**Министерство науки и высшего образования Российской Федерации**

**ФГБОУ ВО «Дагестанский государственный технический университет»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**по дисциплине** «Теория обнаружения вторжении с применением искусственного интеллекта»
(указывается индекс и наименование дисциплины)

Уровень образования — магистратура
(бакалавриат/магистратура/специалитет)

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

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

Разработчик _____ Мирземагомедова М.М., к.т.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 ..... 3
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ ..... 3
3. ОЦЕНКА ОСВОЕНИЯ ДИСЦИПЛИНЫ ..... 4
3.1. Контроль и оценка освоения дисциплины по темам (разделам) ..... 4
3.2. Перечень заданий для текущего контроля ..... 7
4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ..... 12
5. КРИТЕРИИ ОЦЕНКИ ..... 20
5.1. Критерии оценки текущего контроля и промежуточной аттестации ..... 20

## 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью рабочей программы дисциплины «Теория обнаружения вторжении с применением искусственного интеллекта» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. самостоятельной работе обучающихся), освоивших программу данной дисциплины.

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

Рабочей программой дисциплины «Теория обнаружения вторжении с применением искусственного интеллекта» 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-4 Способен разрабатывать и применять методы и алгоритмы машинного обучения для решения задач искусственного интеллекта.

Формой аттестации по дисциплине является экзамен.

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

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

Таблица 1.

| Результаты обучения: индикаторы достижения | Формируемые компетенции |
|---|---|
| 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 обеспечения информационной безопасности | |
| ПК-2.1 Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности | ПК-2 |
| ПК-4.1 Ставит задачи по разработке или совершенствованию методов и алгоритмов для решения комплекса задач предметной области | ПК-4 |

## 3. ОЦЕНКА ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

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

Таблица 2.

| Элемент дисциплины | Формы и методы контроля | | | |
|---|---|---|---|---|
| | Текущий контроль | | Промежуточная аттестация | |
| | Форма контроля | Проверяемые компетенции/ индикаторы достижения | Форма контроля | Проверяемые компетенции/ индикаторы достижения |
| **Раздел 1. Основы теории искусственного интеллекта** | | | | |
| **Тема 1. Искусственный интеллект и проблемы представления знаний.** | Письменная работа № 1<br>Устный опрос<br>Лабораторная работа № 1<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 2. Логические модели представления знаний.** | Письменная работа № 2<br>Устный опрос<br>Лабораторная работа № 2<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 3. Модели представления знаний.** | Письменная работа № 3<br>Устный опрос<br>Лабораторная работа № 3<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 4. Инструментарий искусственного интеллекта.** | Письменная работа № 4<br>Устный опрос<br>Лабораторная работа № 4<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Раздел 2. Теория и технологии обнаружения вторжений** | | | | |
| **Тема 5. Понятие и виды угроз информационной безопасности.** | Письменная работа № 5<br>Устный опрос<br>Лабораторная работа № 5<br>Самостоятельная | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |

| | | | | |
|---|---|---|---|---|
| | работа<br>Реферат | | | |
| **Тема 6. Модели преднамеренных угроз информационной безопасности.** | Письменная работа № 6<br>Устный опрос<br>Лабораторная работа № 6<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 7. Источники сведений системы мониторинга информационной безопасности.** | Письменная работа № 7<br>Устный опрос<br>Лабораторная работа № 7<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 8. Обзор современных технических решений мониторинга информационной безопасности.** | Письменная работа № 8<br>Устный опрос<br>Лабораторная работа № 8<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Раздел 3. Применение искусственного интеллекта в интеллектуальных системах обнаружения** | | | | |
| **Тема 9. Организация интеллектуальной вторжений системы обнаружения вторжений.** | Письменная работа № 9<br>Устный опрос<br>Лабораторная работа № 9<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 10. Особенности организации интеллектуальной системы обнаружения вторжений от APT-атак.** | Письменная работа № 10<br>Устный опрос<br>Лабораторная работа № 10<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема11. Интеллектуальный анализ событий информационной безопасности домена.** | Письменная работа № 11<br>Устный опрос<br>Лабораторная работа № 11<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |

| | | | | |
|---|---|---|---|---|
| **Тема 12. Интеллектуальный анализ событий информационной безопасности Linux-серверов.** | Письменная работа № 12<br>Устный опрос<br>Лабораторная работа № 12<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Раздел 4. Искусственный интеллект** | | | | |
| **Тема 13. Основы разработки информационно-аналитической системы в сфере ИБ.** | Письменная работа № 13<br>Устный опрос<br>Лабораторная работа № 13<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 14. Этапы разработки информационно-аналитической системы в сфере ИБ**. | Письменная работа № 14<br>Устный опрос<br>Лабораторная работа № 14<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 15. Применение моделей машинного обучения для анализа трафика.** | Письменная работа № 15<br>Устный опрос<br>Лабораторная работа № 15<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |
| **Тема 16. Применение методов машинного обучения для анализа трафика.** | Письменная работа № 16<br>Устный опрос<br>Лабораторная работа № 16<br>Самостоятельная работа<br>Реферат | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 | Экзаменационная работа | ПК-1: ПК-1.1, ПК-1.2;<br>ПК-2: ПК-2,1;<br>ПК-4: ПК-4.1 |

## 3.2. Перечень заданий для текущего контроля

***Формируемая компетенция: ПК- 1***

**Перечень заданий закрытого типа**

Задание № 1. Для решения задачи классификации сетевых пакетов как нормальных или аномальных с использованием методов распознавания образов наиболее подходящим алгоритмом машинного обучения является:

A) Алгоритм случайного леса (Random Forest).
B) Алгоритм линейной регрессии.
C) Алгоритм анализа главных компонент (PCA).
D) Алгоритм Apriori.

Задание № 2. Какой компонент классической сигнатурной системы обнаружения вторжений (IDS) отвечает за сравнение наблюдаемой активности с базой известных шаблонов атак?

A) Модуль сбора данных (Sensor).
B) Детектор (Detector).
C) База данных событий.
D) Консоль управления.

Задание № 3. Установите соответствие между типом системы обнаружения вторжений (IDS) и её ключевой характеристикой.

| Тип IDS | Ключевая характеристика |
|---|---|
| 1. Сетевая IDS (NIDS) | A) Анализирует журналы событий и активность на уровне операционной системы отдельного компьютера. |
| 2. Хостовая IDS (HIDS) | B) Мониторит сетевой трафик на уровне пакетов для выявления подозрительной активности. |
| 3. Сигнатурная IDS | C) Обнаруживает отклонения от заданного эталонного поведения системы или пользователя. |
| 4. Аномалийная IDS | D) Использует базу известных шаблонов (сигнатур) атак для поиска совпадений. |

Задание № 4. Установите соответствие между этапом анализа сетевого трафика с применением интеллектуальных средств и типичным действием или методом.

| Этап анализа | Действие / Метод |
|---|---|
| 1. Сбор и захват данных | A) Использование инструментов вроде tcpdump или Wireshark для получения файлов трафика (PCAP). |
| 2. Предобработка и извлечение признаков | B) Нормализация данных, кодирование категориальных признаков, создание новых производных признаков. |
| 3. Обучение и применение модели | C) Использование библиотек машинного обучения для классификации или обнаружения аномалий в данных. |
| 4. Визуализация и интерпретация | D) Построение графиков важности признаков, анализ ложных срабатываний, подготовка отчета. |

Задание № 5. Установите правильную последовательность этапов работы специалиста с системой интеллектуального обнаружения вторжений (IDS) на основе машинного обучения, от получения исходных данных до принятия решения.

а) Провести исследовательский анализ данных для выявления аномалий, распределений и взаимосвязей в сетевых логах.

б) Применить обученную модель машинного обучения к новым, ранее невиданным данным для генерации предсказаний.

в) На основе приоритизации и контекста сформулировать рекомендации по реагированию на инцидент

г) Произвести сбор и консолидацию сетевых журналов и данных о трафике из различных источников.
д) Обогатить исходные данные, добавив контекстную информацию.
е) Приоритизировать и проанализировать сгенерированные алерты, сопоставив их с моделью угроз MITRE ATT&CK.
ж) Обучить модель машинного обучения на размеченном историческом наборе данных.
з) Выполнить предобработку данных: очистку от шума, нормализацию, кодирование категориальных признаков, создание новых признаков.

