Министерство образования Ставропольского края

Государственное бюджетное профессиональное образовательное учреждение
«Светлоградский региональный сельскохозяйственный колледж»

УТВЕРЖДАЮ:
Директор ГБПОУ СРСК
А.Д. Шаповалов

_____

ПРОГРАММА ОБЩЕПРОФЕССИОНАЛЬНОЙ ДИСЦИПЛИНЫ

ОП.13 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

09.02.03 «Программирование в компьютерных системах»

2020 г.

РАЗРАБОТЧИК
Преподаватель

_____ О.В. Остапенко

ОДОБРЕНА
методической комиссией «Экономика и информационные технологии»
Протокол №11 от 29.06.2020 г.
Председатель МК

_____ Е.А. Алейникова

СОГЛАСОВАНО
Зав.метод.отдела

_____ М.С. Терещенко

Программа ОП.13 «Информационная безопасность» рекомендована Методическим советом государственного бюджетного профессионального образовательного учреждения «Светлоградский региональный сельскохозяйственный колледж»

Заключение Методического совета №11 от 30.06.2020 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Программа учебной дисциплины «**Информационная безопасность**» предназначена для изучения технических средств информатизации в учреждениях среднего профессионального образования, реализующих образовательную программу среднего (полного) общего образования для специальности **09.02.03 Программирование в компьютерных системах,** входящей в укрупнённую группу 09.00.00 Информатика и вычислительная техника.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Информационная безопасность» входит профессиональный цикл.

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

В результате освоения учебной дисциплины обучающийся должен

уметь:

- организовывать и проводить мероприятия по защите работников и населения от негативных воздействий чрезвычайных ситуаций;
- предпринимать профилактические меры для снижения уровня опасностей различного вида и их последствий в профессиональной деятельности и быту;
- использовать средства индивидуальной и коллективной защиты от оружия массового поражения;
- применять первичные средства пожаротушения;
- ориентироваться в перечне военно-учетных специальностей и самостоятельно определять среди них родственные полученной специальности;
- применять профессиональные знания в ходе исполнения обязанностей военной службы на воинских должностях в соответствии с полученной специальностью;
- владеть способами бесконфликтного общения и саморегуляции в повседневной деятельности и экстремальных условиях военной службы;
- оказывать первую помощь пострадавшим;

знать:

- принципы обеспечения устойчивости объектов экономики, прогнозирования развития событий и оценки последствий при техногенных чрезвычайных ситуациях и стихийных явлениях, в том

числе в условиях противодействия терроризму как серьезной угрозе национальной безопасности России;
- основные виды потенциальных опасностей и их последствия в профессиональной деятельности и быту, принципы снижения вероятности их реализации;
- основы военной службы и обороны государства;
- задачи и основные мероприятия гражданской обороны;
- способы защиты населения от оружия массового поражения;
- меры пожарной безопасности и правила безопасного поведения при пожарах;
- организацию и порядок призыва граждан на военную службу и поступления на нее в добровольном порядке;
- основные виды вооружения, военной техники и специального снаряжения, состоящие на вооружении (оснащении) воинских подразделений, в которых имеются военно-учетные специальности, родственные специальностям СПО;
- область применения получаемых профессиональных знаний при исполнении обязанностей военной службы;
- порядок и правила оказания первой помощи пострадавшим.

В результате освоения дисциплины формируются компетенции:

общие:

Код	Наименование результата обучения
ПК 1.1.	Выполнять разработку спецификаций отдельных компонент.
ПК 1.2.	Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.
ПК 1.3.	Выполнять отладку программных модулей с использованием специализированных программный средств.
ПК 1.4.	Выполнять тестирование программных модулей.
ПК 1.5.	Осуществлять оптимизацию программного кода модуля.
ПК 1.6.	Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.
ПК 2.1.	Разрабатывать объекты базы данных.
ПК 2.2.	Реализовывать базу данных в конкретной СУБД.
ПК 2.3.	Решать вопросы администрирования базы данных.
ПК 2.4.	Реализовывать методы и технологии защиты информации в базах данных.
ПК 3.1.	Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.
ПК 3.2.	Выполнять интеграцию модулей в программную систему.
ПК 3.3.	Выполнять отладку программного продукта с использованием специализированных программных средств.
ПК 3.4.	Осуществлять разработку тестовых наборов и тестовых сценариев.
ПК 3.5.	Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.
ПК 3.6.	Разрабатывать технологическую документацию.

ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые 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), 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.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 105 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 70 часа;

самостоятельной работы обучающегося 35 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «Информационная безопасность»

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 *предусмотрено)*	-
практические занятия	36
контрольные работы	-
Зачёт	2
курсовая работа (проект) (не *предусмотрено)*	-
Самостоятельная работа обучающегося (всего)	35
в том числе:	
Повторение пройденного материала Конспектирование Подготовка доклада Работа с дополнительной литературой Подготовка к контрольной работе Подготовка к зачету	
Итоговая аттестация в форме: дифференцированный зачёт	

2.2. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения	Освоение компетенций
1	2	3	4	5
Раздел 1.	**Информационная безопасность и уровни ее обеспечения**	**42**		
Тема 1.1. Понятие "информационная безопасность"	**Содержание учебного материала**			
	1. различные подходы к определению понятия "информационная безопасность", составляющие понятия "информационная безопасность", определение целостности, конфиденциальности и доступности информации, задачи информационной безопасности, уровни формирования режима информационной безопасности.	1	1	
	2. составляющие понятия "информационная безопасность", определение целостности информации, определения конфиденциальности и доступности информации.	1	2	
	Практических и лабораторных работ (не предусмотрено)			
	Самостоятельная работа Повторение пройденного материала	2		
Тема 1.2. Система формирования режима информационной безопасности	**Содержание учебного материала**			
	1. задачи информационной безопасности, уровни формирования режима информационной безопасности, особенности законодательно-правового и административного уровней, подуровни программно-технического уровня.	2	2	
	Практическое занятие			
	1. распределять задачи информационной безопасности по уровням ее обеспечения	2	2	
Тема 1.3. Нормативно-правовые основы информационной безопасности в РФ и стандарты информационной безопасности	**Содержание учебного материала**			
	1. нормативно-правовые основы информационной безопасности общества; основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации, ответственность за нарушения в сфере информационной безопасности.	2	2	
	2. основное содержание оценочного стандарта ISO/IEC 15408,отличия функциональных требований от требований доверия, классы функциональных требований и требований доверия.	2	2	
	Практическое занятие			
	1. Законодательство РФ в области информационной безопасности	2		

	2.	Изучение положения о сертификации средств вычислительной техники и связи	2		
	Самостоятельная работа Подготовка доклада		10		
Тема 1.4. Стандарты информационной безопасности распределенных систем РФ	**Содержание учебного материала**				
	1.	основное содержание стандартов по информационной безопасности распределенных систем, основные сервисы безопасности в вычислительных сетях, наиболее эффективные механизмы безопасности, задачи администрирования средств безопасности.	1	2	
	2.	роли Гостехкомиссии в обеспечении информационной безопасности в РФ, документы по оценке защищенности автоматизированных систем в РФ.	1		
	Практических и лабораторных работ (не предусмотрено)				
Тема 1.5. Административный уровень обеспечения информационной безопасности	**Содержание учебного материала**				
	1.	цели и задачи административного уровня обеспечения информационной безопасности, содержание административного уровня, направления разработки политики безопасности	2	2	
	Практическое занятие				
	1.	определять политику безопасности организации, Конституция Российской Федерации, доктрина информационной безопасности Российской Федерации, федеральные законы в области информации и информационной безопасности, указы президента РФ и постановления правительства РФ в области информации и информационной безопасности, правовые режимы защиты информации.	4	2	
Тема 1.6. Классификация угроз "информационной безопасности"	**Содержание учебного материала**				
	1.	классы угроз информационной безопасности, причины и источники случайных воздействий на информационные системы, каналы несанкционированного доступа к информации	2	1	
	Практическое занятие			2	
	1.	выявлять и классифицировать угрозы информационной безопасности	4		
	Самостоятельная работа Повторение пройденного материала		2		
Раздел 2.	**Компьютерные вирусы и защита от них.**		**17**		
Тема 2.1. Классификация компьютерных вирусов	**Содержание учебного материала**				
	1.	характерные черты компьютерных вирусов, проблемы при определении компьютерного вируса.	1	1	
	2.	классы компьютерных вирусов, характеристику различных компьютерных вирусов	1	2	
	3.	виды "вирусоподобных" программ, деструктивные возможности	1		

		"вирусоподобных" программ.			
	4.	виды антивирусных программ, принципы функционирования антивирусных программ, факторы, определяющие качество антивирусной программы.	1		
	Практических и лабораторных работ (не предусмотрено)				
	Самостоятельная работа Конспектирование		2		
Тема 2.2. Профилактика компьютерных вирусов и обнаружение неизвестного вируса	**Содержание учебного материала**				
	1.	наиболее распространенные пути заражения компьютеров вирусами, правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей	1	2	
	2.	общий алгоритм обнаружения неизвестного вируса.	1		
	Практическое занятие				
	1.	проводить профилактику компьютерных вирусов.	2	1	
	2.	проверить систему на наличие макровируса	2		
	Самостоятельная работа Подготовка к контрольной работе		5		
Раздел 3.	**Информационная безопасность вычислительных сетей**		**26**		
Тема 3.1. Особенности обеспечения информационной безопасности в компьютерных сетях	**Содержание учебного материала**				
	1.	особенности обеспечения информационной безопасности компьютерных сетей, основные цели информационной безопасности компьютерных сетей, специфику методов и средств защиты компьютерных сетей.	1	2	
	2.	теоретические основы построения компьютерных сетей, протоколы передачи данных.	1		
	Практических и лабораторных работ (не предусмотрено)				
Тема 3.2. Модель взаимодействия открытых систем OSI/ISO	**Содержание учебного материала**				
	1.	структура модели открытых систем OSI/ISO и назначение ее уровней	2	3	
	Практическое занятие				
	1.	использовать модель OSI/ISO для описания процесса передачи данных между узлами компьютерной сети.	4	1	
Тема 3.3. Адресация в глобальных сетях	**Содержание учебного материала**				
	1.	принципы адресации в современных вычислительных сетях, классы адресов протокола IP и структуру IP-адреса, иерархический принцип системы доменных имен	2	2	
	Практическое занятие				
	1.	преобразовывать двоичный IP-адрес в десятичный, определять тип сети по IP-адресу.	4	2	

Тема 3.4. Классификация удаленных угроз в вычислительных сетях	**Содержание учебного материала**				
	1.	классы удаленных угроз и их характеристику.	1	2	
	2.	типовые удаленные атаки и механизмы их реализации.	1		
	Практическое занятие				
	1.	классифицировать типовые удаленные атаки по совокупности признаков.	4	2	
	Самостоятельная работа Работа с дополнительной литературой		4		
Тема 3.5. Причины защиты и успешной реализации удаленных угроз в вычислительных сетях	**Содержание учебного материала**				
	1.	принципы защиты распределенных вычислительных сетей.	1	2	
	2.	причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.	1	1	
	Практических и лабораторных работ (не предусмотрено)				
Раздел 4.	**Механизмы обеспечения "информационной безопасности"**		**20**		
Тема 4.1. Идентификация, аутентификация, криптография и шифрование	**Содержание учебного материала**				
	1.	механизмы идентификации и аутентификации, идентификаторы, используемые при реализации механизма идентификации и аутентификации.	1	1	
	2.	структуру криптосистемы, методы шифрования данных.	1	1	
	Практическое занятие				
	1.	структуру криптосистемы, методы шифрования данных.	2		
Тема 4.2. Методы разграничение доступа. Регистрация и аудит.	**Содержание учебного материала**				
	1.	методы разграничения доступа, методы управления доступом, предусмотренные в руководящих документах Гостехкомиссии.	1	2	
	2.	защитные свойства механизма регистрации и аудита, методы аудита безопасности информационных систем.	1	2	
	Практическое занятие				
	1.	использовать механизмы регистрации и аудита для анализа защищенности системы.	2	3	
	Самостоятельная работа Подготовка к зачету		10		
	Дифференцированный зачет		2	2	
		Всего:	105		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории «технические средства информатизации»;

Оборудование лаборатории и рабочих мест лаборатории технические средства информатизации:

- автоматизированные рабочие места обучающихся;
- автоматизированное рабочее место преподавателя;
- комплект учебно-методической документации;
- источники бесперебойного питания;
- внешние накопители информации;

Технические средства обучения:

- оборудование электропитания;
- серверное оборудование;
- коммутируемое оборудование;
- мультимедийное оборудование;
- источники бесперебойного питания;
- интерактивная доска;
- проектор;
- сканер;
- аудиосистема;
- внешние накопители информации;
- мобильные устройства для хранения информации;
- локальная сеть;
- подключение к глобальной сети Интернет.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Мельников В.П., Куприянов А.И. Информационная безопасность. (СПО). Учебник. 2020. https://www.book.ru/view5/677c4d5762ccaf88b11a51af6f5586cd
2. Бубнов А.А., В.Н. Пржегорлинский, О.А. Савинкин Основы информационной безопасности. Учебник Москва «Академия» 2018 г.

