Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 16.06.2026 10:24:26
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1a8

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационных технологий»
_____ / Д.Г. Демидов /
«26» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы машинного обучения и технологии искусственного интеллекта»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2026 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:
Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине 4
2. Цели, задачи и планируемые результаты обучения по дисциплине 5
3. Структура и содержание дисциплины....5
3.1. Виды учебной работы и трудоемкость 5
3.2. Тематический план изучения дисциплины 6
3.3. Содержание дисциплины 7
3.4. Тематика семинарских/практических и лабораторных занятий 8
3.5. Тематика курсовых проектов (курсовых работ) 9
4. Учебно-методическое и информационное обеспечение....9
4.1. Нормативные документы и ГОСТы 9
4.2. Основная литература 10
4.3. Дополнительная литература 10
4.4. Электронные образовательные ресурсы....11
4.5 Лицензионное и свободно распространяемое программное обеспечение....11
4.6 Современные профессиональные базы данных и информационные справочные системы....11
5. Материально-техническое обеспечение....11
6. Методические рекомендации 11
6.1 Методические рекомендации для преподавателя по организации обучения 11
6.2 Методические указания для обучающихся по освоению дисциплины....12
7 Фонд оценочных средств 13
7.1 Методы контроля и оценивания результатов обучения....13
7.2 Шкала и критерии оценивания результатов обучения....13
7.3 Оценочные средства 14

1. Цели, задачи и планируемые результаты обучения по дисциплине

К основным **целям** освоения дисциплины «Методы машинного обучения и технологии искусственного интеллекта» следует отнести:

- изучение современных методов и технологий машинного обучения и искусственного интеллекта для решения прикладных задач анализа данных, распознавания образов, прогнозирования и поддержки принятия решений;
- формирование навыков разработки, обучения и оптимизации моделей машинного обучения для интеллектуальных информационных систем;
- развитие компетенций по выбору, оценке и внедрению алгоритмов искусственного интеллекта в профессиональной деятельности;
- подготовка специалистов, способных применять технологии искусственного интеллекта для автоматизации процессов и повышения эффективности цифровых решений.

К основным **задачам** освоения дисциплины «Методы машинного обучения и технологии искусственного интеллекта» следует отнести:

- освоение математических и алгоритмических основ машинного обучения и искусственного интеллекта;
- изучение методов обучения с учителем и без учителя, а также современных подходов глубокого обучения;
- формирование навыков подготовки, анализа и визуализации данных для построения моделей;
- освоение методов оценки качества моделей и повышения их обобщающей способности;
- изучение инструментальных средств и библиотек для разработки и внедрения моделей машинного обучения;
- формирование практических навыков решения прикладных задач с использованием технологий искусственного интеллекта.

Обучение по дисциплине «Методы машинного обучения и технологии искусственного интеллекта» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения	знать: • основные технологии создания и внедрения информационных систем; • стандарты управления жизненным циклом информационной системы. уметь: • проектировать блоксхемы алгоритмов; оценивать производительность алгоритмов и затраты памяти на работу алгоритма;

	• разрабатывать программы на основе спроектированного алгоритма и проводить отладку программы; • применять методы системного анализа и математического моделирования при разработке и эксплуатации ИС; • проводить структурный анализ, функциональный анализ, объектно-ориентированный анализ иерархии классов; • осуществлять организационное обеспечение выполнения работ на всех стадиях и в процессах жизненного цикла информационной системы. владеть: • навыками разработки программ, построения блок-схем алгоритмов и оценки производительности алгоритмов, работы с унифицированным языком визуального моделирования, составления плановой и отчетной документации по управлению проектами создания информационных систем на стадиях жизненного цикла.

2. Цели, задачи и планируемые результаты обучения по дисциплине

Дисциплина «Методы машинного обучения и технологии искусственного интеллекта» относится к числу учебных дисциплин блока 1 обязательной части (Б1.1) основной образовательной программы (Б1.1.42).

Дисциплина логически и содержательно-методически взаимосвязана со следующими дисциплинами и практиками ООП: «Языки программирования» «Математические методы анализа данных».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1. Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	9	
	В том числе:			
1.1	Лекции	18	9	
1.2	Семинарские/практические занятия	-		
1.3	Лабораторные занятия	**54**	9	
2	**Самостоятельная работа**	**72**	9	
3	**Промежуточная аттестация**			
	Экзамен		9	По расписанию
	Итого	**144**		

