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

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 Информационная безопасность технологический профиль

Специальность	09.02.03 Программирование в компьютерных системах
Курс	3
Группа	П-31, П-32

Ставрополь 2022

ОДОБРЕНО
На заседании кафедры «Программного обеспечения и информационных технологий»
Протокол № 10 от 24.05.2022 г.
Зав. кафедрой
_____ Т. М. Белянская

СОГЛАСОВАНО
Методист
_____О.С. Диба

Разработчик: преподаватель ГБПОУ СРМК Н.А. Есауленко

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

Заключение Экспертного совета Протокол № 13 от 27 мая 2022 г.

2

Рабочая программа учебной дисциплины разработана за счет часов вариативной части Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.03 Программирование в компьютерных системах 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»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 5

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 7

2.2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 8

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 14

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 18

5. ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РАБОЧУЮ ПРОГРАММУ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 19

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 **09.02.03 Программирование в компьютерных системах** 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 ПООП СПО по данной специальности, а также личностных результатов реализации программы воспитания с учетом особенностей специальности (профессии):

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 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

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):

б**) профессиональные компетенции (ПК):**

ПК 1.5. Осуществлять оптимизацию программного кода модуля.

ПК 2.3. Решать вопросы администрирования базы данных.

ПК 3.2. Выполнять интеграцию модулей в программную систему.

ПК 3.3. Выполнять отладку программного продукта с использованием специализированных программных средств.

в) личностные результаты:

ЛР 4 Проявлять и демонстрировать уважение к людям труда, осознавать ценность собственного труда. Стремиться к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 13 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ЛР 14 Использовать информационные технологии в профессиональной деятельности.

ЛР 15 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ЛР 16 Активно применять полученные знания на практике.

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

- применять организационно-правовые методы защиты информации в информационных системах;
- обеспечивать антивирусную защиту информации;
- использовать криптостойкие алгоритмы защиты данных;
- выполнять аутентификацию информации.

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

- сущность информационной безопасности информационных систем;
- состав и методы организационно-правовой защиты информации;
- источники возникновения информационных угроз;
- методы антивирусной защиты информации;
- алгоритмы традиционных методов шифрования данных;
- современные методы криптозащиты информации;
- протоколы идентификации и проверки подлинности пользователя;
- процедуры аутентификации данных и постановки электронной цифровой подписи.

1.4. Количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 105 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 70 часов;

самостоятельной работы обучающегося 35 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)	*105*
Обязательная аудиторная учебная нагрузка (всего)	*70*
в том числе:	
лабораторные занятия (*не предусмотрена)*	-
практические занятия	*36*
контрольные работы	-
курсовая работа (проект) (*не предусмотрена)*	-
Самостоятельная работа обучающегося (всего)	*35*
в том числе:	
самостоятельная работа над курсовой работой , проектом *(не предусмотрена)*	-
выполнение индивидуальных заданий по темам	*4*
составление презентаций, рефератов, сообщений	*16*
–мини – проект	*1*
–опорный конспект	*2*
– составление блок-схем	*12*
Итоговая аттестация в форме экзамена	

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	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Безопасность информационных систем.		**30**	
Тема 1.1. Понятие информационной безопасности.	**Содержание учебного материала**	2	
	1 **Понятие информационной безопасности. Основные принципы информационной безопасности**: целостность, конфиденциальность, доступность. Методы защиты информации в информационной системе.		1
	Лабораторные работы: (не предусмотрены)		
	Практические занятия: (не предусмотрены)		
	Самостоятельная работа обучающихся: 1. Составление презентации/сообщения по темам: - Двадцать первый век и проблемы информационной безопасности. - Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность».	1	
Тема 1.2. Угрозы безопасности.	**Содержание учебного материала**	2	
	1 **Угрозы информационной безопасности:** классификации, источники возникновения и пути реализации. Санкционированный и несанкционированный доступ к данным. Виды несанкционированного доступа к информации. Средства и механизмы защиты от несанкционированного доступа.		2
	Лабораторные работы (не предусмотрены)		
	Практические занятия: 1. Анализ рисков информационной безопасности.	2	
	Самостоятельная работа обучающихся: 2. Составление презентаций или сообщений по темам: - Технические средства современных систем безопасности в информационных системах.	1	

	- Наиболее распространенные угрозы доступности. - Основные угрозы целостности. - Основные угрозы конфиденциальности. - Управление рисками.			
Тема 1.3. Антивирусная защита информации.	**Содержание учебного материала**		4	
	1	**Компьютерные вирусы.** Понятие компьютерного вируса, сущность и возможности проявления. Классификации компьютерных вирусов. Структура современных вирусных программ.		2
	2	**Основные методы и средства защиты от воздействия компьютерных вирусов.** Современные пакеты антивирусных программ. Характеристики и возможности применения.		3
	Лабораторные работы (не предусмотрены)			
	Практические занятия:		2	
	1	Анализ пакетов антивирусных программ.		
	Самостоятельная работа обучающихся:		1	
	Выполнение индивидуальных заданий по теме.			
	3.Выполнение мини-проекта по теме: Сравнительный анализ компьютерных вирусов. Сравнительный анализ антивирусных программ.			
Тема 1.4. Организационно-правовое обеспечение информационной безопасности.	**Содержание учебного материала**		4	
	1	**Концепция правового обеспечения информационной безопасности Российской Федерации**. Законодательная база, стандарты, нормативно-методические документы РФ в области обеспечения информационной безопасности. Ответственность за нарушения законодательства в информационной сфере. Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью.		2
	2	**Организационная защита информации и её место в системе комплексной защиты информации в информационной системе.** Методы и формы организационной защиты информации. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.		3

	Лабораторные работы (не предусмотрены)			
	Практические занятия:		6	
	1	Проведение анализа современных нормативных актов по обеспечению безопасности информации.		
	2	Построение концепции информационной безопасности предприятия.		
	3	Разработка должностной инструкции сотрудника подразделения информационной безопасности.		
	Самостоятельная работа обучающихся:		5	
	Выполнение индивидуальных заданий по теме.			
	4.Подготовка реферата/презентации по темам: - Стратегия обеспечения информационной безопасности предприятия. - Информационная безопасность в бизнесе. - Сертификация, лицензирование, сертификация и аттестация в области информационной безопасности. - Служебная тайна. Коммерческая тайна. Государственная тайна. - Экономика и правовые основы рынка интеллектуальной собственности. - Экономическая информационная безопасность. 5. Подготовка опорного конспекта по теме: Модели систем безопасности.			
Раздел 2. Основы криптографии в информационных системах.			**75**	
Тема 2.1. Традиционные симметричные криптосистемы.	**Содержание учебного материала**		6	
	1	**Принципы криптографической защиты информации:** основные понятия и определения; обобщённая структура криптосистемы; классификация крипто аналитических атак.		2
	2	**Шифры перестановки**: шифрующие таблицы, применение магических квадратов. **Шифры простой замены**: система шифрования Цезаря; аффинная система подстановок Цезаря; система Цезаря с ключевым словом; шифрующие таблицы Трисемуса; биграммный шифр Плейфера; криптосистема Хилла.		3

	3	**Шифры сложной замены**: система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама.		
	Лабораторные работы (не предусмотрены)			
	Практические занятия:		8	
	1	Исследование шифров перестановки.		
	2	Исследование шифров простой замены		
	3	Исследование шифров сложной замены.		
	4	Программирование алгоритмов традиционных методов шифрования.		
	Самостоятельная работа обучающихся:		9	
	6.Выполнение индивидуальных заданий по теме: шифрование и расшифровывание тестовых сообщений с использованием традиционных симметричных криптосистем. 7.Составление блок-схем алгоритмов традиционных методов шифрования. 8. Составление презентаций и сообщений по теме: Шифрование методом гаммирования: методы генерирования псевдослучайных последовательностей чисел.			
Тема 2.2. Современные симметричные криптосистемы.	Содержание учебного материала		4	
	1	**Американский стандарт шифрования DES**. Режимы работы DES: «Электронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру»; «Обратная связь по выходу». Области применения алгоритма DES. Комбинирование блочных алгоритмов.		2
	2	**Отечественный стандарт шифрования данных ГОСТ 28147-89.** Режимы работы: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.		3
	Лабораторные работы (не предусмотрены)			
	Практические занятия:		12	
	1	Шифрование данных в стандарте DES.		
	2	Шифрование данных в ГОСТ 28147-89. Режим простой замены.		
	3	Шифрование данных в ГОСТ 28147-89. Режим гаммирования.		

	4	Шифрование данных в ГОСТ 28147-89. Режим гаммирования с обратной связью.		
	5	Шифрование данных в ГОСТ 28147-89. Режим выработки имитовставки.		
	6	Программирование алгоритма шифрования данных в ГОСТ 28147-89.		
	Самостоятельная работа обучающихся:		9	
	9. Составление блок-схем алгоритмов шифрования данных в ГОСТ 28147-89.			
	10. Составление презентаций, рефератов по темам: - Стандарты шифрования данных. - Алгоритм шифрования данных IDEA. - Блочные и поточные шифры. - Криптосистема с депонированием ключа. - Сеть Файстеля.			
Тема 2.3. Асимметричные криптосистемы.	**Содержание учебного материала**		4	
	1	**Концепция и структура криптосистем с открытым ключом.** Однонаправленные функции.		2
	2	**Криптосистема шифрования данных RSA**: процедуры шифрования и расшифрования, быстродействие и безопасность. Комбинированный метод шифрования.		
	Лабораторные работы (не предусмотрены)			
	Практические занятия:		2	
	1	Шифрование данных в криптосистеме RSA.		
	Самостоятельная работа обучающихся:		3	
	Выполнение индивидуальных заданий по теме.			
	11. Составление презентаций, сообщений по темам: - Схема шифрования Полига-Хеллмана. - Схема шифрования Эль Гамаля.			
Тема 2.4. Идентификация и	**Содержание учебного материала**		4	

проверка подлинности пользователя.	1	**Идентификация и аутентификация пользователя.** Типовые схемы идентификации и аутентификации пользователя. Особенности применения пароля для аутентификации пользователя.		2
	2	**Биометрическая идентификация и аутентификация.** Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний: упрощённая схема идентификации, параллельная схема идентификации.		
	Лабораторные работы (не предусмотрены)			
	Практические занятия: (не предусмотрены)			
	Самостоятельная работа обучающихся:		2	
	12. Составление презентации, сообщения по теме: - Схема идентификации Гиллоу - Куискуотера.			
Тема 2.5. Электронная цифровая подпись.	**Содержание учебного материала**		4	
	1	**Проблемы аутентификации данных и электронная цифровая подпись**. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.		2
	2	**Алгоритмы электронной цифровой подписи**. Алгоритм электронной цифровой подписи RSA. Отечественный стандарт хэш-функции. Отечественный стандарт цифровой подписи.		3
	Лабораторные работы (не предусмотрены)			
	Практические занятия:		4	
	1	Создание сертификатов, удостоверяющих подлинность пользователя. Аутентификация данных.		
	2	Постановка электронной цифровой подписи. Аутентификация данных.		
	Самостоятельная работа обучающихся:			
	Выполнение индивидуальных заданий по теме.		4	
	13. Составление презентации, сообщения по теме: - Закон РФ об электронной цифровой подписи. - Управление криптографическими ключами: генерация, хранение, распределение ключей.			
		Всего:	**105**	

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

1. – 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: 27.04.2021). – Режим доступа: по подписке.

2. Баранова, Е. К. Основы информационной безопасности : учебник / Е. К. Баранова, А. В. Бабаш. - Москва : РИОР : ИНФРА-М, 2021. — 202 с. — (Среднее профессиональное образование). - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1209579 (дата обращения: 27.04.2021). – Режим доступа: по подписке.

3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 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: 19.05.2021). — Режим доступа: для авторизир. пользователей.

Печатные издания

1. Богомазова, Г.Н. Обеспечение информационной безопасности компьютерных сетей: учебник для студ. учреждений сред. проф. образования /Г.Н Богомазова– М.: Издательский центр «Академия, 2017.-224 с.-(Профессиональное образование).-ISBN978-5-4468-3453-2.-Текст :непосредственный.

3.3. Образовательные технологии

3.3.1. В соответствии с ФГОС СПО по специальности **09.02.03 Программирование в компьютерных системах** базовой подготовки в разделе VII. п.7.1. Требования к условиям реализации основной профессиональной образовательной программы указано, что «образовательное учреждение при формировании ОПОП: 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	применять правовые, организационные, технические и программные средства защиты информации	Проверка и оценка выполнения практических работ, оценка домашнего задания, зачет
	создавать программные средства защиты информации.	Проверка и оценка выполнения практических работ, оценка домашнего задания, зачет
	Знания	
	источники возникновения информационных угроз	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, зачет
	модели и принципы защиты информации от несанкционированного доступа;	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, зачет
	методы антивирусной защиты информации	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, зачет
	состав и методы организационно-правовой защиты информации	Тестирование, опрос, оценка выполнения внеаудиторной самостоятельной работы, зачет

5. ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РАБОЧУЮ ПРОГРАММУ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 Информационная безопасность

№ п/п	Содержание внесенных обновлений	Обоснование обновления
1	**Актуализированная литература** 1. – 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: 27.04.2021). – Режим доступа: по подписке. 2. Баранова, Е. К. Основы информационной безопасности : учебник / Е. К. Баранова, А. В. Бабаш. - Москва : РИОР : ИНФРА-М, 2021. — 202 с. — (Среднее профессиональное образование). - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1209579 (дата обращения: 27.04.2021). – Режим доступа: по подписке. 3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html (дата обращения: 19.05.2021). — Режим доступа: для авторизир. пользователей. Печатные издания 1. Богомазова, Г.Н. Обеспечение информационной безопасности компьютерных сетей: учебник для студ. учреждений сред. проф. образования /Г.Н Богомазова– М.: Издательский центр «Академия, 2017.-224 с.-(Профессиональное образование).-ISBN978-5-4468-3453-2.-Текст :непосредственный.	Приказ ГБПОУ СРМК №… от мая 2021года «Об утверждении перечней литературы, используемых при реализации ППССЗ и ППКРС в 2021 -2022 уч. год»