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

УТВЕРЖДАЮ

Директор ГБПОУ СРМК
_____Е.В. Бледных

«20» мая 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 Информационная безопасность

Ставрополь 2020

ОДОБРЕНА
кафедрой программного обеспечения
и информационных технологий
Протокол № г.
Зав. кафедрой
_____

Согласовано:
Методист
_____

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

Заключение Экспертного совета

Рабочая программа учебной дисциплины разработана за счет часов вариативной части Федерального государственного образовательного стандарта по специальности среднего профессионального образования **09.02.01 Компьютерные системы и комплексы** базовой подготовки, 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:

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 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 **09.02.01 Компьютерные системы и комплексы** базовой подготовки, 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 общепрофессиональным дисциплинам профессионального цикла.

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

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС СПО и ППССЗ по данному направлению подготовки:

а) общих компетенций (ОК), включающих в себя способность**:**

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

ОК 2. Организовывать собственную деятельность, определять 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. Использовать информационно-коммуникационные технологии в профессиональной деятельности

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

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

б) профессиональных компетенций (ПК),

ПК 1.1. Разрабатывать схемы цифровых устройств на основе интегральных схем разной степени интеграции.

ПК 1.2. Выполнять требования технического задания на проектирование цифровых устройств.

ПК 1.3. Использовать средства и методы автоматизированного проектирования при разработке цифровых устройств

ПК 1.4. Определять показатели надежности и качества проектируемых цифровых устройств.

ПК 1.5. Выполнять требования нормативно – технической документации.

ПК 2.1. Создавать программы на языке ассемблера для микропроцессорных систем.

ПК 2.2. Производить тестирование и отладку микропроцессорных систем.

ПК 2.3. Осуществлять установку и конфигурирование персональных компьютеров и подключение периферийных устройств.

ПК 2.4. Выявлять причины неисправности периферийного оборудования.

ПК 3.1. Проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов.

ПК 3.2. Проводить системотехническое обслуживание компьютерных систем и комплексов.

ПК 3.3. Принимать участие в отладке и технических испытаниях компьютерных систем и комплексов; инсталляции, конфигурировании и настройке операционной системы, драйверов, резидентных программ.

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

- применять правовые, организационные, технические и программные средства защиты информации;
- создавать программные средства защиты информации.

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

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации.

1.4. Количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 84 часа, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 56 часов;

самостоятельной работы обучающегося 28 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)	*84*
Обязательная аудиторная учебная нагрузка (всего)	*56*
в том числе:	
лабораторные занятия (*не предусмотрена)*	-
практические занятия	*22*
контрольные работы	-
курсовая работа (проект) (*не предусмотрена)*	-
Самостоятельная работа обучающегося (всего)	*28*
в том числе:	
самостоятельная работа над курсовой работой , проектом *(не предусмотрена)*	-
–домашнее задание	*5*
–презентация	*5*
–мини – проект	*4*
–опорный конспект	*8*
–опорно-логическая схема	*6*
Итоговая аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины ОП.13 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов	Уровень освоения
1	**2**	**3**	**4**
Раздел 1. Борьба с угрозами несанкционированного доступа к информации		**42**	
Тема 1.1. Актуальность проблемы обеспечения безопасности информации	**Содержание учебного материала**	*4*	
	1 **Актуальность проблемы обеспечения безопасности информации** Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации.		*2*
	2 **Угрозы информационной безопасности** Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности.		
	Лабораторные работы: ***(не предусмотрены)***	-	
	Практические занятия 1. Анализ рисков информационной безопасности. 2. Анализ обеспечения информационной безопасности в ведущих зарубежных странах.	*4*	
	Контрольные работы ***(не предусмотрены)***	-	
	Самостоятельная работа обучающихся:	*2*	
	Выполнение домашнего задания по теме 1.1.		
	Тематика внеаудиторной самостоятельной работы: Наиболее распространенные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Управление рисками. – опорный конспект.		
Тема 1.2.	**Содержание учебного материала**	*4*	

Виды мер обеспечения информационной безопасности	1	**Виды мер обеспечения информационной безопасности**: законодательные, морально-этические, организационные, технические, программно-математические.		*2*
	2	**Специфические приемы управления техническими средствами.** Методы защиты от копирования. Некопируемые метки. Защита от средств отладки и дисассемблирования. Защита программ в оперативной памяти.		
	Лабораторные работы : *(не предусмотрены)*		-	
	Практическое занятие 1. Построение концепции информационной безопасности предприятия		*2*	
	Контрольные работы: *(не предусмотрены)*		-	
	Самостоятельная работа обучающихся:		*4*	
	Выполнение домашнего задания по теме 1.2.			
	Тематика внеаудиторной самостоятельной работы: Политика безопасности. Модели систем безопасности. Реагирование на нарушения режима безопасности. – опорный конспект.			
Тема 1.3. **Основные принципы построения систем защиты информации**	**Содержание учебного материала**		*8*	
	1	**Основные защитные механизмы.** Идентификация и аутентификация. Разграничение доступа. Контроль целостности..		*2*
	2	**Криптографические механизмы** Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Обнаружение и противодействие атакам		
	3	**Симметричное шифрование, открытого ключа, хэш-функции, электронной подписи.** Основные сведения. Общая схема. Требования. Виды симметричных шифров. Параметры алгоритмов.		
	4	**Криптографические алгоритмы защиты информации** Назначение и особенности применения алгоритмов DES, ГОСТ 28147-89, RSA, DSS, SHA и MD5. Понятие инфраструктуры открытых ключей и проблемы ее создания.		
	Практические занятия*:*		*8*	

