МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
МИНЕРАЛОВОДСКИЙ РЕГИОНАЛЬНЫЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ

УТВЕРЖДАЮ
Директор ГБПОУ МРМК
_____ А.Ф.Цимбалов
«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.12. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

по профессиональной образовательной программе подготовки специалистов среднего звена

09.02.03 Программирование в компьютерных системах

г. Минеральные Воды
2018 г.

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по программе подготовки специалистов среднего звена 09.02.03 Программирование в компьютерных системах (базовой подготовки), утвержденного приказом министерства образования и науки РФ №804 от 28 июня 2014г.

Организация-разработчик: Государственное бюджетное образовательное учреждение среднего профессионального образования «Минераловодский региональный многопрофильный колледж»

Разработчики:
Селютина Ольга Николаевна – преподаватель профессиональных дисциплин
Батищев Виктор Васильевич – преподаватель профессиональных дисциплин

РАССМОТРЕНА И РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ

на заседании методического объединения отделения сервисных технологий

ГБПОУ МРМК, протокол №1 от «30» августа 2018 г.

Руководитель объединения _____

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.11 Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.03. Программное обеспечение компьютерных систем (базовой подготовки).

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: дисциплина входит в общепрофессиональный цикл, вариативная часть.

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

В результате освоения дисциплины обучающийся должен уметь:

применять правовые, организационные, технические и программные средства защиты информации;

создавать модели обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен знать:

основные положения, понятия и определения информационной безопасности;

её место в системе национальной безопасности государства;

источники возникновения информационных угроз; модели и принципы защиты информации от несанкционированного доступа;

методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации.

Результатом освоения дисциплины является овладение обучающимися профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 1.7.	Применять правовые, организационные, технические и программные средства защиты информации
ПК 2.3	Решать вопросы администрирования базы данных.
ПК 2.4.	Реализовывать методы и технологии защиты информации в базах данных.
ПК 3.7	Создавать модели обеспечения информационной безопасности
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	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
ОК 6	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Быть готовым к смене технологий в профессиональной деятельности.

1.4. Количество часов на освоение программы дисциплины:
максимальной учебной нагрузки обучающегося 159 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 106 часов;
самостоятельной работы обучающегося 53 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	*159*
Обязательная аудиторная учебная нагрузка (всего)	*106*
в том числе:	
лабораторные занятия	*Не предусмотрено-*
практические занятия	*54*
контрольные работы	*Не предусмотрено*
курсовая работа (проект) (*если предусмотрено)*	
Самостоятельная работа обучающегося (всего)	*53*
в том числе:	
самостоятельная работа над курсовой работой (проектом) *(если предусмотрено)*	*Не предусмотрено*
Изучение основных свойств информации.	*2*
Выполнение домашнего задания по составлению классификации угроз ИБ	*1*
Рассмотрение особенности обеспечения ИБ РФ в различных сферах общественной жизни.	*2*
Изучение эволюции подходов к обеспечению ИБ	*2*

Классификация методов парирования угроз. Классификация методов нейтрализации угроз	*4*
Рассмотрение модели анализа безопасности программного обеспечения. Изучение моделей анализа безопасности взаимодействия объектов ВС	*4*
Изучение «Европейских критериев» и американских критериев защиты информации	*2*
Изучение ответственности за нарушение законодательства в информационной сфере	*2*
Классификация недостатков запретов процессов обработки информации АСОД и изучение путей их преодоления	*2*
Изучение многоуровневой защиты объектов	*2*
Обзор современных систем оповещения о вторжении. Изучение автоматизированного технического контроля защиты потоков информации	*3*
Изучение история криптографической деятельности. Рассмотрение аспектов документального обеспечения криптографии. Изучение организации протоколирования связи и распределения ключей. Анализ и сравнительная характеристика методов шифрования	*9*
Изучение отдельных аспектов системы разграничения доступа к информации. Изучение рекомендаций при организации парольной защиты	*5*
Изучение документального обеспечения подразделения ОБИ. Составление перечня данных, необходимых при организации подразделения ОБИ.	*4*
Подготовка сообщения об истории возникновения вирусов. Методы удаления последствий воздействия вирусов антивирусными программами	*6*
Изучение аппаратных средств защиты данных в ВС	*3*
Итоговая аттестация в форме экзамена	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование

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.	**Информационная безопасность. Основные положения, понятия, определения**	**21**	
Тема 1.1 Информационная безопасность деятельности общества и её основные положения	**Содержание учебного материала**	2	2
	Основные составляющие национальных интересов РФ в информационной сфере		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Определение ценности и количества информации различными методами		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Изучение основных свойств информации.		
Тема 1.2 Угрозы информационной безопасности	**Содержание учебного материала**	4	2
	Угрозы, основные понятия. Классификация угроз информационной безопасности		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия - не предусмотрены	-	
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся:	1	
	1 Выполнение домашнего задания по составлению классификации угроз ИБ		
Тема 1.3. Комплексное обеспечение информационной безопасности государства	**Содержание учебного материала**	2	2
	Основные положения государственной политики обеспечения ИБ РФ. Основные функции системы обеспечения ИБ РФ и элементы её организационной основы. Источники угроз ИБ РФ.		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Изучение общих методов обеспечения ИБ РФ.		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Рассмотрение особенности обеспечения ИБ РФ в различных сферах общественной жизни.		
Раздел 2.	**Методология обеспечения информационной безопасности общества**	**30**	
Тема 2.1. Области и объекты по обеспечению ИБ и защите информационной деятельности	**Содержание учебного материала**	4	2
	Области и сферы обеспечения ИБ. Объекты защиты информационной деятельности и обеспечения ИБ		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия – не предусмотрены	-	
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Изучение эволюции подходов к обеспечению ИБ		

Тема 2.2 Технология обеспечения безопасности обработки информации	**Содержание учебного материала**	4	2
	Современные подходы к технологиям и методам обеспечения ИБ. Технология предотвращения угроз ИБ		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	4	
	1 Изучение методов и средств парирования угроз		
	2 Изучение методов и средств нейтрализации угроз		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	4	
	1 Классификация методов парирования угроз		
	2 Классификация методов нейтрализации угроз		
Тема 2.3 Модели обеспечения ИБ деятельности фирм и систем	**Содержание учебного материала**	4	2
	Стратегии обеспечения ИБ фирм. Модели безопасности по обеспечению доступа в систему. Модели защиты при отказе в обслуживании.		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	4	
	1 Разработка графической модели системы безопасности с полным перекрытием.		
	2. Разработка модели целостности информации в системе		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	4	
	1 Рассмотрение модели анализа безопасности программного обеспечения		
	2 Изучение моделей анализа безопасности взаимодействия объектов ВС		
Раздел 3	**Организационно-правовое обеспечение информационной безопасности**	**18**	
Тема 3.1. Международные, российские и отраслевые правовые документы	**Содержание учебного материала**	2	2
	Отечественные и международные нормативно-правовые акты обеспечения ИБ. Принципы государственной информационной политики		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Изучение государственных стандартов по защите информации		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Изучение «Европейских критериев» и американских критериев защиты информации		
Тема 3.2. Организационное регулирование защиты процессов переработки информации	**Содержание учебного материала**	2	2
	Категорирование объектов и защита ИС. Основные направления защиты информационной собственности: государственная тайна, коммерческая тайна, банковская тайна. Основные объекты интеллектуальной собственности		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Изучение Закона РФ «О тайне»		
	2 Изучение законов о защите персональных данных		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Изучение ответственности за нарушение законодательства в информационной сфере		

Тема 3.3. Анализ и оценка концепций защиты процессов переработки информации	**Содержание учебного материала**	2	2
	Научные направления защиты информации в автоматизированных системах. Классификация средств защиты информации в АСОД. Аппаратные и программные средства защиты		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Анализ концепций защиты процессов переработки информации		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Классификация недостатков запретов процессов обработки информации АСОД и изучение путей их преодоления		
Раздел 4.	**Техническое и методическое обеспечение ИБ**	**40**	
Тема 4.1 Организационное противодействие технической разведке	**Содержание учебного материала**	2	2
	Системы физической безопасности Модели защиты технических средств и объектов от утечки информации и НСД Средства предупреждения, обнаружения и блокировки случайных воздействий.		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Построение модели защиты объекта от утечки информации		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	2	
	1 Изучение многоуровневой защиты объектов		
Тема 4.2 Методологические основы технического обеспечения защиты процессов переработки информации и контроля её эффективности	**Содержание учебного материала**	4	2
	Системная организация оповещения о попытках вторжения. Основные недостатки технических средств защиты. Система защиты периметра территории. Системы опознавания нарушителя. Механическая защита объекта. Биометрическая идентификация		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Разработка схемы защиты объекта		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	3	
	1 Обзор современных систем оповещения о вторжении.		
	2 Изучение автоматизированного технического контроля защиты потоков информации		
Тема 4.3 Криптографические методы и средства обеспечения ИБ	**Содержание учебного материала**	4	2
	Основные понятия, определения, композиция и синтез шрифтов. Методы шифрования. симметричные и ассиметричные криптосистемы, комбинированные методы шифрования. Программно-аппаратная реализация современных криптографических средств и систем. Стандартизация программно-аппаратных криптографических систем и средств. Ключевые системы разграничения доступа и электронная цифровая подпись.		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	12	
	1 Шифрование с симметричными ключами методом перестановки		
	2 Шифрование с симметричными ключами методом подстановки		

	3	Расшифровка с симметричными ключами		
	4	Шифрование с симметричными ключами при помощи аналитических преобразований		
	5	Шифрование аддитивными методами (гаммирование)		
	6	Шифрование с открытым ключом		
	Контрольные работы – не предусмотрены		-	
	Самостоятельная работа обучающихся		9	
	1	Изучение история криптографической деятельности		
	2	Рассмотрение аспектов документального обеспечения криптографии		
	3	Изучение организации протоколирования связи и распределения ключей		
	4	Анализ и сравнительная характеристика методов шифрования		
Раздел 5.	**Программно-аппаратные средства обеспечения ИБ**		**54**	
Тема 5.1. Программно-аппаратные средства защиты ПЭВМ	**Содержание учебного материала**		4	2
	Методы и средства ограничения доступа к компонентам ЭВМ: доступ к оборудованию, идентификация субъекта доступа, идентификация пользователей, система разграничения доступа, Противодействие несанкционированному подключению устройств к КС .Способы, затрудняющие считывание информации, препятствующие использованию скопированной информации			
	Лабораторные работы – не предусмотрены		-	
	Практические занятия		6	
	1	Изучение организации диспетчера доступа		
	2	Изучение способов защиты от дизассемблирования		
	3	Изучение способов защиты от трассировки		
	Контрольные работы – не предусмотрены		-	
	Самостоятельная работа обучающихся		5	
	1	Изучение отдельных аспектов системы разграничения доступа к информации.		
	2	Изучение рекомендаций при организации парольной защиты		
Тема 5.2. Методы и средства обеспечения хранения и переработки ключевой и другой информации	**Содержание учебного материала**		2	2
	Организационные мероприятия защиты процессов обработки информации: защитные, эксплуатационные			
	Лабораторные работы – не предусмотрены		-	
	Практические занятия		6	
	1	Проектирование подразделения ОБИ		
	2	Изучение законов о защите персональных данных»		
	3	Планирование эксплуатационных мероприятий защиты процессов хранения информации		
	Контрольные работы – не предусмотрены		-	
	Самостоятельная работа обучающихся		4	
	1	Изучение документального обеспечения подразделения ОБИ		
	2	Составление перечня данных, необходимых при организации подразделения ОБИ		
Тема 5.3 Защита программного обеспечения от	**Содержание учебного материала**		6	2
	Основные классификационные признаки компьютерных вирусов. Алгоритмы функционирования вирусов.. «Стелс»-вирусы, полиморфные вирусы. Способы заражения файловыми вирусами, алгоритм заражения файлов. Загрузочные вирусы. Методы и технологии борьбы с компьютерными вирусами. Условия безопасной работы КС и технология			