**Перечень заданий открытого типа**

Задание № 1. Какой класс алгоритмов машинного обучения, не требующий размеченных данных об атаках для обучения, наиболее применим для обнаружения ранее неизвестных (zero-day) угроз в сетевом трафике?
Задание № 2. Назовите популярную Python-библиотеку, которая является стандартным инструментом для интерактивной визуализации данных и может использоваться для анализа и представления результатов работы IDS.
Задание № 3. Как называется основной открытый фреймворк/таксономия, который используется для формального описания техник и тактик злоумышленников и должен применяться для интерпретации и категоризации обнаруженных инцидентов?
Задание № 4. Дополните определение, вставляя пропущенное слово:
Метрика _____, рассчитываемая как отношение ложноположительных срабатываний к общему числу нормальных событий, критически важна для оценки эксплуатационных качеств IDS.
Задание № 5. Дополните определение, вставляя пропущенное слово:
Процесс автоматического обогащения событий IDS контекстной информацией из внешних источников, таких как списки вредоносных IP-адресов или хешей файлов, называется интеграцией с _____.

***Формируемая компетенция: ПК-2***

**Перечень заданий закрытого типа**

Задание № 1. Первым шагом при формализации задачи для интеллектуальной системы обнаружения вторжений является:
A) Написание кода алгоритма машинного обучения.
B) Выбор языка программирования Python или R.
C) Определение целей мониторинга и критичных для защиты активов подразделения (серверы, базы данных, рабочие станции).
D) Запуск системы сбора сетевого трафика (tcpdump).

Задание № 2. Какой метод анализа сетевой обстановки НЕ является типичным для выявления скрытых, многоэтапных атак (APT) и, следовательно, менее приоритетен при формализации задач для современной ИАС?
A) Корреляция событий из разнородных источников (журналы, NetFlow, алерты IDS).
B) Статистический подсчет общего объема входящего/исходящего трафика за сутки.
C) Построение временных профилей нормального поведения пользователей и систем.
D) Поиск аномалий в последовательностях сетевых подключений и команд.

Задание № 3. Установите соответствие между методом/подходом к мониторингу сетевой обстановки и целью его применения при решении задач обнаружения вторжений.

| **Метод / Подход мониторинга** | **Цель применения для обнаружения вторжений** |
|---|---|
| 1. Анализ потоков данных (NetFlow/IPFIX) | A) Выявление скрытого взаимодействия узлов сети, формирования карты атаки и коммуникационных каналов бот-сети. |
| 2. Глубокий анализ пакетов (DPI) | B) Оценка общего объема и направлений трафика для выявления аномалий и целевых для детального изучения сегментов. |

| | |
|---|---|
| 3. Анализ графов связей между хостами | C) Изучение содержимого пакетов для идентификации протоколов, извлечения вредоносных сигнатур и полезных нагрузок. |
| 4. Поведенческий анализ (UEBA) | D) Обнаружение отклонений от шаблонов нормального поведения пользователей и систем, указывающих на компрометацию. |

Задание № 4. Установите соответствие между этапом формализации задачи для ИАС обнаружения вторжений и создаваемым документом или результатом.

| **Этап формализации задачи** | **Документ / Результат** |
|---|---|
| 1. Сбор и анализ требований стейкхолдеров | A) Модель угроз (Threat Model), описывающая активы, уязвимости, векторы атак и последствия. |
| 2. Определение контекста и угроз | B) Перечень и описание источников данных (логи, трафик, Threat Intel), их форматов и способов сбора. |
| 3. Спецификация источников и данных | C) Итоговое Техническое задание (ТЗ), содержащее цели, требования, критерии приемки. |
| 4. Формирование технического задания | D) Список функциональных и нефункциональных требований, приоритетов и ограничений. |

Задание № 5. Установите правильную последовательность этапов формализации задачи для разработки новой системы мониторинга сетевой обстановки.

а) Провести интервью со стейкхолдерами для сбора требований.
б) Выбрать конкретные технологии и инструменты для реализации.
в) Согласовать и утвердить техническое задание.
г) Определить цели и ключевые показатели эффективности системы.
д) Составить модель угроз для защищаемых активов.
е) Разработать проект архитектуры системы.
ж) Составить техническое задание на разработку системы.