	1. Использование процедуры аутентификации пользователя на основе пароля. 2-3. Программная реализация криптографических алгоритмов. 4. Использование механизма контроля целостности данных			
	Контрольные работы *(не предусмотрены)*		-	
	Самостоятельная работа обучающихся:		*6*	
	Выполнение домашнего задания по теме 1.3.			
	Тематика внеаудиторной самостоятельной работы: Идентификация/аутентификация с помощью биометрических данных. Парольная аутентификация. Одноразовые пароли. Блочные шифры. Сеть Файстеля. – опорно-логическая схема			
Раздел 2. **Борьба с вирусным заражением информации**			*22*	
Тема 2.1. **Проблема вирусного заражения и структура современных вирусов**	**Содержание учебного материала**		*6*	
	1	**Компьютерные вирусы** Компьютерный вирус: понятие, пути распространения, проявление действия вируса.		*2*
	2	**Структура современных вирусов** Модели поведения вирусов; деструктивные действия вируса; разрушение программы защиты, схем контроля или изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации		
	3	**Проблема вирусного заражения** Программы-шпионы. Взлом парольной защиты. Защита от воздействия вирусов.		
	Лабораторные работы: *(не предусмотрены)*		-	
	Практические занятия: 1. Алгоритмы поведения вирусных и других вредоносных программ.		*2*	
	Контрольные работы: *(не предусмотрены)*		-	
	Самостоятельная работа обучающихся:		*4*	
	Выполнение домашнего задания по теме 2.1.			

	Тематика внеаудиторной самостоятельной работы: Сравнительный анализ компьютерных вирусов – мини-проект			
Тема 2.2. **Классификация антивирусных программ**	**Содержание учебного материала**		*2*	
	1	**Классификация антивирусных программ** Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Программа Анти-вирус Касперского Personal.		*2*
	Лабораторные работы: *(не предусмотрены)*			
	Практические занятия: 1.Алгоритмы предупреждения и обнаружения вирусных угроз 2. Анализ пакетов антивирусных программ.		*4*	
	Контрольные работы: *(не предусмотрены)*			
	Самостоятельная работа обучающихся:		*4*	
	Выполнение домашнего задания по теме 2.2.			
	Тематика внеаудиторной самостоятельной работы: Сравнительный анализ антивирусных программ – мини-проект.			
Раздел 3. **Организационно-правовое обеспечение информационной безопасности**			*20*	
Тема 3.1. Международные, российские и отраслевые правовые документы	**Содержание учебного материала**		*10*	
	1	**Организационно-правовое обеспечение информационной безопасности.** Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности Российской Федерации.		*2*
	2	**Российские правовые документы обеспечения информационной безопасности** Стандарты и нормативно-методические документы в области обеспечения информационной безопасности		
	3	**Государственная система обеспечения информационной безопасности.** Основные задачи и методы обеспечения информационной		

		безопасности. Общие и частные методы.		
	4	**Международные правовые акты по защите информации.** Конвенция о преступности в сфере компьютерной безопасности. Перечень международных правовых актов		
	5	**Должностные инструкции.** Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.		
	Лабораторные работы: *(не предусмотрены)*		-	
	Практические занятия: *(не предусмотрены)*		-	
	Контрольные работы: *(не предусмотрены)*		-	
	Самостоятельная работа обучающихся:		*8*	
	Выполнение домашнего задания по теме 3.1.			
	Тематика внеаудиторной самостоятельной работы: Изучение нормативно-правовой базы РФ в области ИБ. Изучение международного законодательства в области ИБ. Стандарты информационной безопасности. "Оранжевая книга" как оценочный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Гармонизированные критерии Европейских стран. – опорно-логические схемы			
Дифференцированный зачет			2	
Тематика курсовой работы (проекта) *(не предусмотрена)*			-	
Самостоятельная работа обучающихся над курсовой работой (проектом) *(не предусмотрена)*			-	
		Всего:	**84**	

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.

Оборудование учебного кабинета Информатики:

- посадочные места по количеству обучающихся;
- АРМ студентов;
- АРМ преподавателя;
- комплекты учебно – наглядных пособий;
- комплект учебно-методической документации;
- цифровые образовательные ресурсы;

Технические средства обучения:

- компьютеры (рабочие станции);
- мультимедийный проектор;
- сервер;
- локальная сеть;
- выход в глобальную сеть;
- принтер, сканер, внешние накопители информации;
- мобильные устройства для хранения информации;
- программное обеспечение общего и профессионального назначения;
- аудиовизуальные средства.

