Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Уровень образования: магистратура
(бакалавриат/магистратура/специалитет)

Направление подготовки магистратуры: 10.04.01 Информационная безопасность
(код, наименование направления подготовки)

Направленность: Киберразведка 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 программы практической подготовки в форме преддипломной практики и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. самостоятельной работе обучающихся), освоивших программу данной практики.

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.

Программой практической подготовки в форме преддипломной практики предусмотрено формирование следующих компетенций:

1) ПК-1 Способен разрабатывать и применять процедуры и интеллектуальные средства информационно-аналитических систем поддержки принятия решений по обеспечению информационной безопасности;
2) ПК-2 Способен выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности;
3) ПК-3 Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта;
4) ПК-4 Способен разрабатывать и применять методы и алгоритмы машинного обучения для решения задач искусственного интеллекта;
5) ПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях;
6) ПК-6 Способен выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем искусственного интеллекта по обеспечению требуемых критериев эффективности и качества функционирования;
7) ПК-7 Способен руководить проектами по созданию комплексных систем искусственного интеллекта;
8) ПК-8 Способен руководить проектами по созданию, поддержке и использованию систем искусственного интеллекта на основе нейросетевых моделей и методов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ Преддипломной ПРАКТИКИ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

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

Таблица 1.

Результаты обучения: индикаторы достижения	Формируемые компетенции
ПК – 1.1 Способен решать задачи анализа данных в целях обеспечения информационной безопасности	ПК-1
ПК – 1.2 Способен интерпретировать и использовать результаты решения информационно-аналитических задач безопасности	
ПК – 1.3 Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности	
ПК – 2.1 Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности	ПК-2

ПК – 2.2 Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности	
ПК –3.1 Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области	ПК-3
ПК – 4.1 Ставит задачи по разработке или совершенствованию методов и алгоритмов для решения комплекса задач предметной области	ПК-4
ПК – 4.2 Разрабатывает унифицированные и обновляет методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий	
ПК – 5.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК-5
ПК – 6.1 Выбирает и разрабатывает программные компоненты систем искусственного интеллекта	ПК-6
ПК – 6.2 Проводит экспериментальную проверку работоспособности систем искусственного интеллекта	
ПК – 7.1 Руководит разработкой искусственного интеллекта	ПК-7
ПК – 8.1 Руководит работами по оценке и выбору моделей искусственных нейронных сетей и инструментальных средств для решения поставленных задач	ПК-8

3. ОЦЕНКА ОСВОЕНИЯ Преддипломной ПРАКТИКИ

3.1. Контроль и оценка освоения преддипломной практики по разделам (этапам)

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

Таблица 2.

Элемент производственной (технологической) практики	**Формы и методы контроля**			
	Текущий контроль		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые компетенции/ индикаторы достижения**	**Форма контроля**	**Проверяемые компетенции/ индикаторы достижения**
Организационно-подготовительный этап	Собеседование с руководителем. Утверждение индивидуального плана	ПК-1: ПК-1.1, ПК-1.2, ПК-1.3; ПК-2: ПК-2.1, ПК-2.2, ПК-3: ПК-3.1; ПК-4: ПК-4.1, ПК-4.2; ПК-5: ПК-5.1; ПК-6: ПК-6.1, ПК-6.2; ПК-7: ПК-7.1; ПК-8: ПК-8.1	Собеседование с руководителем. Утверждение индивидуального плана	ПК-1: ПК-1.1, ПК-1.2, ПК-1.3; ПК-2: ПК-2.1, ПК-2.2, ПК-3: ПК-3.1; ПК-4: ПК-4.1, ПК-4.2; ПК-5: ПК-5.1; ПК-6: ПК-6.1, ПК-6.2; ПК-7: ПК-7.1; ПК-8: ПК-8.1
Завершение научно-исследовательской работы и доработка ВКР	Промежуточные консультации. Проверка руководителем текста глав ВКР, результатов экспериментов, исходного кода	ПК-1: ПК-1.1, ПК-1.2; ПК-2: ПК-2.1, ПК-2.2; ПК-4: ПК-4.1; ПК-6: ПК-6.1, ПК-6.2; ПК-8: ПК-8.1	Промежуточные консультации. Проверка руководителем текста глав ВКР, результатов экспериментов, исходного кода	ПК-1: ПК-1.1, ПК-1.2; ПК-2: ПК-2.1, ПК-2.2; ПК-4: ПК-4.1; ПК-6: ПК-6.1, ПК-6.2; ПК-8: ПК-8.1
Оформление выпускной квалификационной работы	Проверка текста ВКР на соответствие требованиям. Справка о результатах проверки на антиплагиат. Заключение нормоконтролера	ПК-1: ПК-1.3; ПК-4: ПК-4.2; ПК-5: ПК-5.1	Проверка текста ВКР на соответствие требованиям. Справка о результатах проверки на антиплагиат. Заключение	ПК-1: ПК-1.3; ПК-4: ПК-4.2; ПК-5: ПК-5.1

			нормоконтролера	
Подготовка к защите ВКР	Предзащита ВКР на кафедре. Проверка презентации и доклада	ПК-3: ПК-3.1, ПК-7: ПК-7.1	Предзащита ВКР на кафедре. Проверка презентации и доклада	ПК-3: ПК-3.1, ПК-7: ПК-7.1
Итоговая аттестация по практике	Защита отчета. Зачет с оценкой.	ПК-1: ПК-1.1, ПК-1.2, ПК-1.3; ПК-2: ПК-2.1, ПК-2.2; ПК-3: ПК-3.1; ПК-4: ПК-4.1, ПК-4.2; ПК-5: ПК-5.1; ПК-6: ПК-6.1, ПК-6.2; ПК-7: ПК-7.1; ПК-8: ПК-8.1	Защита отчета. Зачет с оценкой.	ПК-1: ПК-1.1, ПК-1.2, ПК-1.3; ПК-2: ПК-2.1, ПК-2.2; ПК-3: ПК-3.1; ПК-4: ПК-4.1, ПК-4.2; ПК-5: ПК-5.1; ПК-6: ПК-6.1, ПК-6.2; ПК-7: ПК-7.1; ПК-8: ПК-8.1

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: ПК- 1

Перечень заданий закрытого типа

Задание № 1. Какой основной тип задачи машинного обучения решается при создании модели для автоматического определения, является ли сетевой пакет частью DDoS-атаки или легитимного трафика?

A) Кластеризация.
B) Регрессия.
C) Понижение размерности.
D) Классификация.
E) Ассоциативные правила.

Задание № 2. Какая библиотека Python является стандартом для реализации классических алгоритмов машинного обучения, таких как логистическая регрессия, SVM и Random Forest, и часто используется для быстрого прототипирования решений?

A) TensorFlow.
B) PyTorch.
C) Scikit-learn.
D) Keras.
E) XGBoost.

Задание № 3. Какой метод машинного обучения без учителя может быть первым этапом для исследования логов безопасности с целью обнаружения ранее неизвестных группировок аномальных событий?

A) Линейная регрессия.
B) Кластеризация.
C) Классификация.
D) Градиентный бустинг.
E) Сверточные нейронные сети.

Задание № 4. Какой алгоритм, основанный на ансамбле деревьев решений и известный высокой точностью, часто применяется в задачах классификации угроз информационной безопасности?

A) Метод k-ближайших соседей.
B) Наивный байесовский классификатор.
C) Случайный лес (Random Forest).
D) Однослойный персептрон.
E) Метод главных компонент.

Задание № 5. При подготовке набора данных для обучения модели классификации фишинговых URL-адресов категориальный признак «тип протокола (http/https)» необходимо преобразовать в числовой формат. Какой метод для этого чаще всего применяется?

A) Нормализация Min-Max.
B) Стандартизация Z-score.
C) Логарифмическое преобразование.
D) One-Hot Encoding (прямое кодирование).
E) Кодировка меток (Label Encoding).

Задание № 6. Как называется фундаментальная проблема, когда модель машинного обучения слишком точно подстраивается под обучающие данные, включая их шум, и плохо работает на новых данных?

A) Недообучение (Underfitting).
B) Переобучение (Overfitting).
C) Дисперсия ошибки.

D) Смещение ошибки.
E) Проклятие размерности.

Задание № 7. Установите соответствие между задачей анализа данных в области информационной безопасности и наиболее подходящим для её решения классом алгоритмов машинного обучения:

Задача в области ИБ	Класс алгоритмов
1. Прогнозирование вероятности успешного эксплуатации уязвимости на основе её характеристик.	A) Кластеризация.
2. Автоматическое разделение пользователей на группы по паттернам поведения для выявления внутренних угроз.	B) Регрессия (логистическая).
3. Определение, относится ли новый файл к вредоносному ПО, на основе анализа его признаков.	C) Классификация.
4. Выделение новых, ранее неизвестных типов сетевых атак из потока событий.	D) Кластеризация.

Задание № 8. Установите соответствие между этапом жизненного цикла модели машинного обучения и его ключевой целью при решении задач ИБ:

Этап жизненного цикла ML	Ключевая цель в контексте ИБ
1. Сбор и подготовка данных.	A) Обеспечить репрезентативность данных, очистить их от шума и преобразовать в формат для обучения.
2. Обучение модели.	B) Настроить параметры алгоритма так, чтобы он научился выявлять закономерности, характерные для угроз.
3. Валидация и тестирование.	C) Оценить, насколько точно модель обнаруживает угрозы на новых, неизвестных данных, и измерить уровень ложных срабатываний.
4. Внедрение (деплой).	D) Интегрировать модель в рабочий контур SIEM/SOC для автоматического анализа событий в реальном времени.

Задание № 9. Установите правильную последовательность этапов построения пайплайна обработки данных для обучения модели обнаружения аномалий в сетевом трафике.

а) Применение алгоритма машинного обучения (например, Isolation Forest) к обработанным данным.

б) Нормализация числовых признаков (например, объёма трафика) и кодирование категориальных (например, типа флагов TCP).

в) Сбор сырых данных из сетевых дампов и систем логирования.

г) Выделение признаков из сырых данных (например, длительность сессии, количество пакетов, порт назначения).

д) Разделение итогового набора признаков на обучающую и тестовую выборки.

Задание № 10. Установите правильную последовательность шагов для оценки эффективности модели классификации при обнаружении фишинговых писем.

а) Расчет метрик качества: точности (Accuracy), полноты (Recall), точности (Precision) и F1-меры на тестовой выборке.

б) Применение обученной модели к тестовой выборке для получения предсказаний.

в) Анализ матрицы ошибок (Confusion Matrix) для определения количества ложноположительных и ложноотрицательных срабатываний.

г) Разделение размеченного датасета писем на обучающую и тестовую части, сохраняя распределение классов.

Перечень заданий открытого типа

Задание № 1. Как называется популярный ансамблевый алгоритм, который последовательно строит деревья решений, где каждое следующее дерево обучается исправлять ошибки предыдущих?

Задание № 2. Как называется метод, при котором часть данных не используется при обучении, а откладывается для итоговой объективной проверки качества модели?

Задание № 3. Как называется процесс автоматического подбора оптимальных параметров алгоритма машинного обучения (например, глубины дерева) для повышения его эффективности?

Задание № 4. Как называется фундаментальная библиотека Python для научных вычислений, предоставляющая поддержку многомерных массивов и математических функций, и являющаяся основой для многих инструментов анализа данных?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Метрика _____, гармонически усредняющая точность (Precision) и полноту (Recall), является одной из ключевых для сбалансированной оценки моделей классификации в условиях несбалансированных данных, характерных для задач ИБ.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Процесс создания новых, более информативных признаков на основе имеющихся сырых данных (например, вычисление частоты определённых слов в логе) для повышения эффективности моделей машинного обучения называется _____ признаков.

Формируемая компетенция: ПК-2

Перечень заданий закрытого типа

Задание № 1. Какой из перечисленных элементов является ключевым компонентом формализованной процедуры мониторинга источников информации, определяющим порядок и периодичность действий?

A) Список сотрудников.
B) Алгоритм.
C) Финансовая смета.
D) Рекламный буклет.

Задание № 2. При разработке процедуры мониторига социальных сетей на предмет утечек конфиденциальной информации, какой принцип обеспечивает ее эффективность и адаптивность?

A) Полная автоматизация без участия аналитика.
B) Единоразовый запуск в начале проекта.
C) Регулярное обновление списка ключевых слов и источников.
D) Использование только платных инструментов.

Задание № 3. Для процедуры верификации индикаторов компрометации, полученных из открытых источников, в первую очередь необходимо определить:

A) Стоимость подписки на threat intelligence.
B) Критерии достоверности и перечень эталонных баз для перепроверки.
C) Цветовую схему для визуализации.

D) Количество рабочих мест для аналитиков.

Задание № 4. Какой формат документа наиболее подходит для описания стандартизированной процедуры сбора и первичной оценки данных из технических логов?

A) Поэма.
B) Регламент или инструкция.
C) Художественный рассказ.
D) Пресс-релиз.

Задание № 5. При создании процедуры кросс-платформенного мониторинга медиапространства, какой фактор является наименее значимым для ее работоспособности?

A) Юридические ограничения на сбор данных в конкретных регионах.
B) Наличие API у целевых платформ.
C) Личные предпочтения аналитика в выборе браузера.
D) Возможности инструментов для обработки больших данных.

Задание № 6. Какой этап является завершающим в цикле разработки процедуры мониторинга и подразумевает ее проверку на практике?

A) Пилотное внедрение и корректировка.
B) Написание текста.
C) Согласование с бухгалтерией.
D) Публикация в открытом доступе.

Задания № 7. Установите соответствие между этапом разработки процедуры мониторига и его ключевым результатом:

Этап разработки процедуры	**Ключевой результат**
1. Определение целей и задач	A) Чек-лист, алгоритм или пошаговая инструкция для исполнителя.
2. Выбор источников и методов	B) Конкретные измеримые показатели: количество обрабатываемых источников, время реакции.
3. Формализация последовательности действий	C) Перечень целевых платформ, поисковых запросов, инструментов и критериев оценки.
4. Определение метрик эффективности	D) Четкая формулировка: "Своевременно выявлять упоминания об уязвимостях в продуктах компании".

Задание № 8. Установите соответствие между типом источника информации в кибербразведке и рекомендуемой процедурой его первичной верификации:

Тип источника	**Рекомендуемая процедура первичной верификации**
1. Технический индикатор (IoC: хэш, IP)	A) Стилометрический анализ, проверка репутации автора, кросс-проверка с другими экспертами.
2. Новостное сообщение о кибератаке	B) Проверка в эталонных базах (VirusTotal, AbuseIPDB), анализ контекста появления.
3. Данные метаданных файла	C) Сопоставление с событиями в SIEM, проверка журналов сетевой активности.
4. Экспертное мнение в блоге	D) Проверка через архивы Интернета, установление первоисточника, анализ цитируемых данных.

Задания № 9. Установите правильную последовательность этапов разработки процедуры ежедневного мониторинга специализированных форумов и Telegram-каналов на предмет обсуждения уязвимостей:

а) Формализация шагов: сбор ссылок, парсинг, фильтрация по ключевым словам, сохранение результатов.
б) Определение целей: обнаружение обсуждений 0-day уязвимостей в заданном ПО.
в) Тестирование процедуры на исторических данных, оценка уровня ложных срабатываний.
г) Выбор конкретных форумов и каналов, составление словаря ключевых терминов и сленга.
д) Назначение ответственного и графика выполнения процедуры.

Задание № 10. Установите правильную последовательность действий при разработке процедуры реагирования на обнаруженный в открытых источниках индикатор компрометации (IoC):
а) Внесение IoC в черный список в средствах защиты (фаервол, IPS) и мониторинг их срабатываний.
б) Оценка критичности и достоверности IoC по внутренней шкале.
в) Поиск и сбор IoC из утвержденных открытых каналов (паблики, репозитории GitHub).
г) Перепроверка IoC через авторитетные платформы (VirusTotal, MISP).
д) Документирование источника, времени обнаружения и принятых мер.

Перечень заданий открытого типа

Задание № 1. Как называется стандартизированная шкала, часто используемая в разведывательных сообществах (включая киберразведку) для оценки достоверности источника и информации по буквенно-числовому коду?

Задание № 2. Какой класс инструментов используется для автоматизации сбора данных с веб-сайтов в рамках процедур OSINT-мониторинга?

Задание № 3. Как называется ключевой принцип, требующий, чтобы процедура мониторинга оставалась неизменной при смене исполнителя?

Задание № 4. Какой тип диаграммы наиболее наглядно отображает последовательность шагов формализованной процедуры?

Задание № 5. Дополните определение, вставляя пропущенное слово.
Процесс периодического пересмотра и актуализации процедур мониторинга в связи с изменением тактик противника или инфраструктуры объекта наблюдения называется _____ процедур.

Задание № 6. Дополните определение, вставляя пропущенное слово.
Набор заранее определенных правил для автоматической фильтрации и классификации собранной информации в рамках процедуры мониторинга называется _____ правилами.

Формируемая компетенция: ПК-3

Перечень заданий закрытого типа

Задание № 1. Для задачи классификации сетевых пакетов промышленного протокола Modbus TCP на нормальные и вредоносные в реальном времени, где критична низкая задержка и важна интерпретируемость решений, наиболее подходящим комплексом методов ИИ будет:
A) Ансамбль "легких" алгоритмов.
B) Глубокая сверточная нейронная сеть.
C) Генеративно-состязательная сеть.
D) Рекуррентная нейронная сеть с вниманием.

Задание № 2. При выборе инструментальных средств для создания прототипа системы прогнозирования кибератак в сети больницы, где команда обладает сильными навыками в Python, но ограничена во времени, ключевым решающим фактором будет:

A) Возможность развертывания на специализированных AI-ускорителях.
B) Наличие богатой экосистемы библиотек для быстрого прототипирования.
C) Поддержка распределенного обучения на сотнях GPU.
D) Наличие встроенных compliance-отчетов для стандарта HIPAA.

Задание № 3. Какой Python-фреймворк является специализированным инструментальным средством для исследования, генерации и защиты от состязательных атак на модели машинного обучения и должен быть выбран для соответствующих задач в ИБ?

A) Apache Spark.
B) IBM Adversarial Robustness Toolbox.
C) TensorFlow Extended.
D) MLflow.

Задание № 4. Для задачи анализа тональности текстовых сообщений в корпоративном чате на предмет внутренних угроз, где важна высокая точность понимания контекста и сленга, оптимальным выбором будет использование:

A) Метода "мешок слов" с классификатором SVM.
B) Предобученной языковой модели на архитектуре Transformer
C) Скрытой марковской модели.
D) Ручного написания правил.

Задание № 5. При выборе архитектуры системы ИИ для мониторинга видео с камер наблюдения в защищенном помещении на предмет несанкционированного доступа, ключевым нефункциональным требованием, влияющим на выбор, является:

A) Необходимость обработки потока видео в реальном времени с низкой латенцией.
B) Требование к хранению всех видеозаписей в сыром виде в течение 10 лет.
C) Наличие интерфейса на русском языке.
D) Стоимость лицензии на операционную систему для сервера.

Задание № 6. Какой метод машинного обучения является наиболее подходящим для задачи обнаружения новых, ранее неизвестных типов аномалий в поведении пользователей медицинской информационной системы, когда размеченных данных об атаках практически нет?

A) Логистическая регрессия.
B) Обучение без учителя, например, изолирующий лес (Isolation Forest) или автокодировщик.
C) Метод опорных векторов с учителем.
D) Глубокое обучение с подкреплением.

Задание № 7. Установите соответствие между особенностью предметной области и предпочтительным классом методов/инструментов ИИ для её решения.

Особенность предметной области / задачи ИБ	**Класс методов/инструментов ИИ**
1. Анализ последовательностей команд в журналах для выявления многоэтапных APT-атак.	A) Методы анализа временных рядов и последовательностей.
2. Обогащение событий SIEM контекстом из внешних источников угроз в реальном времени.	B) Интеграционные платформы и API для работы с Threat Intelligence Feeds.
3. Автоматическое категорирование инцидентов из тикетов SOC по стандартным тактикам.	C) Алгоритмы классификации текстов на основе предобученных моделей.
4. Визуализация сложных взаимосвязей	D) Инструменты для визуализации графов

между узлами сети и атакующими для расследования.	

Задание № 8. Установите соответствие между задачей в области ИБ для промышленной системы и рекомендуемым специализированным программным обеспечением или фреймворком.

Задача ИБ в АСУ ТП	**Рекомендуемое специализированное ПО / фреймворк**
1. Сбор, парсинг и нормализация данных промышленных протоколов	A) SIEM-платформа с поддержкой Industrial Add-ons.
2. Комплексная корреляция событий из IT и OT сетей, генерация алертов.	B) Специализированные средства анализа сетевого трафика АСУ ТП
3. Создание и управление плейбуками автоматического реагирования на инциденты в технологической сети.	C) Платформы класса SOAR
4. Непрерывный мониторинг активов и уязвимостей в промышленной сети.	D) Пассивные сканеры и платформы для управления активами АСУ ТП

Задание № 9. Установите правильную последовательность выбора комплекса методов и инструментов ИИ для решения задачи классификации типов атак в трафике промышленных протоколов.

а) Выбрать финальный стек технологий.

б) Сформировать список требований к решению: точность, скорость работы в реальном времени, интерпретируемость результатов, устойчивость к шуму.

в) Провести практические эксперименты с 2-3 наиболее подходящими алгоритмами на подготовленных данных.

г) Изучить особенности сетевого трафика целевых протоколов для понимания структуры данных и потенциальных аномалий.

д) Проанализировать доступные инструменты и опубликованные исследования по схожим задачам.

Задание № 10. Установите правильную последовательность выбора методов и инструментов для задачи прогнозирования отказов оборудования на основе данных вибрационных датчиков и телеметрии.

а) Провести сравнительное тестирование выбранных алгоритмов на исторических данных с известными отказами.

б) Сформулировать задачу как проблему прогнозирования временного ряда с целью заблаговременного обнаружения признаков поломки.

в) Определить критерии выбора: точность прогноза, раннее предупреждение, возможность работы в режиме реального времени, интерпретируемость.

г) Изучить предметную область: типы отказов, физику процессов, доступные датчики и характерные признаки в данных.

д) Выбрать инструментарий: библиотеки для обработки временных рядов, фреймворки машинного обучения.

Перечень заданий открытого типа

Задание № 1. При работе с конфиденциальными медицинскими данными для обучения модели, какой математический метод обеспечения приватности следует выбрать, чтобы гарантировать, что модель не запомнит и не раскроет конкретные записи из обучающей выборки?

Задание № 2. Какой открытый фреймворк от MITRE предоставляет таксономию атак на системы ИИ и должен быть использован для выбора методов тестирования и защиты разрабатываемой интеллектуальной системы?

Задание № 3. Какой класс архитектур нейронных сетей является доминирующим выбором для задач обработки естественного языка в системах анализа инцидентов и должен быть предпочтен простым методам "мешка слов" для сложных задач?

Задание № 4. Для интеграции самописной ML-модели детектирования аномалий в существующую корпоративную SIEM-систему, какой стандартный подход или формат данных следует использовать для отправки результатов?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Принцип _____ в разработке безопасных систем ИИ требует внедрения контроля безопасности на всех этапах жизненного цикла — от проектирования до эксплуатации.

Задание № 6. Дополните определение, вставляя пропущенное слово:
_____ вычислительная парадигма позволяет обрабатывать данные непосредственно на edge-устройствах, что снижает задержки и риски утечки при передаче в центр обработки.

Формируемая компетенция: ПК-4.

Перечень заданий закрытого типа

Задание № 1. При решении задачи классификации сетевых соединений на вредоносные и нормальные с использованием широко известного датасета KDD Cup 99, какой из перечисленных алгоритмов машинного обучения демонстрирует высокую точность (до 99%) и хорошую интерпретируемость за счет построения древовидной структуры правил?

A) Логистическая регрессия.
B) Метод опорных векторов (SVM).
C) Дерево решений (Decision Tree) или алгоритм на его основе (например, Random Forest).
D) Наивный байесовский классификатор.

Задание № 2. При постановке задачи по созданию системы для обнаружения ранее неизвестных (zero-day) атак в сетевом трафике, когда размеченные данные об атаках отсутствуют или крайне скудны, какой основной класс методов машинного обучения следует рассмотреть в первую очередь?

A) Методы обучения с учителем (Supervised Learning) для бинарной классификации.
B) Методы обучения без учителя (Unsupervised Learning), в частности, алгоритмы обнаружения аномалий.
C) Методы обучения с подкреплением (Reinforcement Learning).
D) Трансферное обучение (Transfer Learning) на основе предобученных моделей.

Задание № 3. Какой показатель является наиболее подходящим для оценки качества модели обнаружения вторжений, учитывая, что атаки в данных встречаются значительно реже нормального трафика (проблема несбалансированных классов)?

A) Точность (Accuracy).
B) F1-мера (F1-score), гармоническое среднее между точностью (Precision) и полнотой (Recall).
C) Среднеквадратическая ошибка (MSE).
D) Коэффициент детерминации (R^2).

Задание № 4. Для совершенствования существующей сигнатурной системы обнаружения вторжений (IDS) и повышения её эффективности против сложных, многоэтапных атак (APT) предлагается интегрировать модуль машинного обучения. Какой из подходов к архитектуре такого гибридного решения является наиболее перспективным?

A) Полная замена сигнатурного движка на одну сложную модель глубокого обучения.

B) Совместное использование сигнатурных правил для известных угроз и ML-модели для выявления аномалий и новых угроз.
C) Использование только ансамбля простых классических алгоритмов (например, Random Forest, XGBoost).
D) Отказ от правил и использование исключительно методов кластеризации.

Задание № 5. При постановке задачи разработки алгоритма для защиты от DDoS-атак на уровне приложений (L7 OSI), где вредоносные запросы могут маскироваться под легитимную активность, ключевым преимуществом использования машинного обучения будет:
A) Возможность аппаратной ускоренной фильтрации пакетов.
B) Способность анализировать поведенческие паттерны и логику запросов для их различения.
C) Бесконечная масштабируемость без дополнительных ресурсов.
D) Полное отсутствие ложных срабатываний.

Задание № 6. Для решения проблемы недостатка размеченных данных при обучении модели глубокого обучения для обнаружения вторжений наиболее перспективным направлением исследований и разработки является:
A) Увеличение размера нейронной сети.
B) Применение методов трансферного обучения (Transfer Learning) или обучения с самоконтролем (Self-Supervised Learning).
C) Исключительное использование алгоритмов на основе деревьев решений.
D) Ручная разметка всех входящих сетевых пакетов.

Задание № 7. Установите соответствие между типом алгоритма машинного обучения и задачей обнаружения вторжений, для решения которой он наиболее применим.

Алгоритм / Метод ML	**Задача в обнаружении вторжений**
1. Изолирующий лес (Isolation Forest)	A) Классификация сетевых соединений по известным типам атак (DoS, Probe, R2L, U2R) на основе размеченного датасета.
2. Случайный лес (Random Forest)	B) Выявление точечных аномалий и новых угроз в многомерных данных сетевого трафика без заранее известных меток.
3. Сверточная нейронная сеть (CNN)	C) Анализ последовательности событий или временных рядов для обнаружения сложных многоэтапных атак.
4. Рекуррентная нейронная сеть (RNN/LSTM)	D) Автоматическое извлечение пространственных признаков из представления сетевых пакетов или потоков данных.

Задание № 8. Установите соответствие между этапом постановки задачи совершенствования ML-алгоритма для IDS и ключевым решением или методом.

Этап постановки задачи совершенствования	**Ключевое решение / Метод**
1. Повышение точности и снижение ложных срабатываний	A) Применение техник обработки несбалансированных данных: передискретизация (SMOTE), недодискретизация, взвешивание классов.
2. Обнаружение новых атак при дефиците размеченных данных	B) Использование гибридных моделей (например, комбинация CNN и LSTM) для одновременного анализа разных аспектов данных.
3. Улучшение работы с несбалансированными данными (редкие	C) Внедрение адаптивных механизмов обратной связи и периодического дообучения

атаки)	модели на новых данных.
4. Обеспечение адаптивности к изменяющемуся трафику	D) Исследование и внедрение подходов, основанных на обучении без учителя, полуконтролируемом или трансферном обучении.

Задание № 9. Установите правильную последовательность этапов постановки задачи на разработку нового метода машинного обучения для обнаружения сложных сетевых атак.
Предлагаемые этапы:

а) Проанализировать недостатки существующих методов и алгоритмов.
б) Определить целевые метрики для оценки качества нового метода.
в) Сформулировать цель и ожидаемый практический результат разработки.
г) Утвердить техническое задание на исследовательскую работу.
д) Спланировать эксперименты для валидации метода.
е) Составить обзор современных научных публикаций по теме.
ж) Выбрать базовый подход и класс алгоритмов для модификации.

Задание № 10. Установите правильную последовательность действий при постановке задачи на совершенствование алгоритма обнаружения аномалий в потоковом сетевом трафике.
Предлагаемые этапы:

а) Определить аппаратные и временные ограничения для работы алгоритма.
б) Выбрать инструменты для прототипирования и тестирования.
в) Проанализировать характер ложных срабатываний текущей системы.
г) Сформулировать требования к точности и скорости работы нового решения.
д) Составить план сравнительных испытаний с эталонными алгоритмами.
е) Изучить современные методы обработки потоковых данных.
ж) Утвердить план работ по совершенствованию алгоритма.

Перечень заданий открытого типа

Задание № 1. Назовите классический и широко используемый в исследованиях набор данных для оценки алгоритмов обнаружения вторжений, который содержит помеченные сетевые соединения различных типов атак (например, neptune, smurf, guess_passwd).

Задание № 2. Какой метод машинного обучения, основанный на идее «изоляции» аномалий в многомерном пространстве данных, особенно эффективен для обнаружения новых угроз и часто используется в режиме реального времени?

Задание № 3. Какая пара метрик является наиболее критичной для практической оценки модели обнаружения вторжений, так как балансирует между важностью корректного нахождения атак и минимизацией количества ложных тревог?

