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
_____ И.Л. Баламирзоев
«09» 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

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

1. ПАСПОРТ
фонда оценочных средств

по дисциплине Б1.В.ДВ.01.02 Методы и средства защиты компьютерной информации
1.1. Результаты обучения по дисциплине:

Код компетенции	Наименование компетенции	Индикатор достижения компетенции *(закрепленный за дисциплиной)*	В результате освоения дисциплины обучающийся должен:	Другая дисциплина (дисциплины) / практика, участвующая в формировании компетенции
ПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности.	ПК-1.1. Применяет математические и инженерные методы для анализа и обеспечения безопасности систем, в т.ч. с элементами ИИ.	**Знать:** особенности угроз и методов защиты для систем искусственного интеллекта (adversarial attacks, data poisoning). **Уметь:** применять методы защиты (дифференциальная приватность, adversarial training) в контексте ИИ-моделей. **Владеть:** базовыми навыками анализа защищенности алгоритмов машинного обучения.	Архитектура ЭВМ и систем. Программирование. Операционные системы.

1.2. Программа оценивания контролируемой компетенции:

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции/ индикатора	Наименование оценочного средства
1	Модуль 1. Теоретические и нормативные основы защиты информации.	ПК-1.1,	Контрольный тест (блок А), Защита лабораторных работ, Вопросы экзамена
2	Модуль 2-3. Криптографические методы и алгоритмы защиты.	ПК-1.1,	Контрольный тест (блок Б), Защита лабораторных работ, Вопросы экзамена
3	Модуль 4-5. Защита в ОС, СУБД и компьютерных сетях.	ПК-1.1,	Контрольный тест (блок В), Защита лабораторных работ, Вопросы экзамена
4	Модуль 6. Защита от вредоносного ПО.	ПК-1.1,	Контрольный тест (блок Г), Защита лабораторных работ, Вопросы экзамена
5	Модуль 7. Особенности защиты систем ИИ.	ПК-1.1,	Контрольный тест (блок Д), Защита лабораторных работ, Вопросы экзамена
6	Введение в HPC. Архитектуры параллельных систем.	ПК-1.1,	Собеседование. Контрольный тест (Блок А).
7	Параллельное программирование на разделяемой памяти (OpenMP).	ПК-1.1,	Защита лабораторной работы. Контрольный тест (Блок Б).
8.	Параллельное программирование на распределенной памяти (MPI).	ПК-1.1,	Защита лабораторной работы. Контрольный тест (Блок В).
9	Гибридное программирование (MPI + OpenMP).	ПК-1.1,	Защита лабораторной работы. Контрольный тест (Блок Г).
10.	Вычисления на графических процессорах (CUDA).	ПК-1.1,	Защита лабораторной работы. Контрольный тест (Блок Г).
11.	HPC для задач искусственного интеллекта. Оптимизация и профилирование.	ПК-1.1,	Собеседование. Контрольный тест (Блок Д). Отчет по СРС.

3. Контрольные вопросы и задания

Вопросы к 1 аттестации

1. Модуль 1. Теоретические и нормативные основы защиты информации.
2. Введение в ИБ. Базовые принципы (CIA-триада, DAD-триада угроз).
3. Классификация угроз и уязвимостей. Модели безопасности (Bell-LaPadula, Biba, Clark-Wilson). Основы управления рисками ИБ (качественная и количественная оценка).
4. 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.
5. Модуль 2. Криптографические основы защиты информации.
6. Исторический обзор.
7. Задачи криптографии.
8. Основные понятия (криптостойкость, ключи, виды атак). Современные требования к криптографическим алгоритмам.
9. Модуль 3. Алгоритмы и протоколы криптографической защиты.
10. Симметричное шифрование (AES, режимы работы).
11. Асимметричное шифрование (RSA, ECC).
12. Хэш-функции (SHA-2/3) и алгоритмы ЭЦП.
13. Основы PKI (устройство и назначение).

Вопросы ко 2 аттестации

14. Модуль 4. Защита информации в операционных системах и базах данных.
15. Идентификация, аутентификация, авторизация.
16. Дискреционные (DAC), мандатные (MAC) и ролевые (RBAC) модели управления доступом.
17. Встроенные механизмы безопасности ОС Windows (BitLocker, Credential Guard) и Linux (SELinux, AppArmor).
18. Основы защиты СУБД (разграничение прав, аудит, шифрование данных).
19. Модуль 5. Защита информации в компьютерных сетях.
20. Угрозы в сетях (sniffing, spoofing, MitM, DoS/DDoS).
21. Принципы и архитектура межсетевых экранов (firewall).
22. Системы обнаружения и предотвращения вторжений (IDS/IPS).
23. Принципы безопасного сетевого проектирования (сегментация, Zero Trust).
24. Виртуальные частные сети (VPN, IPSec, WireGuard).
25. Модуль 6. Технические средства и методы защиты от вредоносного ПО.
26. 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 анти-

вирусные технологии и песочницы (sandbox). Безопасность веб-браузеров и почтовых клиентов.