Оборудование и технологическое оснащение рабочих мест:

компьютеры, локальная сеть, выход в глобальную сеть.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бардаев Э.А. Документоведение : учебник : [по направлению подготовки "Информационная безопасность"] / Э. А. Бардаев, В. Б. Кравченко. - 3-е изд., перераб. и доп. - Москва : Академия, 2013
2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - М. : Форум : Инфра-М, 2013
3. Малюк А.А. Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев и др.; под ред. В.С.Горбатова. - М. : Горячая линия - Телеком, 2013
4. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 4-е изд., стер. - М. : Горячая линия - Телеком, 2011.

5. Мельников В.П. Защита информации : учебное пособие для студ. Высш. Учеб. заведений/ В.П. Мельников, С.А. Клейменов, А.М. Петраков: под ред. Мельникова В.П. - 1-е изд., - М.: Издательский центр «Академия», 2014
6. Платонов, В. В. Программно-аппаратные средства защиты информации : учебник для вузов / В. В. Платонов. - М. : Академия, 2013.
7. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие для студентов учреждений среднего профессионального образования. ИД «ФОРУМ»-ИНФРА-М, 2011 г.

Дополнительные источники:

1. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1 — 2006).
2. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
3. Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005).

Интернет-ресурсы:

1. федеральный портал «Российское образование» http://www.edu.ru/;
2. федеральный портал «Российский портал открытого образования»;
3. сетевая энциклопедия Википедия http://ru.wikipedia.org/;
4. Интернет – университет http://www.intuit.ru/

Журналы:

1. Хакер
2. Компьютер-Пресс
3. Мир ПК.

3.3. Образовательные технологии

3.3.1. В соответствии с ФГОС СПО по специальности **09.02.01 Компьютерные системы и комплексы** базовой подготовки в разделе VII. п.7.1. Требования к условиям реализации основной профессиональной образовательной программы указано, что «образовательное учреждение при формировании ППССЗ: должно предусматривать в целях реализации компетентностного подхода использование в образовательном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов, групповых дискуссий) в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся».

3.3.2 Используемые активные и интерактивные формы проведения занятий, современные образовательные технологии:

Вид занятия*	Используемые формы занятий, активные и интерактивные образовательные технологии
ТО	**Активные и интерактивные формы занятий:** - урок взаимообучения - урок-диалог - урок открытых мыслей - урок деловых игр - мозговая атака - имитационно-ролевое моделирование - компьютерные симуляции - урок- лекция: - информационная лекция, - проблемная лекция, - лекция-визуализация - лекция-дискуссия, - лекция-беседа - лекция с применением обратной связи - лекция с опорным конспектированием - разбор конкретных ситуаций - групповые дискуссии **Проектно- исследовательской деятельности** наблюдение, поиск, аналогии, ассоциация, сопоставление; участие в конкурсах разного уровня, научно- практических конференциях; конспектирование; работа с литературой, работа над рефератом; поиск информации в библиотеки, в Интернете; создание презентации; **Технология развития критичности мышления** Эффективная лекция, Взаимообучение Ключевые термины Рефлексивные вопросы Дискуссия Самостоятельное формулирование выводов

	Игрового обучения (деятельности) Деловая игра **Контекстного обучения** Моделирование Самостоятельное формулирование выводов **Интегративного обучения** Интеграция знаний Обобщение и систематизация Работа по сопоставлению
ПР	**Витогенного обучения** Сравнение Работа по сопоставлению Группировка и классификация Рефлексия **Информационно- коммуникационного обучения** Наглядное представление учебного материала Видео и аудиосредства **Технология программированного обучения** Выполнение индивидуальных заданий Работа с виртуальным лабораторным практикумом Электронные обучающие программы Компьютерные программы **Развития индивидуального стиля решения информационно-технических задач (ИТ-задач)** Решение функциональных задач Решение ситуационных задач Решение контекстных функциональных задач
ЛР	не предусмотрено
СР	**Проектно- исследовательской деятельности** наблюдение, поиск, аналогии, ассоциация, сопоставление; участие в конкурсах разного уровня, научно- практических конференциях; работа с литературой, работа над рефератом; поиск информации в библиотеки, в Интернете; создание презентации;

	Технология программированного обучения Выполнение индивидуальных заданий Компьютерные программы **Развития индивидуального стиля решения информационно-технических задач (ИТ-задач)** Решение ситуационных задач

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные компетенции)	**Результаты обучения (освоенные умения, усвоенные знания)**	**Формы и методы контроля и оценки результатов обучения**
	Умения	
ОК 1-9 ПК1.1-1.5 ПК 2.1-2.4 ПК 3.1-3.3	применять правовые, организационные, технические и программные средства защиты информации	Проверка и оценка выполнения практических работ, оценка домашнего задания, дифференцированный зачет
	создавать программные средства защиты информации.	Проверка и оценка выполнения практических работ, оценка домашнего задания, дифференцированный зачет
	Знания	
	источники возникновения информационных угроз	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, дифференцированный зачет
	модели и принципы защиты информации от несанкционированного доступа;	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, дифференцированный зачет
	методы антивирусной защиты информации	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, дифференцированный зачет
	состав и методы организационно-правовой защиты информации	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, дифференцированный зачет