

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



Утверждаю:
Врио проректора
по учебной работе и ДО
Ш.Ш.Омариев
«30» апреля 2026 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

**для специальности:
09.02.11 «Разработка и управление программным
обеспечением»**

Форма обучения – очная

Срок обучения СПО по ППССЗ – 3 г.10 м.

Махачкала 2026 г.

Рабочая программа дисциплины **ОП.05 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»** разработана на основе Федерального государственного образовательного стандарта по специальности (профессии) среднего профессионального образования для специальности **09.02.11 «Разработка и управление программным обеспечением»**.

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

Разработчик:



Х.Х. Гитинов

Одобрено на заседании ПЦК
Общепрофессиональных и
специальных дисциплин по специальности
09.02.11 «Разработка и управление
программным обеспечением»
«30» апреля 2026 г., протокол № 8

Председатель ПЦК



Рабданова З.К.

СОГЛАСОВАНО:



Директор АЭТ

подпись

Магомедов Д.А.

СОГЛАСОВАНО:

Директор Компании Color- IT, Интернет решения



Салихов А.Б.

Ф.И.О.

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Программа учебной дисциплины является частью основной профессиональной образовательной программы по специальности СПО 09.02.11 Разработка и управление программным обеспечением.

1.2. Место учебной дисциплины в структуре основной профессиональной программы: дисциплина «Основы информационной безопасности» относится к дисциплинам Общепрофессионального цикла.

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

В результате изучения обязательной части цикла обучающийся должен:

уметь:

- применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;
- точно описывать угрозу и документировать решение проблемы;
- выбирать меры защиты информации для автоматизированного рабочего места;
- осуществлять поиск информации в открытых источниках и работать с технической документацией;
- читать или разрабатывать документацию к существующей или проектируемой информационной структуре предприятия
- классифицировать основные угрозы безопасности информации;
- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- выявлять информационные угрозы;
- анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации,
- сопровождения механизмов информационной безопасности.;

знать:

- методы планирования своей работы;
- методы и приемы, используемые для недопущения/устранения угроз информационной безопасности
- методы и средства сбора информации и ее хранения;
- средства управления, связанные с использованием, обработкой, хранением и передачей данных;
- законодательство в области информационной безопасности;

- отраслевые стандарты и системы профессиональных сертификаций;
- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности.

Полученные знания и приобретенные умения направлены на формирование следующих компетенций: ОК 01.; ОК 02.

1.4. Количество часов на освоение программы учебной дисциплины:

Объем ОП- 106 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 104 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы	106
в том числе:	
теоретическое обучение	48
практические занятия	56
Промежуточная аттестация в форме дифференцированного зачета	2

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Теоретические основы информационной безопасности			12	ОК 01, ОК 02
Тема 1.1 Основные понятия и задачи информационной безопасности	Содержание учебного материала		4	
	1	Введение в дисциплину. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2	
	2	Понятия компонента, класса и семейства	1	
	3	Объективно-ориентированный подход к информационной безопасности	1	
Тема 1.2 Нормативно-правовое регулирование защиты информации	Содержание учебного материала		4	
	1	Российское законодательство в области информационной безопасности	1	
	2	Зарубежное законодательство в области информационной безопасности	1	
	3	Информационная безопасность распределенных систем. Администрирование средств безопасности	1	
Тема 1.3 Классификация безопасности	Содержание учебного материала		2	
	1	Основные понятия и механизмы информационной безопасности	1	
	2	Классы безопасности	1	
Тема 1.4 Документооборот, как способ защиты информации	Содержание учебного материала		2	
	1	Правила и порядок оформления документов	1	
	2	Документооборот и его организация	1	
Раздел 2. Методология защиты информации			36	
Тема 2.1 Угрозы безопасности защиты информации и основы защиты информации	Содержание учебного материала		36	
	1	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Угрозы информационной безопасности	2	
	2	Способы защиты информации Аппаратные и программные средства обеспечения безопасности государства	1	
	3	Защита от информационных утечек	1	
	4	Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи	1	
	5	Защита информации, содержащей коммерческую, государственную и иные виды тайн	1	
Тема2.2 Методологические подходы к защите информации	Содержание учебного материала		30	
	1	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	1	
	2	Виды мер и основные принципы защиты информации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	1	

