МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
Институт кибербезопасности и цифровых технологий

Региональный партнёр
ФГБОУ ВО
«Дагестанский государственный технический университет»

УТВЕРЖДАЮ
И.о. ректора ФГБОУ ВО «ДГТУ»
_____ Н.Л. Баламирзоев
«__25___» _____09_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.01.02 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление подготовки: 09.03.01 «Информатика и вычислительная техника

Направленность (профиль подготовки): «Прикладной искусственный интеллект»

Квалификация выпускника: бакалавр

Форма обучения очная

Махачкала 2023

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ОПОП ВО по направлению подготовки 09.03.01. – Информатика и_вычислительная техника, профилю «Прикладной искусственный интеллект»

Разработчик _____ Магомедов И.А., к.т.н, доцент
подпись ФИО уч. степень, уч. звание)

05.09.2023г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)

_____ Гасанова Н.М., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

05.09. 2023г.

Программа одобрена на заседании выпускающей кафедры УиИТСиВТ

от 12.09.2023 г., протокол № 1

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)

_____ Гасанова Н.М., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

от 12.09.2023 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий, вычислительной техники и энергетики от 22.09.2023 года, протокол № 1.

Председатель Методического совета факультета КТВТиЭ

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

«22» 09. 2023 г

Декан факультета _____ Ш.А. Юсуфов
подпись ФИО

Начальник УО _____ Э.В. Магомаева
подпись ФИО

1. Цель и задачи дисциплины

Цель дисциплины: Формирование у будущих бакалавров в области прикладного искусственного интеллекта системных знаний, умений и навыков в области обеспечения информационной безопасности компьютерных систем и сетей, с акцентом на специфику защиты данных, моделей и алгоритмов ИИ.

Задачи дисциплины:

1. Изучить теоретические основы информационной безопасности (ИБ): понятия угроз, уязвимостей, модели безопасности.
2. Сформировать понимание законодательных и нормативных основ ИБ в РФ.
3. Освоить основные криптографические методы и протоколы защиты информации.
4. Изучить методы и средства аутентификации, управления доступом, защиты от вредоносного ПО.
5. Приобрести навыки анализа угроз и выбора методов защиты для систем, использующих технологии ИИ (защита данных для обучения, целостности моделей, конфиденциальности запросов к ИИ).
6. Научиться применять современные программно-аппаратные средства защиты информации в лабораторном практикуме.
7. Развить способность к самостоятельному изучению новых угроз и средств защиты в быстро меняющейся области ИБ.

2. Место дисциплины в структуре ОПОП бакалавриата

Для успешного освоения необходимы знания и компетенции, полученные при изучении дисциплин: «Программирование», «Алгоритмы и структуры данных», «Архитектура ЭВМ и систем», «Операционные системы», «Математические основы искусственного интеллекта».

3. Результаты освоения дисциплины "Методы и средства защиты компьютерной информации"

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Код	Наименование компетенции	Индикатор достижения компетенции		В результате освоения дисциплины обучающийся должен:	Другая дисциплина (дисциплины) / практика, участвующая в формировании компетенции
ПК-1	Способен проектировать интеллектуальное программное обеспечение для решения практических задач	ПК-1.1 Осуществляет проектирование компонентов программного обеспечения с элементами искусственного интеллекта		Знать: Методы построения и анализа систем аутентификации. Принципы работы межсетевых экранов и систем обнаружения вторжений. Уметь: Настраивать базовые средства защиты ОС и сети. Обрабатывать и анализировать данные аудита безопасности. Владеть: Навыками работы со средствами криптографической защиты (GPG, хэш-функции). Навыками настройки политик безопасно	Архитектура ЭВМ и систем. Программирование. Операционные системы.
		ПК-1.2 Создаѐт варианты реализации компонент ПО на основе анализа предъявляемых требований.			Алгоритмы и структуры данных. Математические основы искусственного интеллекта.

