


**Министерство сельского хозяйства Российской Федерации  
федеральное государственное, бюджетное образовательное учреждение  
высшего образования «Дагестанский государственный аграрный  
университет имени М.М. Джамбулатова»  
Аграрно-экономический техникум**



Утверждаю:

Первый проректор

 М.Д. Мукайлов

«26» марта 2024 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**«ОП.ДЭ.01.02 Информационная безопасность»**

**для специальности:**

**«09.02.07 Информационные системы и программирование»**

**Форма обучения – очная**

*Срок обучения СПО по ППССЗ – 3 з 10 м*

**Махачкала 2024г**

Рабочая программа дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности (профессии) среднего профессионального образования для специальности **09.02.07 «Информационные системы и программирование»**, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1547.

Организация-разработчик: ФГБОУ ВО «Дагестанский государственный аграрный университет имени М.М. Джамбулатова» Аграрно-экономический техникум.

Разработчик:



**Х.Х.Гитинов**

**СОГЛАСОВАНО:**



Директор АЭТ

подпись

Магомедов Д.А.

Одобрено на заседании ПЦК  
Общепрофессиональных и  
Специальных дисциплин  
по специальности 09.02.07  
«Информационные системы и  
программирование»  
«11» марта 2024г., протокол № 7

Председатель ПЦК



Рабданова З.К.

**СОГЛАСОВАНО:**

Директор Компании Color- IT, Интернет решения



Салихов А.Б.

Ф.И.О.

## СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр 3
2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ	9
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	11

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

**1.1. Место учебной дисциплины в структуре основной профессиональной образовательной программы:** учебная дисциплина относится к общепрофессиональному циклу, связана с освоением профессиональных компетенций по всем профессиональным модулям, входящим в специальность.

**1.2. Цель и планируемые результаты освоения учебной дисциплины:**

ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
<b>Обязательные аудиторные учебные занятия (всего)</b>	108
в том числе:	
– теоретические занятия	
– практические занятия	
– контрольные работы	
<b>Самостоятельная работа (всего)</b>	
в том числе:	
– работа с конспектами лекций при подготовке к контрольной работе – составление схемы – составление таблицы	
Промежуточная АТТЕСТАЦИЯ в форме дифференцированного зачёта	

**2.2. Тематический план и содержание учебной дисциплины «ОП.ДЭ.01.02 Информационная безопасность»**

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	
<b>ВВЕДЕНИЕ</b>	<b>Содержание учебного материала</b>	1	ОК 01,ОК 04,ОК 05, ОК 09
	Понятие внешней и внутренней опасности для программ и данных. Цель и назначение учебной дисциплины		
<b>РАЗДЕЛ 1 ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>		<b>9</b>	
Тема 1.1 Основные понятия и анализ угроз информационной безопасности	<b>Содержание учебного материала</b>	1	ОК 01,ОК 04,ОК 05, ОК 09
	Основные понятия и анализ угроз информационной безопасности		
	<b>Самостоятельная работа во взаимодействии с преподавателем</b>	2	
	<b>СР</b> Изучение методов реализации угроз информационной безопасности		
	<b>СР</b> Анализ угроз и уязвимости беспроводных сетей		
	<b>Практические занятия – не предусмотрены</b>		
	<b>Самостоятельная работа студентов</b>		
	Составить и заполнить схему реализации угроз информационной безопасности		
Тема 1.2. Политика безопасности и стандарты информационной безопасности	<b>Содержание учебного материала</b>	2	ОК 01,ОК 04,ОК 05, ОК 09
	Основные понятия политики безопасности		
	Структура политики безопасности организации		
	Международные стандарты информационной безопасности		
	Отечественные стандарты информационной безопасности		
	<b>Самостоятельная работа во взаимодействии с преподавателем</b>	1	
	<b>СР</b> Изучение процедур безопасности		
	<b>Практические занятия</b>		
	<b>ПЗ 1</b> Использование баз данных для изучения нормативных документов в области информационной безопасности.	2	
	<b>Самостоятельная работа студентов</b>		
	Составить обобщенную таблицу систематизации международных стандартов информационной безопасности		

	Контрольная работа №1	1		
РАЗДЕЛ 2 ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ		16		
Тема 2.1. Принципы криптографической защиты информации	Содержание учебного материала	1	ОК 01,ОК 04,ОК 05, ОК 09	
	Симметричные криптосистемы шифрования			
	Асимметричные криптосистемы шифрования			
	Комбинированная криптосистема шифрования			
	Электронная цифровая подпись и функции хеширования			
	Управление криптоключами			
	Самостоятельная работа во взаимодействии с преподавателем	1		
	СР Возможности использования функций хеширования			
	Практические занятия	8		
	ПЗ 2 Реализация логирования на Python			
	ПЗ 3 Шифрование и дешифрование с использованием симметричного алгоритма			
	ПЗ 4 Шифрование RSA Cipher			
	ПЗ 5 Использование методов с открытым ключом			
Самостоятельная работа студентов				
Составить БСА транспозиции				
Тема 2.2. Технологии аутентификации	Содержание учебного материала	2		
	Аутентификация, авторизация и администрирование действий пользователей			
	Методы аутентификации, использующие пароли и PIN-коды			
	Строгая аутентификация			
	Биометрическая аутентификация пользователя			
	Самостоятельная работа во взаимодействии с преподавателем	1		
	СР Использование биометрической аутентификации при шифровании			
	Практические занятия	2		
	ПЗ 6 Реализация аутентификации средствами Python			
	Самостоятельная работа студентов			
	Установить на компьютере библиотеку Cryptography			
	Контрольная работа №2	1		

РАЗДЕЛ 3 ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ		13	
Тема 3.1. Анализ защищенности и обнаружение атак	<i>Содержание учебного материала</i>	1	ОК 01,ОК 04,ОК 05, ОК 09
	Концепция адаптивного управления безопасностью		
	Технологии анализа защищённости		
	Технологии обнаружения атак		
	<i>Самостоятельная работа во взаимодействии с преподавателем</i>	1	
	<i>СР Систематизация средств анализа защищенности ОС</i>		
	<i>Практические занятия</i>	2	
	<b>ПЗ 7</b> Обеспечение безопасности приложения		
	<i>Самостоятельная работа студентов</i>		
	Составить классификационную схему мер обеспечения безопасности приложения		
Тема 3.2. Защита от вирусов	<i>Содержание учебного материала</i>	4	
	Компьютерные вирусы и проблемы антивирусной защиты		
	Антивирусные программы и комплексы		
	Построение системы антивирусной защиты		
	<i>Самостоятельная работа во взаимодействии с преподавателем</i>	1	
	<i>СР Анализ основных каналов распространения вирусов</i>		
	<i>Практические занятия</i>	2	
	<b>ПЗ 8</b> Изучение настроек средств антивирусной защиты информации		
	<i>Самостоятельная работа студентов</i>		
	Изучить алгоритм работы вируса		
	<b>Контрольная работа №3</b>	1	
	<b>Промежуточная аттестация в форме дифференцированного зачёта</b>		1
<b>ВСЕГО:</b>		<b>108</b>	



### 3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

#### *3.1. Материально-техническое обеспечение*

Реализация программы предполагает наличие лаборатории Товароведения продовольственных товаров.

*Оборудование лаборатории и рабочих мест:*

- Автоматизированные рабочие места на 12-15 обучающихся (Процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;)
- Автоматизированное рабочее место преподавателя (Процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;)
- Многофункциональное устройство (МФУ) формата А4;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения (программное обеспечение: БД Консультант плюс, OpenSSL, TrueCrypt, ImageSpy, OpenVPN, MS Office, демоверсии VipNet client, SecretNet)

### 3.2. Информационное обеспечение обучения

*Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы*

#### ОСНОВНЫЕ ИСТОЧНИКИ:

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/385082>
2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для спо / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 96 с. — ISBN 978-5-507-50317-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/417899>

1. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 96 с. — ISBN 978-5-8114-7907-8. — Текст : электронный

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
<b>У1</b> Использовать современные программно-аппаратные средства защиты информации <b>У2</b> Подобрать и обеспечить защиту информации	<i>Правильность, полнота выполнения заданий, точность формулировок, точность расчетов, соответствие требованиям</i>  <i>Адекватность, оптимальность выбора способов действий, методов, техник, последовательностей действий и т.д.</i> <i>Точность оценки</i> <i>Соответствие требованиям инструкций, регламентов</i> <i>Рациональность действий и т.д.</i>	<b>Текущий контроль:</b> - защита отчетов по практическим занятиям; - оценка заданий для внеаудиторной (самостоятельной) работы  - экспертная оценка демонстрируемых умений, выполняемых действий в процессе практических занятий <b>Промежуточная аттестация</b> - экспертная оценка выполнения практических занятий на дифференцированном зачете

<p><b>31</b> Современные законы, стандарты, методы и технологии в области защиты информации</p> <p><b>32</b> Требования к защите информации определенного типа</p>	<p><i>Полнота ответов, точность формулировок, не менее 70% правильных ответов.</i></p> <p><i>Не менее 75% правильных ответов.</i></p> <p><i>Актуальность темы, адекватность результатов поставленным целям, полнота ответов, точность формулировок, адекватность применения профессиональной терминологии</i></p>	<p><b>Текущий контроль при проведении:</b></p> <p><i>-письменного/устного опроса;</i></p> <p><i>-тестирования;</i></p> <p><i>-оценки результатов внеаудиторной (самостоятельной) работы (сообщений теоретической части проектов, учебных исследований и т.д.</i></p> <p><b>Промежуточная аттестация</b></p> <p><i>в форме дифференцированного зачёта по учебной дисциплине</i></p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------