Практические работы:		28	
№1	Порядок и оформление документов, документооборот	2	
№2	Порядок и оформление документов, документооборот	2	
№3	Определение объектов защиты на типовом объекте информатизации.	2	
№4	Определение объектов защиты на типовом объекте информатизации.	2	
№5	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2	
№6	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2	
№7	Определение угроз объекта информатизации и их классификация	2	
№8	Определение угроз объекта информатизации и их классификация	2	
№9	Антивирусные программ и их использование.	2	
№10	Антивирусные программ и их использование	2	
№11	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2	
№12	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2	
№13	Выбор мер защиты информации для автоматизированного рабочего места	2	
№14	Выбор мер защиты информации для автоматизированного рабочего места	2	
Дифференцированный зачет		2	
ВСЕГО		106	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Основ информационной безопасности»:

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.
- компьютер с лицензионным программным обеспечением;
- мультимедиапроектор.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

3.2.1. Печатные издания

1. Самойлов В.В. «Основы информационной безопасности: учебник для СПО» Москва: Академия, 2020. — 288 с.
 2. Михайлов С.Б. «Теоретические основы информационной безопасности: учебное пособие для СПО» Ростов-на-Дону : Феникс, 2021. — 240 с.
 3. Попов А.Д. «Информационные угрозы и методы защиты информации: учебник для СПО» Краснодар : Кубанский гос. технологический университет, 2022. — 224 с.
 4. Петрова О.Ю. «Защита информации в компьютерных сетях: учебное пособие для СПО» Омск : Омский политехнический колледж, 2020. — 160 с.
 5. Щеглов А.Н. «Средства и методы защиты информации: учебник для СПО» Уфа : Башкирский филиал Российского государственного университета правосудия, 2021. — 208 с.
 6. Комарова Е.П. «Основные направления информационной безопасности: учебное пособие для СПО» Владивосток : Дальневосточный федеральный университет, 2022. — 192 с.
 7. Горбачёв С.Ф. «Практикум по информационной безопасности: учебное пособие для СПО» Тверь : Тверской технологический колледж, 2020. — 176 с.
- Нормативные правовые акты и государственные стандарты
1. Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных»
 2. Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»
 3. Постановление Правительства РФ № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»
 4. Приказ ФСБ России № 378 от 10 июля 2014 г. «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»
 5. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
 6. Национальный стандарт Российской Федерации ГОСТ Р 53114-2008 «Информационная безопасность сетей связи общего пользования. Общие положения»
 7. Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовая. Платежные приложения. Требования по защите конфиденциальной информации держателей платежных карт»
 8. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»
 9. Стандарты серии ISO/IEC 27000 («Система менеджмента информационной безопасности»).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Формы и методы контроля и оценки результатов обучения
<i>Перечень умений, осваиваемых в рамках дисциплины:</i> применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей; - точно описывать угрозу и документировать решение проблемы; - выбирать меры защиты информации для автоматизированного рабочего места; - осуществлять поиск информации в открытых источниках и работать с технической документацией; - читать или разрабатывать документацию к существующей или проектируемой информационной структуре предприятия - классифицировать основные угрозы безопасности информации; - классифицировать защищаемую информацию по - выявлять информационные угрозы; - анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации, - сопровождения механизмов информационной безопасности.;	- практическая работа № 1-2 - практическая работа № 1-3 - практическая работа № 3 - практическая работа № 4-5 - практическая работа № 6-7 - практическая работа № 8 - практическая работа № 9-10 - практическая работа № 11-12 - практическая работа № 13-14 - практическая работа № 1-2
<i>Перечень знаний, осваиваемых в рамках дисциплины:</i> - методы планирования своей работы; - методы и приемы, используемые для недопущения/устранения угроз информационной безопасности - методы и средства сбора информации и ее хранения; - средства управления, связанные с использованием, обработкой, хранением и передачей данных; - законодательство в области информационной безопасности; - отраслевые стандарты и системы профессиональных сертификаций; сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; - виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; - основные методики анализа угроз и рисков информационной безопасности.	- практическая работа № 1-3 - практическая работа № 3 - практическая работа № 4-5 - практическая работа № 6-7 - практическая работа № 8 - практическая работа № 9-10 - практическая работа № 11-12 - практическая работа № 13-14
Промежуточная аттестация в форме экзамена	