4. Структура и содержание дисциплины (модуля)
«Методы и средства защиты компьютерной информации

4.1. Структура дисциплины
Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

Форма обучения	*Семестр*	*Общая трудоёмкость по дисциплине (ЗЕТ/ в часах)*	*Лекции, час*	*Практич ские занятия, час*	*Лаб. зан, час*	*СРС. час*	*Контр., час*	*Контроль*
Очно	*5*	*4/144*	*17*	-	34	*57*	*36*	*Экз.*

4.2. Содержание дисциплины (модуля)
«Методы и средства защиты компьютерной информации

№ п/п	Раздел дисциплины, тема лекции и вопросы		Энная форма			Заочная форма			
		ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР
1	2	3	4	5	6	7	8	9	10
1.	Модуль 1. Теоретические и нормативные основы защиты информации. Введение в ИБ. Базовые принципы (CIA-триада, DAD-триада угроз). Классификация угроз и уязвимостей. Модели безопасности (Bell-LaPadula, Biba, Clark-Wilson). Основы управления рисками ИБ (качественная и количественная оценка). Правовое регулирование ИБ в РФ (ФЗ-152, ФЗ-187, ФЗ-276, стратегия ИБ). Национальные и международные стандарты ИБ (ГОСТ Р ИСО/МЭК 27001, PCI DSS). Этические аспекты ИБ в разработке ИИ.	2		4	10				10

2.	Модуль 2. Криптографические основы защиты информации. Темы лекций: Исторический обзор. Задачи криптографии. Основные понятия (криптостойкость, ключи, виды атак). Современные требования к криптографическим алгоритмам.	2		4	5	2		2	15
3.	Модуль 3. Алгоритмы и протоколы криптографической защиты. Темы лекций: Симметричное шифрование (AES, режимы работы). Асимметричное шифрование (RSA, ECC). Хэш-функции (SHA-2/3) и алгоритмы ЭЦП. Основы PKI (устройство и назначение).	2		4	5			2	15
4.	Модуль 4. Защита информации в операционных системах и базах данных. Темы лекций: Идентификация, аутентификация, авторизация. Дискреционные (DAC), мандатные (MAC) и ролевые (RBAC) модели управления доступом. Встроенные механизмы безопасности ОС Windows (BitLocker, Credential Guard) и Linux (SELinux, AppArmor). Основы защиты СУБД (разграничение прав, аудит, шифрование данных).	2		4	5				15
5.	Модуль 5. Защита информации в компьютерных сетях. Темы лекций: Угрозы в сетях (sniffing, spoofing, MitM, DoS/DDoS). Принципы и архитектура межсетевых экранов (firewall). Системы обнаружения и предотвращения вторжений (IDS/IPS). Принципы безопасного сетевого проектирования (сегментация, Zero Trust). Виртуальные частные сети (VPN, IPSec, WireGuard).	2		4	10	2		2	15

6.	Модуль 6. Технические средства и методы защиты от вредоносного ПО. Темы лекций: Классификация вредоносного ПО (вирусы, черви, трояны, руткиты, шпионское ПО, ransomware). Векторы распространения и жизненный цикл атаки. Методы обнаружения (сигнатурный, поведенческий, эвристический анализ). Современные антивирусные технологии и песочницы (sandbox). Безопасность	2		4	5				15
7.	Модуль 7. Особенности защиты систем искусственного интеллекта и данных. Темы лекций: Новый ландшафт угроз для ИИ-систем: атаки на данные (data poisoning, membership inference), атаки на модели (adversarial attacks, model stealing, backdoors), атаки на цепочку поставок (Supply Chain). Методы защиты: дифференциальная приватность (Differential Privacy) для данных, adversarial training и детектирование для моделей, конфиденциальные вычисления (Confidential Computing, Federated Learning). Правовые аспекты (регулирование алгоритмов, bias и fairness).	2		4	5				15
8.	Модуль 8. Инженерно-техническая защита информации и безопасность жизненного цикла ПО (SDLC). Темы лекций: Комплексный подход к ИБ. Резервное копирование и восстановление (стратегии 3-2-1). Физическая безопасность. Принципы безопасной разработки (Secure SDLC, модель Microsoft SDL). Статический и динамический анализ кода (SAST, DAST). Основы пентестинга (цели, этапы, виды).	2		4	5			2	10

9.	Модуль 9. Организационные меры защиты и реагирование на инциденты. Темы лекций: Политика информационной безопасности и ее составные части. Обучение и повышение осведомленности пользователей. Процесс управления инцидентами ИБ (S.I.M.): подготовка, обнаружение, анализ, сдерживание, ликвидация, восстановление, извлечение уроков. Основы цифровой криминалистики (форезики): сбор и сохранение доказательств.	1		2	7				13
10.	Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)	Входная контр, работа. 1 ат-я 1-3 тема 2 ат-я 4-6 тема 3 ат-я 7-9 тема							
11.	Форма промежуточной аттестации (по семестрам)	Экзамен 1 ЗЕТ (36 часов)				Экзамен			
12.	ИТОГО	17		34	57	4	-	8	123

4.3 Перечень и содержание лабораторных занятий.