**Перечень заданий открытого типа**

Задание № 1. Назовите основную международную открытую таксономию, которую необходимо использовать при формализации задач для ИАС с целью детектирования конкретных техник и тактик злоумышленников по всему жизненному циклу атаки.

Задание № 2. Какой ключевой навык (soft skill), упомянутый в исследованиях цифровой грамотности, критически важен для формализации задач ИБ, так как позволяет объективно оценивать данные, выявлять неочевидные связи и не принимать результаты работы систем за абсолютную истину?

Задание № 3. Как называется основной принцип безопасной разработки, который должен быть учтен при формализации задачи на создание модуля ИАС и требует предоставления компонентам системы минимально необходимых для работы привилегий?

Задание № 4. Дополните определение, вставляя пропущенное слово:

Практика _____ мышления и декомпозиции сложных процессов на последовательность шагов является фундаментальной для корректной формализации задач, которые будут делегированы интеллектуальным автоматизированным системам.

Задание № 5. Дополните определение, вставляя пропущенное слово:

При формализации задачи для системы, обрабатывающей персональные данные, необходимо учитывать требования _____ приватности для обеспечения конфиденциальности информации на этапе анализа и обучения моделей.

***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 для бинарной классификации.
B) Методы обучения без учителя, в частности, алгоритмы обнаружения аномалий.
C) Методы обучения с подкреплением.
D) Трансферное обучение на основе предобученных моделей.

Задание № 3. 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 № 4. 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 атаки) | C) Внедрение адаптивных механизмов обратной связи и периодического дообучения 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 № 5. 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.

**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 (назовите обе) является наиболее критичной для практической оценки модели обнаружения вторжений, так как балансирует между важностью корректного нахождения атак и минимизацией количества ложных тревог?

Задание № 4. 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 № 5. 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.

## 4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

***Формируемая компетенция: ПК-1***

**Перечень заданий закрытого типа**

Задание № 1. Для решения задачи классификации сетевых пакетов как нормальных или аномальных с использованием методов распознавания образов наиболее подходящим алгоритмом машинного обучения является:

A) Алгоритм случайного леса (Random Forest).
B) Алгоритм линейной регрессии.
C) Алгоритм анализа главных компонент (PCA).
D) Алгоритм Apriori.

Задание № 2. Какой компонент классической сигнатурной системы обнаружения вторжений (IDS) отвечает за сравнение наблюдаемой активности с базой известных шаблонов атак?

A) Модуль сбора данных (Sensor).
B) Детектор (Detector).
C) База данных событий.
D) Консоль управления.

Задание № 3. При интерпретации результатов работы IDS аналитик видит, что система генерирует много предупреждений о несуществующих атаках. Какой термин описывает этот тип ошибки?

A) Ложноотрицательное срабатывание (False Negative).
B) Ложноположительное срабатывание (False Positive).
C) Истинно положительное срабатывание (True Positive).
D) Истинно отрицательное срабатывание (True Negative).

Задание № 4. Какой из форматов является стандартным для хранения захваченного сетевого трафика и последующего анализа с помощью интеллектуальных средств?

A) Формат PCAP.
B) Формат JSON.
C) Формат XML.
D) Формат CSV.

Задание № 5. Для применения результатов работы IDS в автоматизированной системе блокировки атак (IPS) критически важно, чтобы алгоритм обладал:

A) Максимальной скоростью обучения на исторических данных.
B) Низким процентом ложноположительных срабатываний.
C) Способностью работать без обновления сигнатур.
D) Сложным графическим интерфейсом.

Задание № 6. Какой Python-библиотекой наиболее целесообразно воспользоваться для быстрого прототипирования и сравнения различных классических алгоритмов машинного обучения при разработке детектора аномалий в сетевом трафике?

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

Задание № 7. Установите соответствие между типом системы обнаружения вторжений (IDS) и её ключевой характеристикой.

| Тип IDS | Ключевая характеристика |
|---|---|
| 1. Сетевая IDS (NIDS) | A) Анализирует журналы событий и активность на уровне операционной системы отдельного компьютера. |
| 2. Хостовая IDS (HIDS) | B) Мониторит сетевой трафик на уровне пакетов для выявления подозрительной активности. |
| 3. Сигнатурная IDS | C) Обнаруживает отклонения от заданного эталонного поведения системы или пользователя. |
| 4. Аномалийная IDS | D) Использует базу известных шаблонов (сигнатур) атак для поиска совпадений. |

Задание № 8. Установите соответствие между этапом анализа сетевого трафика с применением интеллектуальных средств и типичным действием или методом.

| Этап анализа | Действие / Метод |
|---|---|
| 1. Сбор и захват данных | A) Использование инструментов вроде tcpdump или Wireshark для получения файлов трафика (PCAP). |
| 2. Предобработка и извлечение признаков | B) Нормализация данных, кодирование категориальных признаков, создание новых производных признаков. |
| 3. Обучение и применение модели | C) Использование библиотек машинного обучения для классификации или обнаружения аномалий в данных. |
| 4. Визуализация и интерпретация | D) Построение графиков важности признаков, анализ ложных срабатываний, подготовка отчета. |

Задание № 9. Установите правильную последовательность этапов работы специалиста с системой интеллектуального обнаружения вторжений (IDS) на основе машинного обучения, от получения исходных данных до принятия решения.

а) Провести исследовательский анализ данных для выявления аномалий, распределений и взаимосвязей в сетевых логах.

б) Применить обученную модель машинного обучения к новым, ранее невиданным данным для генерации предсказаний.

в) На основе приоритизации и контекста сформулировать рекомендации по реагированию на инцидент

г) Произвести сбор и консолидацию сетевых журналов и данных о трафике из различных источников.

д) Обогатить исходные данные, добавив контекстную информацию.

е) Приоритизировать и проанализировать сгенерированные алерты, сопоставив их с моделью угроз MITRE ATT&CK.

ж) Обучить модель машинного обучения на размеченном историческом наборе данных.

з) Выполнить предобработку данных: очистку от шума, нормализацию, кодирование категориальных признаков, создание новых признаков.

Задание № 10. Установите правильную последовательность действий аналитика при обработке и верификации алерта, сгенерированного интеллектуальной системой обнаружения вторжений (IDS).

а) Сопоставить действия злоумышленника с тактиками и техниками матрицы MITRE ATT&CK для понимания вектора атаки.

б) Принять решение об эскалации инцидента и инициировать процедуру реагирования в соответствии с регламентом.

в) Проверить актуальность и контекст сработавшего правила или ML-модели, а также актуальность индикаторов компрометации.

г) Собрать дополнительные артефакты с затронутой системы.

д) Изолировать скомпрометированный узел в сети для предотвращения распространения угрозы.

е) Провести первичный сбор контекста: определить источник, цель, временные метки и критичность актива.

ж) Обогатить исходный алерт информацией из внешних источников и внутренних систем.

з) Задокументировать все этапы расследования, выводы и предпринятые действия в отчете об инциденте.

**Перечень заданий открытого типа**

Задание № 1. Какой класс алгоритмов машинного обучения, не требующий размеченных данных об атаках для обучения, наиболее применим для обнаружения ранее неизвестных (zero-day) угроз в сетевом трафике?

Задание № 2. Назовите популярную Python-библиотеку, которая является стандартным инструментом для интерактивной визуализации данных и может использоваться для анализа и представления результатов работы IDS.

Задание № 3. Как называется основной открытый фреймворк/таксономия, который используется для формального описания техник и тактик злоумышленников и должен применяться для интерпретации и категоризации обнаруженных инцидентов?

Задание № 4. Какой стандартный формат вывода использует IDS Snort для генерации алертов, который затем может быть передан в SIEM-систему для дальнейшей корреляции?

Задание № 5. Дополните определение , вставляя пропущенное слово:

Метрика _____, рассчитываемая как отношение ложноположительных срабатываний к общему числу нормальных событий, критически важна для оценки эксплуатационных качеств IDS.

Задание № 6. Дополните определение, вставляя пропущенное слово:

Процесс автоматического обогащения событий IDS контекстной информацией из внешних источников, таких как списки вредоносных IP-адресов или хешей файлов, называется интеграцией с _____.

***Формируемая компетенция: ПК-2***

**Перечень заданий закрытого типа**

Задание № 1. Первым шагом при формализации задачи для интеллектуальной системы обнаружения вторжений является:

A) Написание кода алгоритма машинного обучения.

B) Выбор языка программирования Python или R.

C) Определение целей мониторинга и критичных для защиты активов подразделения (серверы, базы данных, рабочие станции).

D) Запуск системы сбора сетевого трафика (tcpdump).

Задание № 2. Какой метод анализа сетевой обстановки НЕ является типичным для выявления скрытых, многоэтапных атак (APT) и, следовательно, менее приоритетен при формализации задач для современной ИАС?

A) Корреляция событий из разнородных источников (журналы, NetFlow, алерты IDS).

B) Статистический подсчет общего объема входящего/исходящего трафика за сутки.

C) Построение временных профилей нормального поведения пользователей и систем.

D) Поиск аномалий в последовательностях сетевых подключений и команд.

Задание № 3. При формализации задачи по внедрению алгоритма машинного обучения для обнаружения фишинговых писем в корпоративной почте, ключевым нефункциональным требованием будет:

A) Минимизация доли ложноположительных срабатываний (чтобы не блокировать легитимные письма).

B) Использование исключительно нейронных сетей.

C) Наличие графического интерфейса на русском языке.
D) Скорость обучения модели на исторических данных.

Задание № 4. Какой из перечисленных элементов является обязательной частью формализованного технического задания (ТЗ) на разработку модуля интеллектуального анализа логов?

A) Финансовый план проекта.
B) Биографии членов команды разработчиков.
C) Описание входных данных (форматы логов, источники) и ожидаемых выходных данных (типы алертов, отчеты).
D) Рекомендации по выбору марки серверного оборудования.

Задание № 5. Для формализации задачи мониторинга на предмет утечки данных через внешние порты необходимо в первую очередь определить:

A) Марку межсетевого экрана.
B) Конкретные наблюдаемые индикаторы: аномально большие объемы исходящего трафика, соединения на нестандартные порты, передача архивов.
C) График отпусков сотрудников отдела.
D) Стоимость лицензии DLP-системы.

Задание № 6. Выберите НЕВЕРНОЕ утверждение о процессе формализации задач для систем поддержки принятия решений в ИБ:

A) Формализация позволяет четко разделить ответственность между аналитиками, разработчиками и администраторами.
B) Четко поставленная задача снижает риски неверной интерпретации данных системой и аналитиком.
C) Достаточно описать задачу в общих чертах, так как современные ИИ-системы способны самостоятельно "понять" контекст и детали.
D) Формализация включает определение критериев успеха и метрик для оценки работы системы (например, точность, полнота).

Задание № 7. Установите соответствие между методом/подходом к мониторингу сетевой обстановки и целью его применения при решении задач обнаружения вторжений.

| **Метод / Подход мониторинга** | **Цель применения для обнаружения вторжений** |
|---|---|
| 1. Анализ потоков данных (NetFlow/IPFIX) | A) Выявление скрытого взаимодействия узлов сети, формирования карты атаки и коммуникационных каналов бот-сети. |
| 2. Глубокий анализ пакетов (DPI) | B) Оценка общего объема и направлений трафика для выявления аномалий и целевых для детального изучения сегментов. |
| 3. Анализ графов связей между хостами | C) Изучение содержимого пакетов для идентификации протоколов, извлечения вредоносных сигнатур и полезных нагрузок. |
| 4. Поведенческий анализ (UEBA) | D) Обнаружение отклонений от шаблонов нормального поведения пользователей и систем, указывающих на компрометацию. |

Задание № 8. Установите соответствие между этапом формализации задачи для ИАС обнаружения вторжений и создаваемым документом или результатом.

| **Этап формализации задачи** | **Документ / Результат** |
|---|---|
| 1. Сбор и анализ требований стейкхолдеров | A) Модель угроз (Threat Model), описывающая активы, уязвимости, векторы атак и последствия. |
| 2. Определение контекста и угроз | B) Перечень и описание источников данных (логи, трафик, Threat Intel), их форматов и способов сбора. |
| 3. Спецификация источников и данных | C) Итоговое Техническое задание (ТЗ), |

| | |
|---|---|
| | содержащее цели, требования, критерии приемки. |
| 4. Формирование технического задания | D) Список функциональных и нефункциональных требований, приоритетов и ограничений. |

Задание № 9. Установите правильную последовательность этапов формализации задачи для разработки новой системы мониторинга сетевой обстановки.

а) Провести интервью со стейкхолдерами для сбора требований.
б) Выбрать конкретные технологии и инструменты для реализации.
в) Согласовать и утвердить техническое задание.
г) Определить цели и ключевые показатели эффективности системы.
д) Составить модель угроз для защищаемых активов.
е) Разработать проект архитектуры системы.
ж) Составить техническое задание на разработку системы.

Задание № 10. Установите правильную последовательность действий при подготовке к плановому аудиту защищенности сегмента промышленной сети.

а) Провести инструментальное сканирование сети и узлов на наличие уязвимостей.
б) Сформировать итоговый отчет с оценкой рисков и рекомендациями.
в) Определить перечень критичных активов в сегменте сети.
г) Составить план аудита и программу тестовых работ.
д) Проанализировать политики доступа и конфигурации сетевого оборудования.
е) Задокументировать выявленные несоответствия требованиям стандартов.
ж) Сопоставить выявленные уязвимости с тактиками возможных атак по MITRE ATT&CK.
з) Утвердить границы и цели проверки с руководством.

**Перечень заданий открытого типа**

Задание № 1. Назовите основную международную открытую таксономию, которую необходимо использовать при формализации задач для ИАС с целью детектирования конкретных техник и тактик злоумышленников по всему жизненному циклу атаки.

Задание № 2. Какой ключевой навык (soft skill), упомянутый в исследованиях цифровой грамотности, критически важен для формализации задач ИБ, так как позволяет объективно оценивать данные, выявлять неочевидные связи и не принимать результаты работы систем за абсолютную истину?

Задание № 3. Как называется основной принцип безопасной разработки, который должен быть учтен при формализации задачи на создание модуля ИАС и требует предоставления компонентам системы минимально необходимых для работы привилегий?

Задание № 4. Для формализации задачи по обнаружению аномалий в поведении привилегированных пользователей (администраторов) необходимо использовать данные из журналов событий безопасности Windows. Как называется конкретный журнал, в котором фиксируются события входа/выхода, использования прав и аудита доступа?

Задание № 5. Дополните определение, вставляя пропущенное слово:

Практика _____ мышления и декомпозиции сложных процессов на последовательность шагов является фундаментальной для корректной формализации задач, которые будут делегированы интеллектуальным автоматизированным системам .

Задание № 6. Дополните определение, вставляя пропущенное слово:

При формализации задачи для системы, обрабатывающей персональные данные, необходимо учитывать требования _____ приватности для обеспечения конфиденциальности информации на этапе анализа и обучения моделей.

***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 атаки) | C) Внедрение адаптивных механизмов обратной связи и периодического дообучения 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.

## 5. КРИТЕРИИ ОЦЕНКИ

### 5.1. Критерии оценки текущего контроля и промежуточной аттестации

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности обучающихся. В соответствии с этой системой применяются 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.:<br>– продемонстрирует глубокое и прочное усвоение материала;<br>– исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;<br>– правильно формирует определения;<br>– демонстрирует умения самостоятельной работы с нормативно-правовой литературой;<br>– умеет делать выводы по излагаемому материалу. |
| «Хорошо» - 4 баллов | «Хорошо» - 15 - 17 баллов | «Хорошо» - 70 - 84 баллов | Показывает достаточный уровень сформированности компетенций, т.е.:<br>– демонстрирует достаточно полное знание материала, основных теоретических положений;<br>– достаточно последовательно, грамотно логически стройно излагает материал;<br>– демонстрирует умения ориентироваться в нормальной литературе;<br>– 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.:<br>– демонстрирует общее знание изучаемого материала;<br>– испытывает серьезные затруднения при ответах на дополнительные вопросы;<br>– знает основную рекомендуемую литературу;<br>– умеет строить ответ в соответствии со структурой излагаемого материала. |
| «Неудовлетворительно» - 2 баллов | «Неудовлетворительно» - 1-11 баллов | «Неудовлетворительно» - 1-55 баллов | Ставится в случае:<br>– незнания значительной части программного материала;<br>– не владения понятийным аппаратом дисциплины;<br>– допущения существенных ошибок при изложении учебного материала;<br>– неумение строить ответ в соответствии со структурой излагаемого вопроса;<br>– неумение делать выводы по излагаемому материалу. |

**Критерии оценки тестовых заданий**

Таблица 4.

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

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

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

**Критерии оценки заданий на сопоставление**

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

## КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Таблица 5.

| Формируемые компетенции | № задания | Ответ |
|---|---|---|
| ПК-1 | **Задания закрытого типа** | |
| | № 1 | A |
| | № 2 | B |
| | № 3 | 1-B, 2-A, 3-D, 4-C |
| | № 4 | 1-A, 2-B, 3-C, 4-D |
| | № 5 | гдзажбев |
| | **Задания открытого типа** | |
| | № 1 | Алгоритмы обнаружения аномалий |
| | № 2 | Matplotlib |
| | № 3 | MITRE ATT&CK |
| | № 4 | False Positive Rate |
| | № 5 | Разведкой угроз |
| ПК-2 | **Задания закрытого типа** | |
| | № 1 | C |
| | № 2 | B |
| | № 3 | 1-B, 2-C, 3-A, 4-D |
| | № 4 | 1-D, 2-A, 3-B, 4-C |
| | № 5 | гадежбв |
| | **Задания открытого типа** | |
| | № 1 | MITRE ATT&CK |
| | № 2 | Критическое мышление |
| | № 3 | Наименьших привилегий |
| | № 4 | Алгоритмического |
| | № 5 | Дифференциальной |
| ПК-4 | **Задания закрытого типа** | |
| | № 1 | C |
| | № 2 | B |
| | № 3 | 1-B, 2-A, 3-D, 4-C |
| | № 4 | 1-B, 2-D, 3-A, 4-C |
| | № 5 | аевжбдг |
| | **Задания открытого типа** | |
| | № 1 | KDD Cup 1999 |
| | № 2 | Изолирующий лес |
| | № 3 | Точность, полнота |
| | № 4 | Трансферное |
| | № 5 | Состязательных |

**КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**

Таблица 6.

| Формируемые компетенции | № задания | Ответ |
|---|---|---|
| ПК-1 | **Задания закрытого типа** | |
| | № 1 | A |
| | № 2 | B |
| | № 3 | B |
| | № 4 | A |
| | № 5 | B |
| | № 6 | B |
| | № 7 | 1-B, 2-A, 3-D, 4-C |
| | № 8 | 1-A, 2-B, 3-C, 4-D |
| | № 9 | гдзажбев |
| | № 10 | вежгабдз |
| | **Задания открытого типа** | |
| | № 1 | Алгоритмы обнаружения аномалий |
| | № 2 | Matplotlib |
| | № 3 | MITRE ATT&CK |
| | № 4 | Формат Unified2 |
| | № 5 | False Positive Rate |
| | № 6 | Разведкой угроз |
| ПК-2 | **Задания закрытого типа** | |
| | № 1 | C |
| | № 2 | B |
| | № 3 | A |
| | № 4 | C |
| | № 5 | B |
| | № 6 | C |
| | № 7 | 1-B, 2-C, 3-A, 4-D |
| | № 8 | 1-D, 2-A, 3-B, 4-C |
| | № 9 | гадежбв |
| | № 10 | звгдажеб |
| | **Задания открытого типа** | |
| | № 1 | MITRE ATT&CK |
| | № 2 | Критическое мышление |
| | № 3 | Наименьших привилегий |
| | № 4 | Журнал Security.evtx |
| | № 5 | Алгоритмического |
| | № 6 | Дифференциальной |
| 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 1999 |
| | № 2 | Изолирующий лес |
| | № 3 | Точность, полнота |
| | № 4 | Внедрение многоуровневой системы валидации |
| | № 5 | Трансферное |
| | № 6 | Состязательных |