изучения, вирусного заражения, разрушающих программных действий	обнаружения заражения вирусами. Контроль целостности и системные вопросы защиты программ и данных		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	6	
	1 Изучение способов внедрения вирусов в файлы		
	2 Изучение особенностей работы загрузочных вирусов		
	3 Решение задачи выявления заражения вирусами		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	6	
	1 Подготовка сообщения об истории возникновения вирусов		
	2 Методы удаления последствий воздействия вирусов антивирусными программами		
Тема 5.4. Программно-аппаратные средства обеспечения ИБ в вычислительных сетях	**Содержание учебного материала**	4	2
	Основные положения программно-аппаратного и организационного обеспечения ИБ в ОС. Защита процессов обработки информации в СУБД. Программно-аппаратные средства обеспечения ИБ в ВС		
	Лабораторные работы – не предусмотрены	-	
	Практические занятия	2	
	1 Изучение работы межсетевых экранов		
	Контрольные работы – не предусмотрены	-	
	Самостоятельная работа обучающихся	3	
	1 Изучение аппаратных средств защиты данных в ВС		
	Дифференцированный зачет	2	
Всего		**159**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины предполагает наличие учебного кабинета; лаборатории системного и прикладного программирования.

Оборудование учебного кабинета:

- автоматизированное рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- плакаты, таблицы, схемы;
- стенды, макеты.

Технические средства обучения: компьютер с лицензионным программным обеспечением, мультимедиапроектор и интерактивная доска.

Оборудование лаборатории системного и прикладного программирования:

- автоматизированное рабочее место преподавателя;
- автоматизированное рабочие места обучающихся (по количеству обучающихся);
- локальная сеть, выход в глобальную сеть;
- сетевое периферийное оборудование;
- периферийное оборудование для ввода и вывода информации;
- мультимедийное оборудование
- комплект учебно-методической документации.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Мельников В.П., Клейменов С.А., Петраков А.М.под ред. С.А. Клейменова Информационная безопасность: учеб. пособие для студ. учреждений сред. проф. образования - М.: Издательский центр «Академия», 2016

Дополнительные источники:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ИД «Форум»: ИНФРА-М, 2013
2. ГОСТ Р.34.10 – 94. Информационная технология. Криптографическая защита информации. Процедуры выработки проверки электронной цифровой подписи на базе ассиметричного цифрового алгоритма.
3. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646) Система ГАРАНТ: http://base.garant.ru/71556224/#ixzz4vF4ICQkO
4. Закон РФ «О государственной тайне» от 21.07.93 №5485-1

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, подготовки сообщений по теоретическим вопросам.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Уметь:	
применять правовые, организационные, технические и программные средства защиты информации;	Проверка выполнения практических работ, решение проблемных задач,
создавать модели обеспечения информационной безопасности	тестирование, проверка выполнения практических работ, решение проблемных задач
Знать:	
основные положения, понятия и определения информационной безопасности;	проверка выполнения домашних заданий, выполнения индивидуальных заданий,
место информационной безопасности в системе национальной безопасности государства;	тестирование, защита практических работ, проверка выполнения домашних заданий
источники возникновения информационных угроз; модели и принципы защиты информации от несанкционированного доступа;	тестирование, проверка выполнения практических работ, проверка выполнения домашних заданий
методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации	тестирование, проверка выполнения практических работ, проверка выполнения домашних заданий.
	Итоговый контроль – экзамен