3.2. Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Основы машинного обучения и ИИ						
1.1	Тема 1. Введение в ИИ и ML. Типы задач, история, области применения	11	1		5		5
1.2	Тема 2. Математические основы: линейная алгебра, вероятности, оптимизация, метрики моделей	13	3		5		5
1.3	Тема 3. Классические методы: регрессия, классификация, SVM, деревья, ансамбли (Random Forest, GBM)	15	2		5		8
1.4	Тема 4. Глубокое обучение: нейронные сети, CNN, RNN, Transformers (основы)	15	2		5		8
1.5	Тема 5. Обучение без учителя: кластеризация, снижение размерности, обнаружение аномалий	12	2		5		5
2	Раздел 2. Современные технологии и подходы ИИ						
2.1	Тема 1. Обработка естественного языка (NLP): embeddings, Transformers, LLM	15	2		5		8

2.2	Тема 2. Компьютерное зрение: CNN, современные архитектуры, детекция и сегментация	11	1		5		5
2.3	Тема 3. Генеративные модели: VAEs, GAN, диффузия, основы больших языковых моделей	14	1		5		8
2.4	Тема 4. Обучение с подкреплением и масштабируемое ML (основы RL + MLOps, distributed training)	11	1		5		5
3	Раздел 3. Применение, безопасность и ответственность ИИ						
3.1	Тема 1. MLOps и жизненный цикл моделей: эксперименты, мониторинг, CI/CD для ML	11	1		5		5
3.2	Тема 2. Безопасность ИИ: adversarial атаки, poisoning, защита (adversarial training, DP)	8	1		2		5
3.3	Тема 3. Интерпретируемость и этика ИИ: XAI (SHAP, LIME), bias, fairness, регуляция (EU AI Act, РФ)	8	1		2		5
Итого		**144**	**18**		**54**		**72**

3.3. Содержание дисциплины

Раздел 1. Основы машинного обучения и ИИ

Раздел 1. Основы машинного обучения и ИИ

Тема 1.1. Введение в ИИ и машинное обучение

История развития искусственного интеллекта и машинного обучения. Современные тенденции развития ИИ. Типы задач машинного обучения. Основные области применения ИИ.

Тема 1.2. Математические основы

Векторные пространства и линейная алгебра. Метрики расстояний и сходства. Вероятностные модели и байесовский подход. Основы оптимизации. Функции потерь и метрики качества моделей.

Тема 1.3. Классические методы supervised learning

Методы классификации. Методы регрессии. Регуляризация. Обработка несбалансированных классов. Feature engineering. Подбор гиперпараметров.

Тема 1.4. Глубокое обучение

Основы нейронных сетей. Архитектуры нейронных сетей. Современные практики обучения.

Тема 1.5. Обучение без учителя

Методы кластеризации. Снижение размерности. Обнаружение аномалий. Самообучение и контрастивное обучение.

Раздел 2. Современные технологии и подходы ИИ

Тема 2.1. Обработка естественного языка

Word embeddings. Модели на основе Transformer. Основные задачи обработки текста. Современные подходы к обучению и генерации.

Тема 2.2. Компьютерное зрение

Архитектуры для компьютерного зрения. Основные задачи компьютерного зрения. Современные тенденции.

Тема 2.3. Генеративные модели

Автоэнкодеры и вариационные автоэнкодеры. Генеративно-состязательные сети. Диффузионные модели. Большие языковые модели.

Тема 2.4. Обучение с подкреплением и масштабируемое обучение

Основы обучения с подкреплением. Масштабируемое машинное обучение. Основы MLOps.

Раздел 3. Применение, безопасность и ответственность ИИ

Тема 3.1. MLOps и жизненный цикл моделей

Эксперименты и трекинг. Версионирование данных и моделей. Мониторинг и автоматическое переобучение.

Тема 3.2. Безопасность ИИ-систем

Угрозы ИИ-системам. Методы защиты моделей.

Тема 3.3. Интерпретируемость, этика и регуляция ИИ

Методы explainable AI. Проблемы bias и fairness. Регуляторные рамки и стандарты ИИ.

3.4. Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены программой.

3.4.2 Лабораторные занятия

Лабораторная работа 1.1: реализовать и сравнить логистическую регрессию, svm и деревья решений на датасетах фишинга, вредоносного ПО или сетевых аномалий. Оценить accuracy, precision, recall, f1, roc-auc, pr-auc. Построить confusion matrix, roc-кривые, feature importance.

Лабораторная работа 1.2: реализовать и сравнить random forest, xgboost, lightgbm, catboost. Обработать дисбаланс классов (class_weight, smote). Применить на датасетах фишинга или ВПО. Сравнить время обучения/инференса, метрики и feature importance. Оптимизировать гиперпараметры.

Лабораторная работа 2.1: реализовать isolation forest, one-class svm, autoencoder и local outlier factor для обнаружения аномалий на сетевых датасетах или логах. Оценить по roc-auc и precision@rank. Визуализировать аномалии (t-sne/umap). Сравнить с supervised подходом.

Лабораторная работа 2.2: реализовать кластеризацию (k-means, dbscan, hdbscan) и снижение размерности (pca, t-sne, umap) на датасетах malware или сетевых потоков. Визуализировать кластеры. Оценить качество кластеризации и интерпретировать группы как семейства угроз.

