Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Технологии машинного обучения в кибербезопасности»
(указывается индекс и наименование дисциплины)

Уровень образования — магистратура
(бакалавриат/магистратура/специалитет)

Направление подготовки — 10.04.01 Информационная безопасность
(код, наименование направления подготовки)

Направленность — Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта
(наименование)

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

Фонд оценочных средств обсужден на заседании кафедры ИБиПИ
«05» февраля 2026 г., протокол № 6/1

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

г. Махачкала – 2026

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью рабочей программы дисциплины «Технологии машинного обучения в кибербезопасности» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. самостоятельной работе обучающихся), освоивших программу данной дисциплины.

Целью разработки фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям федерального государственного образовательного стандарта высшего образования (далее - ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность.

Рабочей программой дисциплины «Технологии машинного обучения в кибербезопасности» предусмотрено формирование следующих компетенций:

1) ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

Формой аттестации по дисциплине является экзамен.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по дисциплине осуществляется комплексная проверка индикаторов достижения компетенций их формирования в процессе освоения ОПОП.

Таблица 1.

Результаты обучения: индикаторы достижения	Формируемые компетенции
ОПК-2.2 - Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью	ОПК-2

3. ОЦЕНКА ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1. Контроль и оценка освоения дисциплины по темам (разделам)

Предметом оценки служат индикаторы достижения компетенций, предусмотренные ОПОП, направленные на формирование общепрофессиональных компетенций.

Таблица 2.

Элемент дисциплины	Формы и методы контроля			
	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые компетенции/ индикаторы достижения	Форма контроля	Проверяемые компетенции/ индикаторы достижения
Тема 1. Основные понятия машинного обучения.	Письменная работа №1 Устный опрос Лабораторная работа №1 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 2. Библиотека анализа данных Pandas. Numpy, DataFrame.	Письменная работа №2 Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 3. Метрические методы.	Письменная работа №3 Устный опрос Лабораторная работа №3 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 4. Типы данных, классификация задач машинного обучения.	Письменная работа №4 Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 5. Линейные методы классификации.	Письменная работа №5 Устный опрос Лабораторная работа №5 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 6. Библиотека	Письменная	ОПК-2: ОПК -2.2.	Экзаменационная	ОПК-2: ОПК -2.2.

Scikit-Learn.	работа №6 Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат		работа	
Тема 7. Метод опорных векторов. Логистическая регрессия.	Письменная работа №7 Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 8. Введение в нейронные сети.	Письменная работа №8 Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 9. Метрики качества классификации. Линейная регрессия.	Письменная работа №9 Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 10. Свёрточные нейронные сети.	Письменная работа №10 Устный опрос Лабораторная работа №10 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 11. Композиции алгоритмов.	Письменная работа №11 Устный опрос Лабораторная работа №11 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 12. Обработка текстов.	Письменная работа №12 Устный опрос Лабораторная работа №12	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.

	Самостоятельная работа Реферат			
Тема 13. Кластеризация и визуализация.	Письменная работа №13 Устный опрос Лабораторная работа №13 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 14. Прогнозирование временных рядов.	Письменная работа №14 Устный опрос Лабораторная работа №14 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 15. Машинное обучение в прикладных задачах.	Письменная работа №15 Устный опрос Лабораторная работа №15 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.
Тема 16. Задачи машинного обучения по обработке изображений.	Письменная работа №16 Устный опрос Лабораторная работа №16 Самостоятельная работа Реферат	ОПК-2: ОПК -2.2.	Экзаменационная работа	ОПК-2: ОПК -2.2.

3.2. Перечень заданий для текущего контроля

Формируемая компетенция: ОПК-2

Перечень заданий закрытого типа

Задание № 1. При проектировании системы для выявления неизвестных аномалий в сетевом трафике, для которой отсутствуют размеченные данные об атаках, какой класс методов машинного обучения является предпочтительным?

A) Обучение с учителем.
B) Обучение с подкреплением.
C) Обучение без учителя.
D) Глубокое обучение.
E) Смешанное обучение.

Задание № 2. Если модель классификации для обнаружения вредоносных файлов демонстрирует высокую точность на обучающих данных, но низкую — на новых, как называется эта проблема?

A) Недообучение.
B) Регуляризация.
C) Нормализация.
D) Переобучение.
E) Оптимизация.

Задание № 3. Установите соответствие между задачей защиты информации и наиболее подходящим для её решения алгоритмом машинного обучения.

Задача защиты информации	**Алгоритм машинного обучения**
1. Классификация сетевых пакетов на легитимные и атаки типа DDoS.	A) Кластеризация (K-means).
2. Обнаружение новых, ранее не встречавшихся типов вредоносного ПО по схожести поведения.	B) Метод опорных векторов (SVM).
3. Снижение размерности признакового пространства для ускорения анализа больших объёмов логов.	C) Логистическая регрессия.
4. Прогнозирование вероятности успешной эксплуатации уязвимости.	D) Метод главных компонент (PCA).

Задание № 4. Установите соответствие между методом решения проблемы переобучения модели и его кратким описанием.

Метод борьбы с переобучением	**Описание метода**
1. Регуляризация.	A) Добавление в обучающий набор искусственно созданных примеров.
2. Увеличение данных.	B) Исключение части нейронов сети на каждом шаге обучения.
3. Упрощение модели.	C) Добавление в функцию ошибки штрафа за сложность модели.

Метод борьбы с переобучением	Описание метода
4. Отсев.	D) Уменьшение количества параметров или слоёв модели.

Задание № 5. Установите правильную последовательность этапов разработки и обоснования выбора модели машинного обучения для системы обнаружения вторжений.
а) Оценка качества модели на тестовой выборке с использованием метрик (полнота, F-мера).
б) Сбор и предобработка сетевых логов и данных об атаках.
в) Обучение нескольких моделей-кандидатов на тренировочной выборке.
г) Анализ предметной области и формализация задачи как задачи классификации.
д) Выбор итоговой модели с обоснованием её преимуществ по точности и скорости.

Перечень заданий открытого типа

Задание № 1. Как называется базовый алгоритм кластеризации, используемый для поиска аномальных групп событий в логах безопасности?

Задание № 2. Как называется метод проверки, при котором данные разбиваются на k блоков, каждый из которых по очереди становится тестовой выборкой?

Задание № 3. Как называется основная библиотека Python для реализации классических алгоритмов машинного обучения, таких как SVM и решающие деревья?

Задание № 4. Дополните определение, вставляя пропущенное слово:
Графическое представление зависимости ошибки модели на обучающей и проверочной выборках от её сложности или количества итераций обучения называется кривой _____.

Задание № 5. Дополните определение, вставляя пропущенное слово:
Процесс автоматического подбора наилучших внутренних параметров алгоритма машинного обучения, таких как глубина дерева или скорость обучения, называется _____ гиперпараметров.

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: ОПК-2

Перечень заданий закрытого типа

Задание № 1. При проектировании системы для выявления неизвестных аномалий в сетевом трафике, для которой отсутствуют размеченные данные об атаках, какой класс методов машинного обучения является предпочтительным?

A) Обучение с учителем.
B) Обучение с подкреплением.
C) Обучение без учителя.
D) Глубокое обучение.
E) Смешанное обучение.

Задание № 2. Если модель классификации для обнаружения вредоносных файлов демонстрирует высокую точность на обучающих данных, но низкую — на новых, как называется эта проблема?

A) Недообучение.
B) Регуляризация.
C) Нормализация.
D) Переобучение.
E) Оптимизация.

Задание № 3. Какой метод композиции алгоритмов, основанный на построении ансамбля из множества решающих деревьев, часто выбирают для задач классификации в кибербезопасности из-за высокой устойчивости к переобучению?

A) Метод опорных векторов.
B) Градиентный бустинг.
C) Логистическая регрессия.
D) Случайный лес.
E) Метод ближайших соседей.

Задание № 4. При необходимости разработать компонент для анализа содержимого вредоносных исполняемых файлов, представленных в виде изображений, какой тип нейронной сети следует обоснованно выбрать?

A) Полносвязная сеть.
B) Сверточная сеть.
C) Рекуррентная сеть.
D) Автокодировщик.
E) Персептрон.

Задание № 5. Какой основной метод регуляризации используется для борьбы с переобучением в логистической регрессии и линейных моделях путём добавления штрафа за большие веса?

A) Уменьшение выборки.
B) Ранняя остановка.
C) Отсев.
D) Гребневая регрессия.
E) Увеличение данных.

Задание № 6. Для решения задачи бинарной классификации «нормальный трафик — атака» с высоким требованием к минимизации пропусков атак, на какую метрику качества следует в первую очередь ориентироваться при выборе модели?

A) Точность.
B) Аккуратность.

C) Полнота.
D) F-мера.
E) ROC-AUC.

Задание № 7. Установите соответствие между задачей защиты информации и наиболее подходящим для её решения алгоритмом машинного обучения.

Задача защиты информации	**Алгоритм машинного обучения**
1. Классификация сетевых пакетов на легитимные и атаки типа DDoS.	A) Кластеризация (K-means).
2. Обнаружение новых, ранее не встречавшихся типов вредоносного ПО по схожести поведения.	B) Метод опорных векторов (SVM).
3. Снижение размерности признакового пространства для ускорения анализа больших объёмов логов.	C) Логистическая регрессия.
4. Прогнозирование вероятности успешной эксплуатации уязвимости.	D) Метод главных компонент (PCA).

