Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Защищенные информационные системы
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта

факультет Компьютерных технологий и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность и программная инженерия
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 1 семестр (ы) 1
очная

г. Махачкала – 2026

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению подготовки и программе магистратуры «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик _____ Мирземагомедова М.М., к.т.н.
(подпись) (ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина

_____ Качаева Г.И., к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 03 » февраля 2026 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности и программной инженерии от « 05 » февраля 2026 года, протокол № 6/1

Зав. выпускающей кафедрой по данному направлению подготовки

_____ Качаева Г.И. к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 05 » февраля 2026 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий и энергетики от « 10 » февраля 2026 г., протокол № 5/1

Председатель Методического совета факультета КТиЭ

_____ Исабекова Т.И.. к.ф.-м.н., доцент
(подпись) (ФИО уч. степень, уч. звание)

« 10 » февраля 2026 г.

Декан факультета _____ Т.А. Рагимова
(подпись) (ФИО)

Начальник УО _____ Л.Н. Мусаева
(подпись) (ФИО)

Проректор по УР _____ А.Ф. Демирова
(подпись) (ФИО)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре ОПОП

Дисциплина «Защищенные информационные системы» входит в обязательную часть учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

Последующими дисциплинами являются: Технологии машинного обучения в кибербезопасности, Управление проектами интеллектуальных информационных систем, Теория обнаружения вторжений с применением искусственного интеллекта, Принятие решений на основе проактивного поиска и обнаружения угроз, Системы мониторинга и управления инцидентами информационной безопасности.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Защищенные информационные системы» способствует формированию у обучающихся компетенций. предусмотренных данной рабочей программой в соответствии с требованиями ФГОС ВО и ОПОП ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом специфики направленности подготовки – «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Защищенные информационные системы» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	**Код и наименование индикаторов достижения компетенции**
УК 1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя её составляющие и связи между ними
	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации; критически оценивает надежность источников информации
	УК-1.3 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подхода
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	ОПК-1.1 Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении
	ОПК-1.2 Проектирует информационные системы с учетом технологий обеспечения информационной безопасности
	ОПК-1.3 Формирует актуальные модели угроз и нарушителей для автоматизированных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Таблица 2.

Вид учебной работы	**Форма обучения**
	очная
Объем образовательной программы дисциплины (ЗЕТ/ в часах)	3/108
В том числе:	**Объем в часах**
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа	4
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена, семестр	1 семестр
Часы на экзамен	36

2.2. Содержание дисциплины

Раздел дисциплины, тема лекции и вопросы	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Тема 1. Теоретические вопросы защиты информации	Автоматизированная информационная система. Классификации задач, решаемых с использованием информационных систем. Свойства систем.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 1. Сканирование уязвимостей. Тестирование проникновения.		
	Самостоятельная работа обучающихся: Закон необходимого разнообразия Эшби.		
Тема 2 Классификации систем защиты информации	Классификации систем. Ранги систем. Закон необходимости разнообразия (закон Эшби). Основы теории надежности. Связь с основными задачами информационной безопасности. Надежность программно-аппаратных реализаций информационных систем	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 2. Удаленное администрирование web-сервера		
	Самостоятельная работа обучающихся: Энтропийная форма закона. Следствия из закона Эшби		
Тема 3 Вопросы информационной безопасности	Вопросы информационной безопасности и аспекты построения защищенных систем. Место процесса кодирования и языка программирования в проблемах информационной безопасности.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 3. Классификация внутренних и внешних нарушителей.		

	Самостоятельная работа обучающихся: Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ		
Тема 4 Аспекты построения защищенных систем	Подходы к проектированию и реализации информационных систем. Жизненный цикл информационной системы.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 4. Определение угроз безопасности информации в информационной системе.		
	Самостоятельная работа обучающихся: Принципы распределения и реализации системы полномочий и доступов.		
Тема 5 Требования к архитектуре ИС для обеспечения безопасности ее функционирования	Структурирование ЗИС. Анализ безопасности ИС. Критерии адекватности средств защиты	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 5. Выбор мер защиты информации для их реализации в информационной системе.		
	Самостоятельная работа обучающихся: Принципы распределения и реализации системы полномочий и доступов.		
Тема 6 Модели угроз информационной безопасности	Уязвимость, угроза информационной безопасности. Модели угроз	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 6. Уязвимость, угроза информационной безопасности.		
	Самостоятельная работа обучающихся: Общие принципы обеспечения резервирования и защиты от сбоев		
Тема 7 Модели нарушителей информационной безопасности	Модель нарушителя информационной безопасности. Информационная инфраструктура.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	