Задание № 4. Для борьбы с проблемой высокой доли ложноположительных срабатываний в ML-модели IDS, помимо тонкой настройки порога классификации, какой подход на уровне данных и архитектуры системы можно предложить?

Задание № 5. Дополните определение, вставляя пропущенное слово:
_____ обучение — это подход, при котором модель, предварительно обученная на большой задаче с обилием данных, дорабатывается для решения конкретной целевой задачи (например, обнаружения атак в определенной среде), что особенно полезно при нехватке размеченных данных.

Задание № 6. Дополните определение, вставляя пропущенное слово:
При построении системы обнаружения вторжений на основе машинного обучения крайне важно учитывать возможность _____ атак, когда злоумышленник намеренно искажает входные данные, чтобы обмануть модель.

Формируемая компетенция: ПК-5

Перечень заданий закрытого типа

Задание № 1. Для проектирования аппаратно-программного комплекса ИИ, который будет непрерывно обрабатывать потоки видео с камер наблюдения в режиме реального времени на промышленном объекте, ключевым аппаратным решением, позволяющим эффективно выполнять нейросетевой инференс с низкой задержкой, является:

A) Центральный процессор высокой частоты.
B) Графический процессор или специализированный ускоритель.
C) Большой объем оперативной памяти.
D) Быстрый твердотельный накопитель.

Задание № 2. При разработке программного обеспечения для интеллектуальной системы прогнозирования отказов медицинского оборудования, где точность напрямую влияет на безопасность пациентов, критически важным принципом разработки является:

A) Максимизация быстродействия алгоритмов в ущерб точности.
B) Обеспечение надежности, отказоустойчивости и валидации результатов модели.
C) Использование исключительно open-source библиотек.
D) Минимизация количества строк кода.

Задание № 3. Какой подход является ключевым при модернизации существующей системы контроля доступа с внедрением модуля распознавания лиц для обеспечения его информационной безопасности на этапе разработки?

A) Принцип «Security by Design».
B) Тестирование безопасности после завершения всех работ.
C) Надежда на встроенные механизмы безопасности операционной системы.
D) Использование только аппаратных средств защиты.

Задание № 4. При выборе программного фреймворка для разработки компонента машинного обучения, который будет интегрирован в распределенную систему безопасности умного города, наименее значимым критерием в контексте ПК-5.1 будет:

A) Наличие встроенных средств для обеспечения конфиденциальности данных.
B) Поддержка развертывания в изолированных сетях.
C) Популярность фреймворка в академической среде для исследовательских задач.
D) Соответствие требованиям отраслевых стандартов безопасности.

Задание № 5. Какой аспект аппаратного обеспечения становится критически важным при разработке edge-устройства ИИ для автономного анализа данных датчиков на удаленной нефтяной вышке?

A) Поддержка последней версии графического интерфейса.
B) Устойчивость к экстремальным условиям, энергоэффективность и надежность.
C) Максимальная тактовая частота процессора.
D) Наличие подсветки корпуса.

Задание № 6. При модернизации SCADA-системы завода путем добавления интеллектуального модуля для детектирования аномалий в технологическом процессе, первоочередным требованием информационной безопасности к новому программному компоненту является:

A) Наличие сложной анимации в интерфейсе оператора.
B) Невозможность его несанкционированного воздействия на исполнительные механизмы (ПЛК) и гарантированная целостность данных.
C) Максимальная скорость обучения модели на исторических данных.
D) Использование облачных сервисов для хранения всех данных.

Задание № 7. Установите соответствие между этапом руководства разработкой архитектуры комплексной системы ИИ и ключевым решением или действием руководителя проекта.

Этап руководства разработкой архитектуры	Ключевое решение/действие руководителя проекта
1. Анализ предметной области и требований	A) Выбор парадигмы взаимодействия компонентов и протоколов обмена данными с учетом требований ИБ.
2. Определение высокоуровневой архитектуры	B) Утверждение решений по резервированию, мониторингу работоспособности и аварийному восстановлению компонентов ИИ.
3. Проектирование интеграции и безопасности	C) Определение ключевых нефункциональных требований: латентность, пропускная способность, доступность, безопасность данных
4. Планирование эксплуатационных характеристик	D) Внедрение практик DevSecOps, выбор инструментов статического/динамического анализа кода, планирование аудитов безопасности.

Задание № 8. Установите соответствие между классом интеллектуальных систем для предметной области «Киберфизические системы» и особенностью учета требований ИБ при их разработке/модернизации.

Класс интеллектуальных систем	Особенность учета требований ИБ при разработке
1. Беспилотный транспорт	A) Обеспечение безопасности жизни, защита от дистанционного захвата управления, целостность данных сенсоров.
2. Промышленные АСУ ТП	B) Защита критических технологических процессов от саботажа, устойчивость к целевым APT-атакам, работа в изолированных сетях.
3. Медицинские системы жизнеобеспечения	C) Гарантированная доступность и безотказность, защита конфиденциальных данных пациентов, валидация решений ИИ.
4. Умные энергетические сети	D) Защита от атак, способных вызвать каскадные отказы и масштабные отключения, контроль целостности данных телеметрии.

Задание № 9. Установите правильную последовательность этапов разработки программного обеспечения lightweight-агента для анализа событий безопасности на edge-устройстве в промышленной сети.

а) Разработать и протестировать прототип агента, проверив корректность сбора данных и работу алгоритмов в изолированной среде.

б) Определить технические требования к агенту: поддержка ОС устройства, ограничения по памяти/CPU, защищенный канал связи с сервером.

в) Внедрить в код агента механизмы обеспечения целостности и аутентичности.

г) Провести приемо-сдаточные испытания агента на реальном целевом оборудовании в промышленной сети.

д) Выбрать язык программирования и библиотеки, соответствующие требованиям производительности и безопасности.

Задание № 10. Установите правильную последовательность разработки защищенного шлюза для безопасной передачи телеметрии с промышленных датчиков в облачную систему аналитики.

а) Реализовать и протестировать функции шлюза: сбор данных, предварительная обработка, шифрование, передача по защищенному каналу.

б) Определить требования: поддержка интерфейсов датчиков, пропускная способность, алгоритмы шифрования, стойкость к средам.
в) Внедрить механизмы контроля целостности программного обеспечения шлюза и аутентификации при загрузке.
г) Провести пентест шлюза на предмет уязвимостей и испытания в условиях, близких к эксплуатационным.
д) Выбрать аппаратную платформу и компоненты, соответствующие требованиям надежности и безопасности.

Перечень заданий открытого типа

Задание № 1. При построении интеллектуальной системы для обработки персональных медицинских данных какой математический метод следует применить на этапе обучения модели, чтобы гарантировать конфиденциальность данных и соответствие требованиям регуляторов?

Задание № 2. Назовите ключевой международный стандарт, который необходимо учитывать при модернизации программно-аппаратного обеспечения систем ИИ для промышленных систем управления в части требований кибербезопасности.

Задание № 3. Какой архитектурный стиль является предпочтительным при разработке комплексной, масштабируемой и легко обновляемой системы ИИ, объединяющей модули сбора данных, ML-пайплайны и сервисы инференса?

Задание № 4. Какая практика управления инфраструктурой позволяет единообразно и безопасно разворачивать как программные компоненты ИИ, так и их среду выполнения на различных аппаратных платформах?

Задание № 5. Дополните определение, вставляя пропущенное слово:
_____ обучение — это децентрализованный подход к машинному обучению, позволяющий обучать модель на данных, которые остаются на устройствах-источниках, что повышает безопасность и конфиденциальность данных.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Процесс проверки и подтверждения того, что данные, используемые для обучения и работы модели ИИ, не были намеренно искажены для манипуляции её результатами, называется защитой от _____ данных.

Формируемая компетенция: ПК- 6

Перечень заданий закрытого типа

Задание № 1. Какой программный компонент является ключевым для извлечения структурированных данных из веб-страниц в рамках OSINT-пайплайна?
A) База данных (PostgreSQL).
B) Веб-скрапер/парсер (например, на основе BeautifulSoup или Scrapy).
C) SIEM-платформа (Splunk).
D) Виртуальная машина (VirtualBox).

Задание № 2. Какой критерий является наименее существенным при выборе библиотеки машинного обучения для анализа текстовых OSINT-данных?
A) Наличие предобученных моделей для NLP.
B) Скорость обработки больших объемов текста.
C) Качество документации и активность сообщества.
D) Стоимость коммерческой лицензии для некоммерческого исследования.

Задание № 3. Какой компонент отвечает за преобразование и очистку сырых данных, собранных из открытых источников, перед их загрузкой в хранилище?

A) ETL-процесс (Extract, Transform, Load).
B) Модуль визуализации (Kibana).
C) Система контроля версий (Git).
D) Планировщик задач (cron).

Задание № 4. Какой инструмент наиболее подходит для создания конвейера (pipeline) обработки данных, объединяющего этапы парсинга, очистки и анализа с помощью ML-моделей?

A) Microsoft Excel.
B) Фреймворк для workflow (например, Apache Airflow).
C) Текстовый редактор (Vim).
D) Почтовый клиент (Thunderbird).

Задание № 5. Для хранения неструктурированных текстовых данных, собранных в ходе OSINT-исследования, наиболее целесообразно использовать:

A) Реляционную СУБД (MySQL).
B) Документо-ориентированную СУБД (например, Elasticsearch или MongoDB).
C) Электронную таблицу (Google Sheets).
D) Файловую систему в виде текстовых файлов.

Задание № 6. Какой принцип разработки программных компонентов позволяет легко заменять один алгоритм машинного обучения на другой в системе?

A) Использование модульной архитектуры и четких интерфейсов.
B) Написание всего кода в одном файле.
C) Жесткая привязка логики к конкретной библиотеке.
D) Отказ от использования внешних зависимостей.

Задание № 7. Установите соответствие между типом программного компонента системы ИИ для OSINT и его основной задачей.

Тип компонента	**Основная задача**
1. Компонент сбора данных	A) Автоматическое присвоение категорий или тегов собранным текстовым данным (например, "угроза", "спам").
2. Компонент предобработки	B) Извлечение данных из API, веб-страниц или файлов в заданном формате.
3. Компонент классификации	C) Организация взаимодействия между другими компонентами по заданному расписанию.
4. Оркестратор пайплайна	D) Очистка текста, удаление стоп-слов, лемматизация, векторизация.

Задание № 8. Установите соответствие между технологией/инструментом и этапом жизненного цикла программного компонента ИИ.

Технология/Инструмент	**Этап жизненного цикла компонента**
1. Git	A) Разработка и версионирование исходного кода.
2. Docker	B) Упаковка компонента и его зависимостей в переносимый контейнер.
3. Pytest/Unittest	C) Автоматическая проверка корректности работы компонента.
4. CI/CD (Jenkins, GitLab CI)	D) Автоматизация сборки, тестирования и развертывания компонента.

Задание № 9. Установите правильную последовательность действий при выборе программных компонентов для построения пайплайна машинного обучения в задаче анализа текстовых OSINT-данных.

а) Сопоставить функциональные возможности библиотек с конкретными задачами пайплайна (парсинг, векторизация, классификация).

б) Составить сравнительную таблицу выбранных библиотек по критериям производительности, документации и лицензии.

в) Разработать прототип ключевого компонента пайплайна на выбранной библиотеке для проверки гипотезы.

г) Сформулировать технические требования к каждому этапу пайплайна обработки данных.

д) Провести поиск и предварительный отбор популярных и поддерживаемых библиотек (например, для NLP).

Задание № 10. Установите правильную последовательность этапов при разработке программного компонента для автоматического обогащения сырых OSINT-данных (например, IP-адресов) контекстом из внешних API.

а) Написать код компонента, реализующий логику запросов к API, обработки ответов и объединения данных.

б) Протестировать компонент на тестовом наборе данных, проверив корректность работы и обработку ошибок сети.

в) Составить техническое описание компонента: интерфейсы, форматы входных/выходных данных, протоколы.

г) Выбрать конкретные внешние сервисы (API) для получения контекстной информации и изучить их документацию.

д) Спроектировать архитектуру компонента, определив его место в общем пайплайне и способ интеграции.

Перечень заданий открытого типа

Задание № 1. Какая популярная Python-библиотека является стандартом де-факто для выполнения операций предобработки и анализа структурированных данных (DataFrames)?

Задание № 2. Какой формат часто используется для сериализации данных и конфигураций моделей машинного обучения в рамках компонентов ИИ?

Задание № 3. Какой простой инструмент командной строки в UNIX-системах позволяет планировать регулярный запуск скриптов сбора или обработки данных?

Задание № 4. Какой подход к разработке предполагает, что тесты пишутся до реализации самого функционала компонента?

Задание № 5. Дополните определение, вставляя пропущенное слово.
Процесс автоматической сборки, тестирования и развертывания программных компонентов при каждом изменении кода называется _____ интеграцией и доставкой.

Задание № 6. Дополните предложение, вставляя пропущенное слово.
Для управления зависимостями и виртуальными окружениями в Python-проектах компонентов ИИ чаще всего используется инструмент _____.

Формируемая компетенция: ПК-7

Перечень заданий закрытого типа

Задание № 1. На каком из этапов управления проектом по созданию комплексной системы ИИ для ИБ происходит формальное утверждение объёма работ, бюджета, ключевых ролей и графика высокого уровня?

A) На этапе мониторинга и контроля исполнения.
B) На этапе тестирования и ввода в эксплуатацию.
C) На этапе инициации проекта.
D) На этапе сбора требований.

Задание № 2. Какой архитектурный стиль наиболее предпочтителен для построения комплексной, масштабируемой и легко обновляемой системы ИИ, объединяющей модули сбора данных, ML-пайплайны и сервисы инференса?
A) Монолитная архитектура.
B) Архитектура на основе готовых коробочных решений.
C) Микросервисная архитектура.
D) Архитектура "большой файл скриптов".

Задание № 3. Какой из перечисленных компонентов НЕ является типичным для архитектуры комплексной системы ИИ в сфере ИБ, построенной по принципам MLOps?
A) Хранилище признаков .
B) Реестр моделей и система версионирования.
C) Единая реляционная база данных для хранения всех логов, сырых данных и метаданных моделей.
D) Конвейер CI/CD для моделей машинного обучения.

Задание № 4. Какой ключевой документ, создаваемый архитектором на ранней стадии, визуализирует высокоуровневую структуру системы, ключевые технологические решения и потоки данных между основными компонентами?
A) Пользовательская история .
B) Диаграмма архитектуры решения.
C) Отчет о тестировании.
D) План коммуникаций с заказчиком.

Задание № 5. Руководитель проекта вносит в план рисков вероятность того, что выбранная открытая ML-библиотека может содержать уязвимость, приводящую к компрометации модели. Какой тип риска это представляет?
A) Операционный риск.
B) Риск безопасности цепочки поставок (Supply Chain Risk).
C) Финансовый риск перерасхода бюджета.
D) Риск несоответствия требованиям законодательства.

Задание № 6. Какой критерий является НАИМЕНЕЕ значимым при выборе между облачной и on-premise инфраструктурой для развертывания системы ИИ, обрабатывающей конфиденциальные данные разведки?
A) Требования к задержке при обработке данных в реальном времени.
B) Стоимость месячной подписки на облачные сервисы.
C) Нормативные требования к локализации и суверенитету данных.
D) Наличие у команды экспертизы по администрированию выбранной платформы.

Задание № 7. Установите соответствие между этапом разработки архитектуры комплексной системы ИИ и его ключевым результатом.

Этап разработки архитектуры	**Ключевой результат**
1. Анализ бизнес-требований и ограничений	A) Выбор конкретных технологий, фреймворков, протоколов и их версий.
2. Определение архитектурных паттернов и стилей	B) Утверждённый перечень нефункциональных требований: масштабируемость, отказоустойчивость, безопасность.
3. Выбор технологического стека	C) Концептуальная модель системы,

	диаграммы компонентов и взаимодействий.
4. Детальное проектирование	D) Чёткое понимание целей системы, KPI успеха, бюджетных и нормативных рамок.

Задание № 8. Установите соответствие между ключевым компонентом архитектуры безопасной системы ИИ для SOC и его основной функцией.

Компонент системы	Основная функция
1. Feature Store (Хранилище признаков)	A) Централизованное управление жизненным циклом моделей: версионирование, развертывание, мониторинг.
2. ML Metadata Store (Хранилище метаданных)	B) Обеспечение воспроизводимости экспериментов и аудита всех запусков обучения и оценки.
3. Model Registry (Реестр моделей)	C) Согласованное вычисление, хранение и обслуживание актуальных признаков для обучения и инференса.
4. Adversarial Robustness Module	D) Регулярная проверка моделей на устойчивость к состязательным атакам и генерация тестовых данных.

Задание № 9. Установите правильную последовательность ключевых этапов руководства проектом по созданию комплексной системы искусственного интеллекта для центра мониторинга безопасности.

а) Утвердить итоговый архитектурный проект системы и план его реализации.

б) Организовать работу проектной команды: распределить роли, зоны ответственности и утвердить график работ.

в) Согласовать с заказчиком концепцию, цели, ключевые требования и бюджет проекта.

г) Провести аудит и приемку готовой системы, передать документацию и обучить персонал заказчика.

д) Контролировать выполнение работ, проводить регулярные совещания и корректировать план при возникновении рисков.

е) Сформировать техническое задание на основании согласованной концепции.

ж) Согласовать с техническими специалистами выбор технологического стека и ключевых архитектурных решений.

Задание № 10. Установите правильную последовательность ключевых этапов руководства проектом по созданию комплексной системы искусственного интеллекта для центра мониторинга безопасности.

а) Утвердить итоговый архитектурный проект системы и план его реализации.

б) Организовать работу проектной команды: распределить роли, зоны ответственности и утвердить график работ.

в) Согласовать с заказчиком концепцию, цели, ключевые требования и бюджет проекта.

г) Провести аудит и приемку готовой системы, передать документацию и обучить персонал заказчика.

д) Контролировать выполнение работ, проводить регулярные совещания и корректировать план при возникновении рисков.

е) Сформировать техническое задание на основании согласованной концепции.

ж) Согласовать с техническими специалистами выбор технологического стека и ключевых архитектурных решений.

Перечень заданий открытого типа

Задание № 1. Назовите ключевой документ, фиксирующий договорённости между заказчиком и исполнителем по целям, содержанию, срокам, стоимости и критериям приёмки проекта.

Задание № 2. Как называется организационная структура проекта, в которой участники подчиняются как руководителю проекта, так и своему функциональному руководителю?

Задание № 3. Какой класс диаграмм в нотации UML наиболее часто используется на этапе проектирования архитектуры для отображения статической структуры системы в виде компонентов, классов и их взаимосвязей?

Задание № 4. Какая методология управления проектами, основанная на коротких итеративных циклах разработки, наиболее распространена при создании гибких комплексных систем ИИ?
Задание № 5. Дополните определение, вставляя пропущенное слово:
Технология _____, использующая такие инструменты как Docker и Kubernetes, является стандартом для упаковки и развертывания микросервисов системы ИИ, обеспечивая их изоляцию и переносимость.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Ключевой показатель эффективности, измеряющий соотношение полезного результата проекта к понесённым затратам, называется _____ от инвестиций.

Формируемая компетенция: ПК-8

Перечень заданий закрытого типа

Задание № 1. Какой тип архитектуры искусственной нейронной сети (ИНС) является наиболее подходящим для обработки последовательных данных, таких как временные ряды событий безопасности или анализ текстовых логов?

1. Полносвязная нейронная сеть (Fully Connected Network).
2. Сверточная нейронная сеть (Convolutional Neural Network, CNN).
3. Рекуррентная нейронная сеть (Recurrent Neural Network, RNN), например, LSTM или GRU.
4. Генеративно-состязательная сеть (Generative Adversarial Network, GAN).
5. Автокодировщик (Autoencoder).

Задание № 2. При выборе инструментального средства для реализации и обучения нейросетевой модели в условиях ограниченных вычислительных ресурсов, но с требованием высокой скорости прототипирования, ключевым решающим фактором, скорее всего, будет:

1. Поддержка распределенных вычислений на тысячах GPU.
2. Наличие встроенных средств для создания production-пайплайнов.
3. Простота синтаксиса, обширное сообщество и богатая библиотека готовых решений.
4. Возможность развертывания на специализированных ASIC-чипах.

Задание № 3. При выборе между сверточной (CNN) и рекуррентной (RNN) нейронной сетью для анализа файлов на наличие вредоносного кода, ключевым решающим фактором в пользу CNN будет:

1. Необходимость анализа последовательности системных вызовов во времени.
2. Возможность эффективного выявления пространственных паттернов и особенностей в бинарном представлении файла.
3. Ограниченный объем доступных размеченных данных для обучения.
4. Низкая вычислительная сложность алгоритмов обучения.

Задание № 4. Какая из перечисленных метрик является НАИМЕНЕЕ информативной для первичной оценки качества бинарного классификатора вредоносных URL на сильно несбалансированной выборке (99% легитимных, 1% вредоносных)?

1. Матрица ошибок (Confusion Matrix).

2. Точность (Accuracy).
3. Полнота (Recall).
4. Точность (Precision).

Задание № 5. Руководитель проекта ИИ должен выбрать фреймворк для промышленной системы обнаружения аномалий в реальном времени. Помимо точности модели, КРИТИЧЕСКИ важным критерием выбора будет поддержка фреймворком:

1. Эффективного инференса (вывода) с низкой задержкой на целевой аппаратной платформе.
2. Визуального конструктора нейронных сетей.
3. Написания кода на языке программирования R.
4. Наибольшего числа «лайков» на GitHub.

Задание № 6. Какой тип нейросетевой архитектуры наиболее целесообразно рассмотреть в первую очередь для задачи снижения размерности многомерных данных сетевых потоков (NetFlow) перед их дальнейшим анализом?

1. Сеть прямого распространения (Feedforward Network).
2. Сверточная нейронная сеть (CNN).
3. Автокодировщик (Autoencoder).
4. Генеративно-состязательная сеть (GAN).

Задание № 7. Установите соответствие между типом архитектуры ИНС и задачей в области кибербезопасности, для решения которой она преимущественно применяется.

Архитектура ИНС	**Задача в области ИБ**
1. Сверточная нейронная сеть (CNN)	а) Обнаружение аномалий в поведении пользователя на основе последовательности его действий.
2. Автокодировщик (Autoencoder)	б) Классификация вредоносных PE-файлов на основе их визуализации (бинарные изображения).
3. Рекуррентная нейронная сеть (LSTM)	в) Снижение размерности данных для выявления скрытых паттернов в сетевом трафике.
4. Генеративно-состязательная сеть (GAN)	г) Создание реалистичных образцов вредоносного трафика для усиления тренировочных данных.

Задание № 8. Установите соответствие между этапом оценки модели ИНС и используемым для этого ключевым документом или показателем.

Этап оценки модели ИНС	**Документ / Ключевой показатель**
1. Оценка бизнес-требований	а) Матрица ошибок (Confusion Matrix), значения Precision, Recall, F1-score.
2. Сравнение производительности моделей	б) Технико-экономическое обоснование (ТЭО) с расчетом ROI.
3. Оценка эксплуатационных качеств	в) Тестовый план с валидационной и тестовой выборками.
4. Финализация выбора	г) Требования к инфраструктуре (задержка инференса, потребление памяти).

Задание № 9. Установите правильную последовательность этапов руководства работами по оценке и выбору модели ИНС для задачи классификации типов сетевых атак.

а) Провести сравнительное тестирование отобранных моделей-кандидатов на едином валидационном наборе данных.

б) Сформулировать требования к модели: точность, скорость инференса, интерпретируемость, ресурсопотребление.

в) Утвердить итоговый выбор модели и инструментального стека для проекта.

г) Проанализировать задачу и доступные данные для определения подходящего класса архитектур ИНС.

д) Сформировать short-list моделей и инструментов (например, TensorFlow vs PyTorch, CNN vs RNN).

е) Составить и согласовать план работ по оценке и выбору с командой.

Задание № 10. Установите правильную последовательность действий руководителя проекта при выборе инструментальных средств и архитектуры для системы обнаружения аномалий на основе ИНС.

а) Принять финальное решение по технологическому стеку и архитектуре на основе отчетов об испытаниях.

б) Оценить соответствие выбранных инструментов (фреймворков, библиотек) корпоративным стандартам и инфраструктуре.

в) Определить ключевые критерии выбора: поддержка production-развертывания, наличие готовых предобученных моделей, сообщество.

г) Инициировать практическое тестирование (proof-of-concept) для проверки производительности стека на реальных данных.

д) Согласовать с архитекторами и инженерами данных предварительный выбор технологий.

Перечень заданий окрытого типа

Задание № 1. Какой популярный фреймворк с динамическим вычислительным графом, разработанный Facebook, часто выбирают для исследовательских задач и быстрого прототипирования нейросетевых моделей?.

Задание № 2. Какая архитектура нейронной сети, основанная на механизме внимания, в настоящее время является доминирующей для задач обработки естественного языка и также применяется для анализа логов безопасности?

Задание № 3. Как называется процесс автоматического подбора оптимальной архитектуры и гиперпараметров нейронной сети, который является частью работ по оценке и выбору модели?

Задание № 4. Назовите ключевой документ, который является итоговым результатом этапа оценки и выбора модели ИНС и содержит обоснование выбранного варианта, сравнение альтернатив, требования к инфраструктуре и план внедрения.

Задание № 5. Дополните предложение, вставляя пропущенное слово:
Для задачи классификации сетевых пакетов как нормальных или вредоносных, когда важна интерпретируемость решений, часто выбирают _____ архитектуры ИНС, такие как ResNet, а не «черные ящики».

Задание № 6. Дополните предложение, вставляя пропущенное слово:
Ключевым критерием выбора между фреймворками TensorFlow и PyTorch для промышленного внедрения часто считается развитость экосистемы для _____ (развертывания).

5. КРИТЕРИИ ОЦЕНКИ

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности обучающихся. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Таблица 3.

Шкалы оценивания			**Критерии оценивания**
пятибальная	двадцатибальная	стобальная	
«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 ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 5.

ПК-1	**Задания закрытого типа**	
	№ 1	D
	№ 2	C
	№ 3	B
	№ 4	C
	№ 5	D
	№ 6	B
	№ 7	1-B, 2-D, 3-C, 4-D
	№ 8	1-A, 2-B, 3-C, 4-D
	№ 9	вгбда
	№ 10	гбва
	Задания открытого типа	
	№ 1	Градиентный
	№ 2	Холд-аут
	№ 3	Тюнинг
	№ 4	Numpy
	№ 5	F1-мера
	№ 6	Конструированием
ПК-2	**Задания закрытого типа**	
	1.	B
	2.	C
	3.	B
	4.	B
	5.	C
	6.	A
	7.	1-D, 2-C, 3-A, 4-B
	8.	1-B, 2-D, 3-C, 4-A
	9.	бгадв
	10.	вгбад
	Задания открытого типа	
	1.	Admiralty
	2.	Парсеры
	3.	Воспроизводимость
	4.	Блок-схема
	5.	Ревизия
	6.	Фильтрации
ПК-3	**Задания закрытого типа**	
	№ 1	A
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	A
	№ 6	B
	№ 7	1-A, 2-B, 3-C, 4-D
	№ 8	1-B, 2-A, 3-C, 4-D
	№ 9	гбдва

	№ 10	гбвда
	Задания открытого типа	
	№ 1	Дифференциальная приватность
	№ 2	MITRE ATLAS
	№ 3	Трансформеры
	№ 4	API SIEM
	№ 5	Безопасность по умолчанию
	№ 6	Граничные
ПК-4	**Задания закрытого типа**	
	№ 1	C
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	B
	№ 6	B
	№ 7	1-B, 2-A, 3-D, 4-C
	№ 8	1-B, 2-D, 3-A, 4-C
	№ 9	аевжбдг
	№ 10	вегабдж
	Задания открытого типа	
	№ 1	KDD Cup
	№ 2	Изолирующий лес
	№ 3	Точность, полнота
	№ 4	Внедрение МСВ
	№ 5	Трансферное
	№ 6	Состязательных
ПК-5	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	A
	№ 4	C
	№ 5	B
	№ 6	B
	№ 7	1-C, 2-A, 3-D, 4-B
	№ 8	1-A, 2-B, 3-C, 4-D
	№ 9	бдавг
	№ 10	бдавг
	Задания открытого типа	
	№ 1	Дифференциальная приватность
	№ 2	МЭК 62443
	№ 3	Микросервисная архитектура
	№ 4	Контейнеризация
	№ 5	Федеративное
ПК-6	**Задания закрытого типа**	
	№ 1	B
	№ 2	D

	№ 3	A
	№ 4	B
	№ 5	B
	№ 6	A
	№ 7	1-B, 2-D, 3-A, 4-C
	№ 8	1-A, 2-B, 3-C, 4-D
	№ 9	гдабв
	№ 10	гдваб
	Задания открытого типа	
	№ 1	Pandas
	№ 2	Json
	№ 3	Cron
	№ 4	Tdd
	№ 5	Непрерывной
	№ 6	Pip
ПК-7	**Задания закрытого типа**	
	№ 1	C
	№ 2	C
	№ 3	C
	№ 4	B
	№ 5	B
	№ 6	B
	№ 7	1 - D, 2 - B, 3 - A, 4 - C
	№ 8	1 - C, 2 - B, 3 - A, 4 - D
	№ 9	вебжадг
	№ 10	гвдаеб
	Задания открытого типа	
	№ 1	Устав проекта
	№ 2	Матричная структура
	№ 3	Диаграмма компонентов
	№ 4	Гибкая методология
	№ 5	Контейнеризация
	№ 6	Возврат
ПК-8	**Задания закрытого типа**	
	№ 1	3
	№ 2	2
	№ 3	2
	№ 4	2
	№ 5	2
	№ 6	3
	№ 7	1 – б, 2 – в, 3 – а, 4 – г
	№ 8	1 – б, 2 – а, 3 – г, 4 – в
	№ 9	бгедав
	№ 10	вбдга
	Задания открытого типа	
	№ 1	Pytorch

	№ 2	Трансформер
	№ 3	Automl
	№ 4	ТЭ обоснование
	№ 5	Известные/стандартные
	№ 6	Продакшена