Лабораторная работа 3.1: реализовать cnn для классификации pe-файлов как изображений или последовательностей признаков. Применить на датасетах ember, virus-mnist или cic-malMem. Сравнить с классическими методами (random forest/xgboost).

Лабораторная работа 3.2: реализовать rnn/lstm/gru и простой transformer для анализа последовательностей (трафик, системные вызовы, логи). Применить на датасетах cic-ids2017 или android malware. Оценить f1, roc-auc. Сравнить с xgboost на агрегированных признаках

Лабораторная работа 4.1: реализовать модели nlp для обнаружения фишинга: tf-idf + ml (logistic regression, svm) и fine-tuning bert/roberta/distilbert. Применить на датасетах phishing email или url. Оценить метрики, проанализировать ошибки, визуализировать attention/feature importance.

Лабораторная работа 4.2: построить mlops-пайплайн: трекинг экспериментов (mlflow или wandb), версионирование (dvc), логирование метрик. Применить на задаче классификации фишинга или malware. Сравнить модели и воспроизвести результаты.

Лабораторная работа 5.1: реализовать adversarial атаки (fgsm, pgd) на обученной модели (фишинг или malware). Оценить падение точности. Применить базовую защиту (adversarial training). Сравнить результаты до и после.

Лабораторная работа 5.2: реализовать методы explainability (shap, lime, permutation importance, integrated gradients) на моделях из предыдущих работ. Визуализировать важность признаков и объяснить ошибки модели.

3.5. Тематика курсовых проектов (курсовых работ)

Темы курсовых работ:

1. Обнаружение аномалий в сетевом трафике с использованием методов глубокого обучения
2. Классификация вредоносного ПО с помощью алгоритмов машинного обучения
3. Генеративно-состязательные сети (GAN) для создания и обнаружения фишинговых веб-страниц
4. Методы обработки естественного языка (NLP) для анализа текстовых угроз в социальных сетях
5. Обнаружение атак на основе данных журналов событий (SIEM) с применением ансамблевых методов
6. Адверсарные атаки на модели машинного обучения: методы защиты в системах информационной безопасности
7. Детектирование ботнетов на основе поведения устройств в IoT-сетях
8. Кластеризация данных для выявления скрытых угроз в корпоративных сетях
9. Машинное обучение в стеганографии: обнаружение скрытых сообщений в мультимедийных файлах
10. Использование машинного обучения для анализа уязвимостей в программном обеспечении

4. Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: Текст: электронный // КонсультантПлюс. – URL:

http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 23.02.2026).

2. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований к защите информации, содержащейся в государственных информационных системах, информационных системах государственных органов, органов местного самоуправления, государственных и муниципальных учреждений, иных организаций, создаваемых для выполнения государственных и муниципальных функций» (вступ. в силу 01.03.2026): Текст: электронный // Официальный сайт ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117 (дата обращения: 23.02.2026).

4.2. Основная литература

1. Платонов, А. В. Машинное обучение : учебное пособие для вузов / А. В. Платонов. — Москва : Издательство Юрайт, 2023. — 85 с. — (Высшее образование). — ISBN 978-5-534-15561-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520544 (дата обращения: 23.02.2026).
2. Воронов, М. В. Системы искусственного интеллекта : учебник и практикум для вузов / М. В. Воронов, В. И. Пименов, И. А. Небаев. — Москва : Издательство Юрайт, 2023. — 256 с. — (Высшее образование). — ISBN 978-5-534-14916-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519916 (дата обращения: 23.02.2026).
3. Иванов, В. М. Интеллектуальные системы : учебное пособие для вузов / В. М. Иванов ; под науч. ред. А. Н. Сесекина. — Москва : Издательство Юрайт, 2022. — 91 с. — (Высшее образование). — ISBN 978-5-534-00551-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/492094 (дата обращения: 23.02.2026).
4. Загорулько, Ю. А. Искусственный интеллект. Инженерия знаний : учебное пособие для вузов / Ю. А. Загорулько, Г. Б. Загорулько. — Москва : Издательство Юрайт, 2022. — 93 с. — (Высшее образование). — ISBN 978-5-534-07198-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494205 (дата обращения: 23.02.2026).

4.3. Дополнительная литература

1. Бессмертный, И. А. Системы искусственного интеллекта : учебное пособие для вузов / И. А. Бессмертный. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 157 с. — (Высшее образование). — ISBN 978-5-534-07467-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512657 (дата обращения: 23.02.2026).

2. Анализ данных : учебник для вузов / В. С. Мхитарян [и др.] ; под ред. В. С. Мхитаряна. — Москва : Издательство Юрайт, 2023. — 490 с. — (Высшее образование). — ISBN 978-5-534-00616-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511020 (дата обращения: 23.02.2026).

4.4. Электронные образовательные ресурсы

Электронный образовательный ресурс в разработке

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
2. Python 3.10–3.12 (устанавливается через официальный сайт python.org или через Anaconda/Miniconda)
3. Anaconda / Miniconda
4. Git (для скачивания датасетов и репозиториев с GitHub)
5. Visual Studio Code (бесплатный редактор кода с расширениями Python, Jupyter, Git) или PyCharm Community Edition (бесплатная версия)

4.6 Современные профессиональные базы данных и информационные справочные системы

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 23.02.2026). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 23.02.2026). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 23.02.2026). - Текст: электронный.

5. Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран или интерактивная доска) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6. Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к лабораторным работам следует предварительно проработать теоретический материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать правильность выполнения лабораторных работ на всех этапах.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Лабораторные работы проводятся по теоретическим и проблемным вопросам ИБ. Лабораторные работы предполагает творческие дискуссии, активный обмен мнениями по поставленным вопросам, заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении лабораторной работы преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на лабораторной работе учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала,

	но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопросов для экзамена по дисциплине:

1. Какие основные типы задач машинного обучения чаще всего применяются в задачах информационной безопасности?
2. В чём разница между обучением с учителем, обучением без учителя и обучением с подкреплением в контексте обнаружения киберугроз?
3. Перечислите и кратко опишите ключевые метрики качества моделей классификации, используемые при сильном дисбалансе классов (например, в задачах обнаружения атак).
4. Какие преимущества и недостатки имеет метод опорных векторов (SVM) при решении задач классификации вредоносного ПО?
5. Объясните принцип работы градиентного бустинга (на примере XGBoost или LightGBM). Почему эти алгоритмы часто показывают лучшие результаты в задачах обнаружения угроз по сравнению с одиночными деревьями решений?
6. В чём заключается проблема «проклятия размерности» и как с ней борются при анализе больших наборов признаков в задачах информационной безопасности?
7. Опишите основные этапы предобработки данных при работе с сетевым трафиком (на примере датасетов CIC-IDS2017 или UNSW-NB15).
8. Что такое обнаружение аномалий? Перечислите и кратко охарактеризуйте 3–4 популярных алгоритма обнаружения аномалий без учителя.
9. Как автоэнкодеры применяются для обнаружения аномалий? Объясните принцип работы реконструктивного автоэнкодера и как по ошибке реконструкции выявлять аномалии.

10. В чём разница между бинарной и многоклассовой классификацией вредоносного ПО? Какие трудности возникают при многоклассовой постановке задачи?
11. Опишите архитектуру свёрточной нейронной сети (CNN) и объясните, почему она эффективна при анализе статических признаков PE-файлов или визуализации вредоносного кода.
12. Как работают рекуррентные нейронные сети (RNN/LSTM) при анализе последовательных данных? Приведите примеры последовательностей, которые анализируют в задачах кибербезопасности.
13. Что такое Transformer-архитектура? В чём её преимущество перед RNN при обработке длинных последовательностей (логи, сетевой трафик, последовательности системных вызовов)?
14. Перечислите и кратко опишите основные типы adversarial атак на модели машинного обучения. Приведите примеры атак, актуальных для систем обнаружения вторжений.
15. Что такое adversarial training? Как этот метод повышает устойчивость модели к adversarial примерам?
16. Объясните разницу между data poisoning и model poisoning. Как эти атаки могут быть реализованы в реальных системах ИИ для кибербезопасности?
17. Что такое differential privacy? Как этот подход может использоваться для защиты конфиденциальности при обучении моделей на чувствительных данных (логи пользователей, корпоративные данные)?
18. Перечислите основные методы интерпретируемости моделей (XAI), которые применяются для объяснения решений моделей в задачах информационной безопасности.
19. Что показывает значение SHAP-value для конкретного признака? Как интерпретировать summary plot и force plot в библиотеке SHAP?
20. Назовите ключевые этапы жизненного цикла модели в MLOps. Какие проблемы возникают при эксплуатации моделей обнаружения угроз в условиях постоянно меняющегося ландшафта атак?
21. Что такое concept drift и data drift? Как их своевременно обнаруживать и как адаптировать модель в production?
22. Перечислите основные угрозы безопасности самих систем искусственного интеллекта (по классификации OWASP Top 10 for LLM или MITRE ATLAS).
23. Что такое prompt injection? Приведите пример атаки на большую языковую модель, используемую в SOC или threat intelligence.
24. Какие требования предъявляют российские нормативные документы (ФСТЭК, приказы №17, №239 и др.) к применению технологий ИИ в критически важных информационных инфраструктурах?
25. Опишите уровни риска ИИ-систем по классификации EU AI Act. К каким категориям относятся большинство моделей, применяемых в кибербезопасности?