	Лабораторная работа № 7. Классификация инструментальных средств анализа уязвимостей.		
	Самостоятельная работа обучающихся: Принципы защиты информации в ИСПДН.		
Тема 8 Классификация каналов проникновения в систему	Причины уязвимости информационных систем.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 8. Нетехнические меры защиты от внутренних угроз		
	Самостоятельная работа обучающихся: Принципы защиты информации в ИСПДН.		
Тема 9 Утечки информации	Прямые и косвенные каналы проникновения в систему и утечки информации.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 9. Классические методы взлома.		
	Самостоятельная работа обучающихся: Понятие модель данных		
Тема 10 Обеспечение надежности и бесперебойного функционирования информационных систем среды	Слабости системных утилит, команд и сетевых сервисов. Слабости современных технологий программирования и ошибки в программном обеспечении.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 10. Классификация типовых удаленных атак		
	Самостоятельная работа обучающихся: Иерархическая модель данных		
Тема 11 Виды угроз ресурсам Интернета	Виды угроз ресурсам Интернета.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 11. Типы компьютерных атак. URLs и cookies.		
	Самостоятельная работа обучающихся: Сетевая модель данных.		
Тема 12 Средства защиты открытых информационных	Сервисы безопасности. Средства обеспечения ИБ в сетях. Назначение, особенности применения и примеры.	**2**	УК-1, ОПК-1

систем	**в том числе лабораторных занятий:**	**2**	
	Лабораторная работа № 12. Обеспечение безопасности технологий создания активного содержимого сайта		
	Самостоятельная работа обучающихся: Реляционная модель данных		
Тема 13 Средства защиты открытых информационных систем	Аутентификация в сетях. Назначение, особенности применения и примеры. Создание специального оценщика из существующей модели Keras.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 13. Аутентификация, основанная на IP адресе. Сканирование уязвимостей.		
	Самостоятельная работа обучающихся: Постреляционная модель данных		
Тема 14 Мониторинг и аудит в информационных системах	Методы и способы обеспечения идентификации, аутентификации и авторизации в информационных системах.	**2**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 14. Аутентификация, основанная на IP адресе. Сканирование уязвимостей.		
	Самостоятельная работа обучающихся: Объектно-ориентированная модель данных		
Тема 15 Мониторинг и аудит в информационных системах	Понятие несанкционированного доступа и принципы защиты от несанкционированного доступа. Мониторинг и аудит в информационных системах	**4**	УК-1, ОПК-1
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 15. Криптографическая защита информации.		
	Самостоятельная работа обучающихся: Многомерная модель данных		
Тема 16 Криптографическая защита информации	Криптографические методы защиты информации. Управление криптографическими ключами. Симметричная (секретная) методология. Асимметричная (открытая) методология.	**4**	УК-1, ОПК-1

	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 16. Запуск и настройка защищенного web-сервера		
	Самостоятельная работа обучающихся: Руководящие документы Гостехкомиссии России.	**4**	
Итого за 1 семестр:			
Лекции		**34**	
Лабораторные работы		**34**	
Самостоятельная работа		**4**	
Промежуточная аттестация в форме экзамена		**36**	
Всего:		**108**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Защищенные информационные системы» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория программно-аппаратных средств защиты информации	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор интерактивная доска Программное и программно-аппаратное обеспечение: Система защиты информации от НСД «Страж NT»; «ФИКС» - программа фиксации и контроля исходного состояния программного комплекса; TERRIER» - программа поиска и гарантированного уничтожения информации на дисках; «Ревизор 1 XP» - средство создания модели системы разграничения доступа; «Ревизор 2 XP» - программа контроля полномочий доступа к информационным ресурсам; Сетевой сканер «Ревизор Сети»; «ПИК-Lite» - программа подсчета контрольных сумм; Dallas Lock - система защиты информации от несанкционированного доступа в процессе хранения и обработки; Система резервного копирования Кибер Бэкап Расширенная редакция для универсальной платформы; Программный комплекс по предотвращению утечек данных (DLP) Кибер Протего Компьютер RAMEC GALE - корпоративная рабочая станция; Электронный ключ GUARDANT ID; Электронный ключ Rutoken; Средство контроля эффективности применения СЗИ; Программа фиксации и контроля исходного состояния программного комплекса, «Фикс-Unix 1.0»; Программа расчета контрольных сумм «gostum» из состава ОС специального назначения «Astra Linux SE»; Средство контроля эффективности применения СЗИ; Программа фиксации и контроля исходного состояния программного комплекса, «Фикс»; Средство создания модели системы разграничения доступа, «Ревизор 1XP»; Средство контроля защищенности информации от НСД в АС; Программа контроля полномочий доступа к информационным ресурсам, «Ревизор 2XP»; Средство защиты и контроля эффективности применения СЗИ; Программа поиска и гарантированного уничтожения информации на дисках «Terrier»; Средство сбора информации о программном и аппаратном обеспечении в АС «Агент инвентаризации»; СЗИ НСД Аккорд-АМДЗ. Базовый набор функций, шина PCI-express, прошивка с поддержкой UEFI (арт.P79UGX); Съемник информации с контактным устройством DS-USB (арт. 920500); Персональный идентификатор iButton (арт. 930300); Право на использование СПО ПАК СЗИ НСД «Аккорд-Win64»;

	Право на использование СПО «Аккорд-Х»; Служебный носитель «Секрет Особого Назначения» криптографический с быстрым процессором, 32Гб (арт. 620520)
Аудитория для проведения занятий лекционного типа	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска
Аудитория для самостоятельной работы обучающихся	Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска

3.2. Учебно-методическое и информационное обеспечение программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями

3.2.1. Печатные издания

Основная литература:

1. Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 160 с URL: https://e.lanbook.com/book/114699
2. Никифоров С. Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 96 с. – URL: https://e.lanbook.com/book/114697
3. Никифоров С. Н. Методы защиты информации. Защищенные сети [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2018. - 96 с URL: https://e.lanbook.com/book/110935

Дополнительные источники:

1. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст: электронный // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/156401
2. Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург: Лань, 2023. — 544 с. — ISBN 978-5-507-47085-3. — Текст: электронный // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/326153

3.2.2. Основные электронные издания

1. COMSOL Multiphysics® ПО для мульти физического моделирования https://www.comsol.ru
2. Информационный портал Российского научного фонда http://www.rscf.ru
3. Российский фонд фундаментальных исследований https://www.rfbr.ru
4. Электронная библиотека - Режим доступа: http://elibrary.ru
5. Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
6. Электронная библиотечная система издательства «Лань» − http://e.lanbook.com/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения	**Критерии оценки**	**Методы оценки**
- Анализирует проблемную ситуацию как систему, выявляя её составляющие и связи между ними - Определяет пробелы в информации, необходимой для решения проблемной ситуации; критически оценивает надежность источников информации - Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подхода - Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении - Проектирует информационные системы с учетом технологий обеспечения информационной безопасности - Формирует актуальные модели угроз и нарушителей для автоматизированных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности	*Шкала оценивания для экзамена* *«Отлично»* Показывает высокий уровень сформированности компетенций, т.е.: - демонстрирует высокое и прочное освоение материала; - исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; - правильно формирует определения; - демонстрирует умения самостоятельной работы с нормативно-правовой литературой; - умеет делать выводы по излагаемому материалу. *«Хорошо»* Показывает достаточный уровень сформированности компетенций, т.е.: - демонстрирует достаточно полное знание материала, основных теоретических положений; - достаточно последовательно, грамотно и логически стройно излагает теоретический материал; - демонстрирует умения ориентироваться в нормативно-правовой литературе; - умеет делать достаточно обоснованные выводы по излагаемому материалу. *«Удовлетворительно»* Показывает пороговый уровень сформированности компетенций, т.е.: - демонстрирует общее знание изучаемого материала; - испытывает затруднения при ответах на дополнительные вопросы; - знает основную рекомендуемую литературу; - умеет строить ответ в соответствии со структурой излагаемого материала. *Неудовлетворительно»* Ставится в случае: - незнания значительной части программного материала; - невладения понятийным аппаратом дисциплины; - допущения существенных ошибок при изложении учебного материала; - неумения строить ответ в соответствии со структурой излагаемого вопроса; - неумения делать выводы по излагаемому материалу.	Текущий контроль при проведении: - письменного/устного опроса; - тестирования; - оценки результатов самостоятельной работы (докладов, рефератов). Промежуточная аттестация в форме: -экзамен, - письменных/ устных ответов, - тестирования.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

- приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене