандарты информационного обмена	**Содержаниеучебногоматериала**	**4**	
	1.Основные понятияи определения. Понятияинформация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средствазащиты информации. 2.Международныестандарты информационногообмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность защиты информации: инструментальная, структурная,		
	Практическиезанятия: Защита документооборота в вычислительных системах	**2**	
	Самостоятельнаяработаобучающихся:1.Проведение анализа информационной системы. 2.Доклад на тему «Защита информации,тайна»	**1**	
Тема1.2Понятияиугрозы.	**Содержаниеучебногоматериала**	**4**	
	1. Основныепонятия. Механизмы безопасности.Классы безопасности. 2. Основныеопределения и критерии классификацииугроз		
	Практическаяработа Криптографические методы защиты	**2**	
	Самостоятельнаяработаобучающихся:1.Выявлениеугроз иуязвимостей, каналовутечки информации 2.Презентация потеме«Основныеугрозы»	**1**	

Раздел2.	**Государственнаясистемаинформационнойбезопасности**	**10**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4, ПК.11.
Тема2.1	**Содержаниеучебногоматериала**	**4**	
ИнформационнаябезопасностьвусловияхфункционированиявРоссииглобальныхсетей.	1.Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочныедокументы. Назначение и задачи в сфереобеспечения информационнойбезопасности науровне государства. Доктрина информационной безопасности РоссийскойФедерации 2.Структура государственнойсистемы информационной безопасности.Структура законодательнойбазыпо вопросам информационной безопасности.Лицензирование и сертификация в области защитыинформации.Место информационной безопасности экономическихсистем в национальнойбезопасностистраны, опасностистраны.	**4**	
	Практическиезанятия: Шифрование методомIDEA	**4**	
	Самостоятельнаяработаобучающихся:1.Краткий конспект потеме«Концепция информационнойбезопасности.» 2.Исследовательская работа	**2**	
Раздел3.	**Угрозыбезопасности**	**8**	
Тема3.1Угрозы безопасности.	**Содержаниеучебногоматериала**	**2**	
	1.Понятиеугрозы.Виды противниковили«нарушителей». Классификацияугроз информационной безопасности. Видыугроз. Основные нарушения 2.Характер происхожденияугроз (умышленные иестественныефакторы). Источники угроз. Предпосылки появленияугроз. Классыканалов несанкционированного		
	Практическиезанятия: Шифрование методом RC6	**4**	
	Самостоятельнаяработаобучающегося: 1.Виды противников или«нарушителей».Понятие о видахвируса	**2**	

Раздел4.	**Теоретическиеосновыметодовзащитыинформационныхсистем**	**8**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4,
Тема4.1Теоретическиеосновыметодовзащитыинформационныхсистем	**Содержаниеучебногоматериала**	**4**	
	1.Основные положения теорииинформационной безопасностиинформационных систем. Моделибезопасности иих применение.Формальные моделибезопасности 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		
	Практическиезанятия: Шифрование методом SAFER K-64	**2**	
	Самостоятельнаяработаобучающегося: 1.Три вида возможных нарушений информационной системы. 2.Доклад по теме«Правадоступа Take-Grant»	**1**	
Раздел5.	**Методызащитысредстввычислительнойтехники**	**10**	
Тема5.1Методызащитысредстввычислительной техники	**Содержаниеучебногоматериала**	**4**	
	1.Использование защищенных компьютерныхсистем. Аппаратные и программные средствадля защиты компьютерныхсистемотНСД. 2.Средства операционной системы. Средства резервирования данных.Проверка		
	Практическиезанятия: Криптосистема Эль-Гамаля	**2**	
	Самостоятельнаяработаобучающегося 1.Виды защиты 2.Выявлениеугроз иуязвимостей	**2**	
Раздел6.	**Основыкриптографии**	**8**	
Тема6.1	**Содержаниеучебногоматериала**	**4**	
Основыкриптографии	1.Методы криптографии.Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись.Алгоритмыэлектронно-цифровой подписи. 2.Хеширование. Имитовставки. Криптографические генераторы случайныхчисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атакина криптосистемы.		

	Практическиезанятия Шифрование методомВернам	**2**	ОК.02, ОК.06, ОК.07, ОК.09, ПК.4.4, ПК.11. ПК.11.
	Самостоятельнаяработаобучающегося: 1.Презентация потеме«Криптоанализ»	**1**	
Раздел7.	**Архитектуразащитныхэкономическихсистем**	**4**	
Тема7.1Архи тектуразащи тных **экономическихсистем**	**Содержаниеучебногоматериала**	**4**	
	1.Основные технологиипостроения защищенныхэкономическихинформационных систем.		
	2.Функции защиты информации. Классы задач защиты информации. Архитектура систем		
	защиты информации		
	Самостоятельнаяработаобучающегося	**-**	
	Промежуточная аттестация –дифференцированный зачет Всего	**2** **60час.**-	

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;
- мультимедийный проектор;
- экран настенный.

Программное обеспечение:
•Антивирус Kaspersky
•Kerio control
• Windows 10, baseAlt
• СПС Консультант +
• УМКдисциплины.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основной источник литературы

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519614 (дата обращения: 06.06.2023)

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006 (дата обращения: 06.06.2023).

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1910870 (дата обращения: 02.06.2023). – Режим доступа: по подписке.

4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для

среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005 (дата обращения: 06.06.2023).

5. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1898839 (дата обращения: 02.06.2023). – Режим доступа: по подписке.

6. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189328 (дата обращения: 03.03.2023). – Режим доступа: по подписке.

Дополнительная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861 (дата обращения: 06.06.2023).

2. Баранова, Е. К. Основы информационной безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1860126 (дата обращения: 02.06.2023). – Режим доступа: по подписке.

3. Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-466-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189325 (дата обращения: 20.04.2023). – Режим доступа: по подписке.

4. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. – Москва : ФОРУМ, 2022. – 366, [1] с. : ил. – (Среднее профессиональное образование). – ISBN 978-5-16-104336-3. – Текст : электронный // Znanium.com : электронно-библиотечная система : [сайт]. – URL: https://znanium.com/catalog/product/1836631 (дата обращения: 05.04.2023). – Режим доступа: для авторизир. пользователей.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Программасоставленавсоответствииистребованиями ФГОССПОдляспециальностей технического профиля

Результатыобучения(освоенные умения,усвоенныезнания)	**Формыиметодыконтроляи оценкирезультатовобучени я**
1.выполнять мониторинги анализ работылокальнойсети с помощью программно-аппаратных средств;	Выполнение и защитазаданий по практическимработам.
2.осуществлятьдиагностикуи поиск неисправностей технических средств;	Выполнение и защитазаданий по практическимработам.
3.тестироватькабелии коммуникационныеустройства;	Выполнение и защитазаданий по практическимработам.
4.правильно оформлять техническую документацию;	Выполнение изащита заданийпо практическимработам.
5.наблюдать за трафиком, выполнять операции резервногокопированияи восстановления данных;	Выполнение и защитазаданий по практическимработам.
6.устанавливать,тестировать и эксплуатироватьинформационныес истемы, согласно технической документации, обеспечивать антивирусную защиту;	Выполнение и защитазаданий по практическимработам.

Результаты(освоенныеобщиекомпе тенции)	**Формыиметодыконтроля**
ПК 4.4. Обеспечивать защитупрограммного обеспечения компьютерныхсистем программными средствами. ПК 11.6. Защищать информацию в базе данных с использованием технологии защитыинформации.	Экспертное оценивание выполнения практическихработи самостоятельной работы