Вопросы к 3 аттестации

27. Модуль 7. Особенности защиты систем искусственного интеллекта и данных.
28. 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).
29. Методы защиты: дифференциальная приватность (Differential Privacy) для данных, adversarial training и детектирование для моделей, конфиденциальные вычисления (Confidential Computing, Federated Learning).
30. Правовые аспекты (регулирование алгоритмов, bias и fairness).
31. Модуль 8. Инженерно-техническая защита информации и безопасность жизненного цикла ПО (SDLC).
32. Комплексный подход к ИБ.
33. Резервное копирование и восстановление (стратегии 3-2-1).
34. Физическая безопасность.
35. Принципы безопасной разработки (Secure SDLC, модель Microsoft SDL).
36. Статический и динамический анализ кода (SAST, DAST).
37. Основы пентестинга (цели, этапы, виды).

3.1. Вопросы к экзамену по дисциплине Б1.В.ДВ.01.02 Методы и средства защиты компьютерной информации

Инструкция: Тест состоит из 30 заданий, разделенных на 6 блоков (A-E) по 5 вопросов в каждом. В вопросах 1-25 выберите один правильный ответ. В вопросах 26-30 выберите все правильные ответы.

БЛОК А. Теоретические и нормативные основы

1. Триада CIA (КЦД) в информационной безопасности расшифровывается как:
   а) Контроль, Целостность, Доступ
   б) Конфиденциальность, Целостность, Доступность
   в) Кодирование, Цифровизация, Деплоймент

2. Модель безопасности, запрещающая субъекту с низким уровнем допуска читать информацию с высоким уровнем классификации, называется:
   а) Модель Биба
   б) Модель Кларка-Уилсона
   в) Модель Белла-ЛаПадулы

3. Какой Федеральный закон РФ является базовым для регулирования защиты персональных данных?
   а) ФЗ-187 «О безопасности критической информационной инфраструктуры»
   б) ФЗ-152 «О персональных данных»
   в) ФЗ-149 «Об информации, информационных технологиях и о защите информации»

4. К какому типу угроз по модели STRIDE относится подмена IP-адреса отправителя?
   а) Spoofing (подмена)
   б) Tampering (несанкционированное изменение)
   в) Spoofing (подмена) и Information Disclosure (раскрытие информации)

5. Какой из перечисленных документов НЕ является международным стандартом по управлению информационной безопасностью?
а) ISO/IEC 27001
б) PCI DSS
в) ГОСТ Р 34.10-2012 (стандарт на ЭЦП)

БЛОК Б. Криптографические методы

6. К какому типу криптографии относится алгоритм AES (Advanced Encryption Standard)?
а) Симметричное шифрование
б) Асимметричное шифрование
в) Хэширование

7. Основное назначение хэш-функции (например, SHA-256) – это:
а) Шифрование конфиденциальных данных для передачи
б) Проверка целостности данных (формирование дайджеста)
в) Управление криптографическими ключами

8. Протокол, обеспечивающий защищенное соединение между веб-браузером и сервером, называется:
а) SSH
б) TLS/SSL
в) IPsec

9. Какой принцип лежит в основе работы асимметричной криптографии?
а) Использование одного секретного ключа для шифрования и расшифрования
б) Использование пары ключей: открытого (public) и закрытого (private)
в) Необратимое преобразование данных в фиксированный размер

10. Цифровая подпись (ЭЦП) обеспечивает:
а) Только конфиденциальность документа
б) Аутентификацию автора и целостность документа
в) Только невозможность отказа от авторства

БЛОК В. Защита в ОС, СУБД и сетях

11. Модель управления доступом в ОС Windows, основанная на списках ACL (Access Control List), является примером:
а) Мандатного управления доступом (MAC)
б) Дискреционного управления доступом (DAC)
в) Ролевого управления доступом (RBAC)

12. Основная функция межсетевого экрана (firewall) заключается в:
а) Обнаружении сигнатур вирусов в трафике
б) Фильтрации сетевого трафика на основе заданных правил
в) Шифровании всего исходящего трафика

13. Технология, позволяющая создать защищенный логический канал в публичной сети (например, интернет), – это:
а) IDS (Система обнаружения вторжений)
б) VPN (Виртуальная частная сеть)

в) SIEM (Система управления событиями ИБ)

14. Атака типа "Отказ в обслуживании" (Denial-of-Service, DoS) направлена в первую очередь на нарушение:
а) Конфиденциальности
б) Целостности
в) Доступности

15. Для безопасного удаленного администрирования сервера по протоколу командной строки следует использовать:
а) Telnet
б) SSH (Secure Shell)
в) RDP без дополнительных настроек

БЛОК Г. Защита от вредоносного ПО

16. Вредоносная программа, которая шифрует файлы пользователя и требует выкуп за расшифровку, называется:
а) Троян
б) Шпионское ПО (Spyware)
в) Программа-вымогатель (Ransomware)

17. Какой метод обнаружения вредоносного ПО НЕ является сигнатурным?
а) Сравнение хэша файла с базой известных вредоносных хэшей
б) Поиск в файле известной последовательности байт (сигнатуры)
в) Анализ аномального поведения программы в изолированной среде (песочнице)