Дополнительные источники:

1. Михеева Е.В. Информатика. Практикум (2-е изд., стер.) учеб. Пособие– Москва «Академия» 2018 г
2. Крылов Г.О., Ларионова С.Л., Никитина В.Л. Базовые понятия информационной безопасности Русайнс 2020 https://www.book.ru/book/932492
3. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум (для бакалавров) Электронные приложения на сайте www.book.ru КноРус 2020 https://www.book.ru/view5/b287a41e6d7c7c27681c35893dad500f

Интернет-ресурсы:

1) Компьютер своими руками [Электронный ресурс]. - Режим доступа: http://ruslan-m.com, свободный.
2) Лошаков, С. Периферийные устройства вычислительной техники [Электронный ресурс]: учебное пособие/С.Лошаков. - М.: Интернет-Университет информационных технологий (ИНТУИТ), 2013. - Режим доступа: http://old.intuit.ru/department/hardware/perdevcom/, свободный.
3) Ремонт, настройка и модернизация компьютера [Электронный ресурс]. - Режим доступа: http://www.remont-nastroyka-pc.ru/, свободный.
4) Собираем компьютер своими руками [Электронный ресурс]. - Режим доступа: http://www.svkcomp.ru/, свободный.
5) Сперанский, Д.В. Моделирование, тестирование и диагностика цифровых устройств [Электронный ресурс]: учебное пособие/Д.В. Сперанский, Ю.А. Скобцов, В.Ю. Скобцов. - М.: Интернет-Университет информационных технологий (ИНТУИТ), 2012. - Режим доступа: http://old.intuit.ru/department/hardware/mtddig/, свободный.

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 умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Уметь:	
Организовывать и проводить мероприятия по защите работников и населения от негативных воздействий чрезвычайных ситуаций	Оценка качества выполненных практических заданий.
Предпринимать профилактические меры для снижения уровня опасностей различного вида и их последствий в профессиональной деятельности и быту	Оценка качества выполненных практических заданий.
Использовать средства индивидуальной и коллективной защиты от оружия массового поражения	Оценка качества выполненных практических заданий
Применять первичные средства пожаротушения	Оценка качества выполненных практических заданий
Ориентироваться в перечне военно-учетных специальностей и самостоятельно определять среди них родственные полученной специальности	Оценка качества выполненных практических заданий
Применять профессиональные знания в ходе исполнения обязанностей военной службы на воинских должностях в соответствии с полученной специальностью	Оценка качества выполненных практических заданий
Владеть способами бесконфликтного общения и саморегуляции в повседневной деятельности и экстремальных условиях военной службы	Оценка качества выполненных практических заданий
Оказывать первую помощь пострадавшим	Оценка качества выполненных практических заданий
Знать:	
Принципы обеспечения устойчивости объектов экономики, прогнозирования развития событий и оценки последствий при техногенных чрезвычайных ситуациях и стихийных явлениях, в	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа

том числе в условиях противодействия терроризму как серьезной угрозе национальной безопасности России;	
Основные виды потенциальных опасностей и их последствия в профессиональной деятельности и быту, принципы снижения вероятности их реализации;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Основы военной службы и обороны государства;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Задачи и основные мероприятия гражданской обороны;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Способы защиты населения от оружия массового поражения;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Меры пожарной безопасности и правила безопасного поведения при пожарах;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Организацию и порядок призыва граждан на военную службу и поступления на нее в добровольном порядке;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Основные виды вооружения, военной техники и специального снаряжения, состоящие на вооружении (оснащении) воинских подразделений, в которых имеются военно-учетные специальности, родственные специальностям СПО;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Область применения получаемых профессиональных знаний при исполнении обязанностей военной службы;	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа
Порядок и правила оказания первой помощи пострадавшим.	тест, фронтальный опрос, собеседование, внеаудиторная самостоятельная работа