№ п/п	№ разделов	Наименование лабораторных работ	Кол. ч
1.	1	Анализ угроз для типовой ИС с использованием методик (например, STRIDE). Работа с реестрами уязвимостей (CVE, NVD). Изучение структуры ФЗ-152 «О персональных данных».	4
2.	2	Знакомство с инструментами криптоанализа (частота символов, взлом шифра Цезаря). Работа с генераторами криптографически стойких случайных чисел.	4
3.	3	Практикум по использованию GnuPG/PGP для шифрования, подписи и верификации. Создание и анализ самоподписанных и центрированных SSL/TLS сертификатов. Работа с утилитами командной строки (`openssl`)	4
4.	4	Настройка политик сложности паролей и блокировки учетных записей в Windows. Работа с списками контроля доступа (ACL) в Linux. Настройка базовой ролевой модели в PostgreSQL/MySQL. Шифрование дискового раздела с помощью VeraCrypt.	4
5.	5	Анализ сетевого трафика в Wireshark (выявление незашифрованных протоколов). Настройка базовых правил межсетевого экрана в Linux (`iptables`/`nftables`). Знакомство с сетевым сканером Nmap. Настройка простого VPN-соединения (например, WireGuard).	4
6.	6	Статический анализ подозрительного файла (exif-данные, хэши, строки). Динамический анализ в изолированной среде (виртуальная машина). Исследование фишингового письма. Обзор современных платформ для анализа угроз (VirusTotal, Any.Run).	4
7.	7	Демонстрация adversarial-атаки на простую нейронную сеть (с использованием библиотек типа FoolBox, ART). Эксперимент с добавлением шума для реализации базовой дифференциальной приватности набора данных. Анализ кода на наличие уязвимостей в типовом ML-пайплайне.	4
8.	8	Настройка автоматического резервного копирования с помощью скриптов. Знакомство с инструментом статического анализа кода для Python/Java (Bandit, SpotBugs). Разбор отчета сканера безопасности (например, OWASP ZAP).	4
9.	9	Разработка фрагмента политики ИБ (например, политики паролей или использования съемных носителей). Разбор кейса по реагированию на инцидент (на примере утечки данных). Знакомство с основами анализа логов (на примере журналов событий Windows или `journalctl` в Linux).	2
Итого за семестр			**34**

5. Образовательные технологии

В ходе освоения дисциплины "**Высокопроизводительные вычисления**" при проведении аудиторных занятий используется образовательная технология, предусматривающая такие методы и формы изучения материала как лекция, лабораторное занятие, включающие активные и интерактивные формы занятий:

- Проведение лекции проблемного характера: тема 1.1. " Принципы построения численных методов поиска безусловного экстремума. Методы нулевого порядка»; тема 3.3. "Методы решения транспортных задачей".
- Проведение лабораторных занятий в интерактивной форме и публичная защита отчетов по лабораторным работам, работа в малых группах.

Занятия, проводимые в интерактивной форме, составляют 25 % от общего количества аудиторных занятий.

Лабораторные занятия проводятся в с использованием специализированных пакетов.

Самостоятельная работа студентов подразумевает работу под руководством преподавателя (консультации, помощь в написании и отладке программ и др.) и индивидуальную работу студента, выполняемую как дома, так и в компьютерном классе с выходом в Интернет.

При реализации образовательных технологий используются следующие виды самостоятельной работы:

- работа с конспектом лекции и литературой;
- подготовка к лабораторной работе: изучение теоретического материала, разработка и отладка программ заданий по лабораторным работам;
- обработка результатов лабораторных работ и подготовка письменных отчетов;
- выполнение и оформление индивидуальных домашних заданий: изучение теоретического материала, разработка алгоритма решения задачи, разработка и отладка программ, вычислительный эксперимент с разработанной программой, оформление письменного отчета по индивидуальному заданию;
- поиск информации в Интернет и литературе;
- подготовка к сдаче лабораторных работ и индивидуальных заданий;
- подготовка к сдаче экзамена.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения. возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

В качестве других видов контактной работы запланированы консультации при подготовке и проведении текущей и промежуточной аттестации.

При организации самостоятельной работы студентов и, при необходимости, при проведении аудиторных занятий используются /могут быть использованы дистанционные образовательные технологии.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

6.1. План самостоятельной работы студентов

Неделя	Тема (модуль)	Вид самостоятельной работы	Задание	Рекомендуемая литература*	Часы
1-2	М1: Теоретические и нормативные основы.	1. Изучение лекционного материала. 2. Аналитическая работа. 3. Подготовка к ЛР.	1. Конспектирование базовых моделей (Bell-LaPadula, Biba). 2. Сравнительный анализ положений ФЗ-152 (О ПДн) и GDPR (ЕС). 3. Подготовка таблицы угроз для типового веб-приложения (по методологии STRIDE).	[1, 2, 7]	8
3	М2: Криптографические основы.	1. Решение задач. 2. Работа с инструментами.	1. Решение задач на расчет энтропии информации и криптостойкости. 2. Установка и первичное знакомство с инструментами криптографического анализа (например, CrypTool 2).	[1, 3]	4
4	М3: Алгоритмы и протоколы.	1. Проработка примеров. 2. Исследовательская работа.	1. Самостоятельное шифрование/дешифрование файлов с помощью GnuPG (создание ключей, обмен). 2. Поиск и анализ информации о реальных инцидентах, связанных со слабостями SSL/TLS (например, Heartbleed).	[3, 4]	4

5	М4: Защита в ОС и СУБД.	1. Написание отчета. 2. Проектирование.	1. Анализ журналов событий безопасности (Windows Event Log / Linux auditd) своей рабочей станции. 2. Разработка схемы ролевого доступа (RBAC) для гипотетической системы учета с ИИ-модулем.	[2, 5]	4
6	М5: Защита в сетях.	1. Работа с инструментами. 2. Аналитическая работа.	1. Самостоятельное исследование открытых портов на тестовом стенде с помощью Nmap (сканирование, анализ выводов). 2. Подготовка сравнительной таблицы технологий VPN (IPSec vs WireGuard vs OpenVPN) по заданным критериям.	[4, 5]	6
7	М6: Защита от вредоносного ПО.	1. Исследовательская работа. 2. Подготовка к тестированию.	1. Анализ отчета антивирусного сканера (VirusTotal) для легитимного и подозрительного файла. Написание выводов. 2. Изучение рекомендаций OWASP Top 10 для обеспечения безопасности веб-приложений.	[4, 6]	6
8-9	М7: Защита систем ИИ.	1. Анализ статей. 2. Экспериментальная работа. 3. Проектирование.	1. Конспектирование научной статьи по методам adversarial attacks на нейросети (на рус./англ.). 2. Самостоятельный запуск и анализ скрипта, демонстрирующего базовую adversarial атаку (на предоставленном коде). 3. Разработка раздела «Требования	[5, 6, 8, 9]	8

			по ИБ» для техзадания на создание ИИ-сервиса распознавания изображений.		
10	М8: Инженерно-техническая защита и SDLC.	1. Работа с инструментами. 2. Написание сценария.	1. Написание простого скрипта (bash/Python) для автоматизации резервного копирования каталога. 2. Разработка чек-листа из 10 пунктов для безопасной приемки кода (code review) с учетом уязвимостей ИИ-моделей.	[2, 6]	5
11-12	М9: Организационные меры и реагирование.	1. Кейс-стади. 2. Проектная работа.	1. Разбор публичного кейса об утечке данных (на выбор). Анализ причин и действий по реагированию. 2. Создание проекта «Политика использования облачных сервисов (CSP)» для небольшой команды разработки ИИ.	[2, 7]	5
13-17	Подготовка к экзамену и итоговое проектирование.	1. Повторение. 2. Проектная работа. 3. Консультация.	1. Систематизация знаний по всем модулям. Решение тестовых заданий из ФОС. 2. Разработка итогового проекта: «Архитектура безопасности для чат-бота с LLM». Включение разделов: угрозы, криптография, управление доступом, защита модели, мониторинг. 3. Подготовка вопросов для консультации перед экзаменом.	[1-9]	7
			Итого часов:		57

6.2 Методические указания по организации самостоятельной работы студентов

Планируются следующие виды самостоятельной работы:

- подготовка к лабораторным и лекционным занятиям,
- выполнение индивидуального задания,
- оформление отчётов по лабораторным работам,
- подготовка к экзамену.

Подготовка к лабораторным занятиям проводится посредством изучения курса лекций, дополнительной литературы, Интернет-ресурсов.

Задание к выполнению каждой лабораторной работы состоит из общей части, которая сформулирована в разделе «Задание к выполнению» и уточнения варианта, который приведен в разделе «Варианты заданий». Студент должен заранее ознакомиться со своим заданием и, если у него возникают какие-либо вопросы относительно задания, поставить эти вопросы преподавателю до начала работы.