18. Основной вектор распространения фишинговых атак – это:
а) Съемные USB-носители
б) Электронная почта и сообщения в мессенджерах
в) Локальная сеть предприятия

19. Инструмент или методика, используемая для динамического анализа подозрительного файла в изолированной среде без риска для основной системы, – это:
а) Антивирусный сканер
б) Песочница (Sandbox)
в) Межсетевой экран

20. Базовое правило "не открывать вложения из непроверенных источников" относится к мерам защиты на уровне:
а) Техническом
б) Организационном и человеческого фактора
в) Аппаратном

БЛОК Д. Защита систем ИИ

21. Атака на систему машинного обучения, при которой злоумышленник вносит малозаметные искажения во входные данные, чтобы модель дала ошибочный вывод, – это:
а) Data Poisoning
б) Adversarial Attack
в) Model Inversion

22. Метод защиты конфиденциальности обучающих данных в ML, основанный на добавлении контролируемого шума, – это:
а) Federated Learning
б) Homomorphic Encryption
в) Differential Privacy (Дифференциальная приватность)

23. Угроза, при которой злоумышленник пытается определить, входили ли конкретные данные в обучающую выборку модели, называется:
а) Adversarial Attack
б) Membership Inference Attack
в) Backdoor Attack

24. Какой из перечисленных подходов НЕ является типичным методом защиты от adversarial атак?
а) Adversarial Training (добавление adversarial примеров в обучающую выборку)
б) Увеличение размера модели (количества параметров) в 10 раз
в) Использование детекторов adversarial примеров

25. Фреймворк, позволяющий обучать модель на данных, которые остаются на устройствах пользователей, без их централизации, – это:
а) Federated Learning (Обучение на федеративных данных)
б) Transfer Learning
в) Differential Privacy

БЛОК Е. Инженерно-техническая и организационная защита

26. Какие из перечисленных мер относятся к организационным мерам защиты информации? (Выберите ВСЕ правильные ответы)
а) Разработка и внедрение Политики информационной безопасности
б) Обучение и повышение осведомленности сотрудников в области ИБ
в) Установка антивирусного ПО на все рабочие станции
г) Регламентация процедур резервного копирования и восстановления

27. Принцип "минимальных привилегий" (Principle of Least Privilege) в управлении доступом означает, что: (Выберите ВСЕ правильные ответы)
а) Пользователь должен иметь права администратора для удобства работы
б) Пользователю предоставляются только те права, которые необходимы для выполнения его задач
в) Рекомендуется использовать учетные записи с повышенными правами только когда это абсолютно необходимо
г) Все пользователи в отделе должны иметь одинаковые права

28. Какие из перечисленных технологий/стандартов непосредственно связаны с обеспечением безопасного жизненного цикла разработки ПО (Secure SDLC)? (Выберите ВСЕ правильные ответы)
а) Статический анализ кода (SAST)
б) Динамический анализ кода (DAST)
в) Алгоритм шифрования AES-256
г) Протокол HTTP

29. Основные фазы процесса управления инцидентами информационной безопасности (S.I.M.) включают: (Выберите ВСЕ правильные ответы)

а) Обнаружение (Detection)
б) Анализ (Analysis)
в) Игнорирование (Ignoring)
г) Ликвидация (Eradication) и восстановление (Recovery)

30. К техническим мерам защиты информации от утечки по каналам побочных электромагнитных излучений (ПЭМИН) можно отнести: (Выберите ВСЕ правильные ответы)
а) Использование средств маскирующей обработки (генераторы шума)
б) Экранирование помещений
в) Установку межсетевого экрана
г) Обязательное шифрование всех жестких дисков

Ключ к тесту (правильные ответы):
1. б, 2. в, 3. б, 4. а, 5. в, 6. а, 7. б, 8. б, 9. б, 10. б,
11. б, 12. б, 13. б, 14. в, 15. б, 16. в, 17. в, 18. б, 19. б, 20. б,
21. б, 22. в, 23. б, 24. б, 25. а, 26. а, б, г, 27. б, в, 28. а, б, 29. а, б, г, 30. а, б

Описание показателей и критериев оценивания теста:

Форма проведения: Письменное тестирование или компьютерное тестирование в системе Moodle/Прометеус.

Время выполнения: 40 минут.

Система оценивания: За каждый правильный ответ в вопросах 1-25 начисляется 1 балл. За полностью правильный ответ в вопросах 26-30 (все верные варианты выбраны, лишние не выбраны) начисляется 2 балла. Частично правильный ответ (выбраны не все верные варианты или добавлены неверные) оценивается в 0 баллов.

Максимальный балл: 25 1 + 5 2 = 35 баллов.

Шкала перевода в оценку за тест (в рамках текущего контроля/рубежного рейтинга):

30-35 баллов (86-100%) – «отлично»
25-29 баллов (71-85%) – «хорошо»
18-24 балла (51-70%) – «удовлетворительно»
Менее 18 баллов (<51%) – «неудовлетворительно»

Сведения о дополнениях и изменениях, внесенных в ФОС дисциплины

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные в ФОС дополнения и изменения	Подпись заведующего кафедрой