Задание № 8. Установите соответствие между методом решения проблемы переобучения модели и его кратким описанием.

Метод борьбы с переобучением	**Описание метода**
1. Регуляризация.	A) Добавление в обучающий набор искусственно созданных примеров.
2. Увеличение данных.	B) Исключение части нейронов сети на каждом шаге обучения.
3. Упрощение модели.	C) Добавление в функцию ошибки штрафа за сложность модели.
4. Отсев.	D) Уменьшение количества параметров или слоёв модели.

Задание № 9. Установите правильную последовательность этапов разработки и обоснования выбора модели машинного обучения для системы обнаружения вторжений.
а) Оценка качества модели на тестовой выборке с использованием метрик (полнота, F-мера).
б) Сбор и предобработка сетевых логов и данных об атаках.
в) Обучение нескольких моделей-кандидатов на тренировочной выборке.
г) Анализ предметной области и формализация задачи как задачи классификации.
д) Выбор итоговой модели с обоснованием её преимуществ по точности и скорости.

Задание № 10. Установите правильную последовательность шагов для применения регуляризации при обучении модели логистической регрессии с целью избежать переобучения.
а) Выбор оптимального коэффициента регуляризации с помощью кросс-валидации.
б) Добавление регуляризационного штрафа в функцию потерь модели.
в) Определение необходимости регуляризации по высокой разнице в ошибке на обучающей и валидационной выборках.
г) Переобучение итоговой модели с выбранным коэффициентом на всех данных.

д) Тестирование регуляризованной модели на отложенной тестовой выборке.

Перечень заданий открытого типа

Задание № 1. Как называется базовый алгоритм кластеризации, используемый для поиска аномальных групп событий в логах безопасности?

Задание № 2. Как называется метод проверки, при котором данные разбиваются на k блоков, каждый из которых по очереди становится тестовой выборкой?

Задание № 3. Как называется основная библиотека Python для реализации классических алгоритмов машинного обучения, таких как SVM и решающие деревья?

Задание № 4. Как называется метрика, гармонически усредняющая точность и полноту для оценки классификатора?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Графическое представление зависимости ошибки модели на обучающей и проверочной выборках от её сложности или количества итераций обучения называется кривой _____.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Процесс автоматического подбора наилучших внутренних параметров алгоритма машинного обучения, таких как глубина дерева или скорость обучения, называется _____ гиперпараметров.

5. КРИТЕРИИ ОЦЕНКИ

5.1. Критерии оценки текущего контроля и промежуточной аттестации

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности обучающихся. В соответствии с этой системой применяются пятибалльная, двадцати бальная и стобалльная шкалы знаний, умений, навыков.

Таблица 3.

Шкалы оценивания			**Критерии оценивания**
пятибалльная	двадцати бальная	стобалльная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение 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» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

Критерии оценки тестовых заданий

Таблица 4.

Процент выполненных тестовых заданий	**Оценка**
до 50%	неудовлетворительно
50-69%	удовлетворительно
70-84%	хорошо
85-100%	отлично

Критерии оценки тестовых заданий, заданий на дополнение, с развернутым ответом и на установление правильной последовательности

Верный ответ - 2 балла.
Неверный ответ или его отсутствие - 0 баллов.

Критерии оценки заданий на сопоставление

Верный ответ - 2 балла
1 ошибка - 1 балл
более 1-й ошибки или ответ отсутствует - 0 баллов.

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Таблица 5.

Формируемые компетенции	№ задания	Ответ
ОПК-2	**Задания закрытого типа**	
	№ 1	C
	№ 2	D
	№ 3	1 – C, 2 – A, 3 – D, 4 – B
	№ 4	C, 2 – A, 3 – D, 4 – B
	№ 5	г б в а д
	Задания открытого типа	
	№ 1	K-средних
	№ 2	Кросс-валидация
	№ 3	Scikit-learn
	№ 4	Обучения
	№ 5	Тюнингом

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

Формируемые компетенции	**№ задания**	**Ответ**
ОПК-2	**Задания закрытого типа**	
	№ 1	C
	№ 2	D
	№ 3	D
	№ 4	B
	№ 5	D
	№ 6	C
	№ 7	1 – C, 2 – A, 3 – D, 4 – B
	№ 8	C, 2 – A, 3 – D, 4 – B
	№ 9	г б в а д
	№ 10	в б а г д
	Задания открытого типа	
	№ 1	K-средних
	№ 2	Кросс-валидация
	№ 3	Scikit-learn
	№ 4	F-мера
	№ 5	Обучения
	№ 6	Тюнингом