Отчёт к лабораторной работе должен содержать:

- Тему работы;
- Цель работы;
- Задание для выполнения, включая индивидуальное задание;
- Описание алгоритма программы (при необходимости, со схемой алгоритма);
- Описание переменных и структур данных, которые применяются в программе;
- Описание ключевых программных решений, принятых при реализации алгоритма в тексте программы;
- Текст программы;
- Результат работы программы;
- Выводы.

Подготовка к экзамену проводится посредством изучения курса лекций, изучения литературы, Интернет-ресурсов.

Студентам из числа лиц с ограниченными возможностями здоровья могут быть предложены электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий: проверка выполнения индивидуального задания на лабораторной работе	Разделы 1 – 9	ПК-1
2	Текущий: собеседование при защите лабораторных работ	Разделы 1 – 9	ПК-1
3	Итоговый: Экзамен	Разделы 1 – 9	ПК-1

Материалы для проведения текущего контроля знаний и промежуточной аттестации составляют отдельный документ – Фонд оценочных средств по дисциплине «**Методы и средства защиты компьютерной информации**.

Учебно-методическое и информационное обеспечение дисциплины " Высокопроизводительные вычисления "

а) основная литература:

1. Основная литература: Галатенко В.А. Основы информационной безопасности; Щербаков А.Ю. Современная компьютерная безопасность.
2. Дополнительная литература: Мамаев М.А. Защита в операционных системах; Статьи по adversarial machine learning.
3. Программное обеспечение: VMware Workstation, Kali Linux, Security Onion, Wireshark, GnuPG, средства виртуализации Python для ЛР по ИИ.
4. Базы данных, ИР: ЭБС «Лань», «Znanium», IEEE Xplore, портал SecurityLab.ru.

5. Гергель В.П. Теория и практика параллельных вычислений. – М.: Интернет-Университет Информационных Технологий, 2007.
6. Э. Таненбаум, М. ван Стеен. Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2020.
7. Sanders, J., Kandrot, E. CUDA by Example: An Introduction to General-Purpose GPU Programming. – Addison-Wesley, 2010.
8. Дополнительная литература:
9. Официальная документация OpenMP, MPI, CUDA.
10. Foster, I. Designing and Building Parallel Programs. – Addison-Wesley, 1995.
11. Программное обеспечение: Компиляторы с поддержкой OpenMP (gcc, Intel), библиотека MPI (OpenMPI, MPICH), NVIDIA CUDA Toolkit, Python, Jupyter Notebook.

б) Интернет-ресурсы:

№ п/п	Адрес сайта	Описание материала, содержащегося на сайте
1.	http://www.io-sotech.com/ru/	Практическое применение задач оптимизации
2.	http://matlab.exponenta.ru/optimiz/book_1/index.php	А.Г. Трифонов. "Optimization Toolbox 2.2 Руководство пользователя "
3.	http://matlab.exponenta.ru/optimiz/book_7/index.php	Статьи, материалы по практическим приложениям
4.	http://matlab.exponenta.ru/optimiz/book_2/index.php	А.Г. Трифонов. "Постановка задачи оптимизации и численные методы ее решения"
5.	http://matlab.exponenta.ru/optimiz/book_6/index.php	А.Г.Трифонов "Optimization Toolbox 3"
6.	http://matlab.exponenta.ru/optimiz/book_4/index.php	Список функций Optimization Toolbox

в) Программное обеспечение: Все лабораторные работы выполняются на персональных компьютерах с использованием специализированных математических пакетов (MATLAB)

г) Другое материально-техническое обеспечение: Реализация программы учебной дисциплины требует наличия учебной компьютерной лаборатории.

Оборудование компьютерной лаборатории: посадочные места по количеству обучающихся; рабочее место преподавателя; маркерная доска; учебно-методическое обеспечение.

Технические средства обучения: компьютеры по количеству обучающихся; локальная компьютерная сеть и глобальная сеть Интернет; лицензионное системное и прикладное

программное обеспечение; лицензионное антивирусное программное обеспечение; лицензионное специализированное программное обеспечение; медиа-проектор.

Для лиц с ограниченными возможностями здоровья по ходатайству заведующего кафедрой на отдельные ПЭВМ может устанавливаться индивидуальный набор программного обеспечения.

Сведения о переутверждении программы на очередной учебный год

и регистрации изменений

Учеб-ный год	Решение ка-федры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой