**Министерство науки и высшего образования Российской Федерации**

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

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**по дисциплине** «Система для сбора событий и логов»

Уровень образования — магистратура
(бакалавриат/магистратура/специалитет)

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

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

Разработчик _____ (подпись) Мирземагомедова М.М. к.т.н.
(ФИО уч. степень, уч. звание)

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

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

г. Махачкала 2026

СОДЕРЖАНИЕ

## 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью рабочей программы дисциплины «Система для сбора событий и логов» 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 «Система для сбора событий и логов» предусмотрено формирование следующей компетенции:

ПК-2. Способность выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности

ПК-4. Способность разрабатывать и применять методы и алгоритмы машинного обучения для решения задач искусственного интеллекта профессиональных задач

ПК-6. Способность выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем искусственного интеллекта по обеспечению.

Формой аттестации по дисциплине является зачет

## 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-2.2 Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности | ПК-2 |
| ПК-4.2 Разрабатывает унифицированные и обновляемые методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий | ПК-4 |
| ПК-6.1 Выбирает и разрабатывает программные компоненты систем искусственного интеллекта | ПК-6 |

## 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 |
| Тема 1. Способы машинного обучения | Письменная работа №.1.<br>Устный опрос<br>Лабораторная работа №<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 2 Методы машинного обучения | Письменная работа №.1.<br>Устный опрос<br>Лабораторная работа №2<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 3 Многоуровневое машинное обучение для обнаружения продвинутых угроз ИБ | Письменная работа №.1.<br>Устный опрос<br>Лабораторная работа №3<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 4 Глобальные аналитические данные по угрозам | Письменная работа №.2.<br>Устный опрос<br>Лабораторная работа №4<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 5 Моделирование поведения при внутренних угрозах | Письменная работа №.2.<br>Устный опрос<br>Лабораторная работа №5<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 6 Создание системы сбора событий безопасности домена | Письменная работа №.2.<br>Устный опрос<br>Лабораторная работа №6<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 7 Реализация и мониторинг политик сегментации | Письменная работа №.3.<br>Устный опрос<br>Лабораторная работа №7<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |
| Тема 8 Создание системы сбора событий безопасности домена. | Письменная работа №.3.<br>Устный опрос<br>Лабораторная работа №8<br>Самостоятельная работа<br>Реферат | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 | зачетная работа | ПК-2: ПК-2.2,<br>ПК-4: ПК-4.3,<br>ПК-6: ПК-6.1 |

### 3.2. Перечень заданий для текущего контроля

**Фор*мируемая компетенция: ПК-2***

**Перечень заданий закрытого типа**

Задание № 1. Какой способ машинного обучения предполагает наличие размеченных данных с известными ответами для обучения модели?

а) Обучение без учителя

б) Обучение с подкреплением

в) Обучение с учителем

г) Самообучение

Задание № 2. Какой метод машинного обучения основан на построении древовидной структуры решений на основе признаков?

а) Метод опорных векторов (SVM)

б) Дерево решений

в) Логистическая регрессия

г) Метод k-ближайших соседей

Задание № 3. Установите соответствие между этапом обработки логов в типовой SIEM-архитектуре и его описанием.

| **Этап обработки логов в типовой SIEM-архитектуре** | **Описание** |
|---|---|
| 1. Коллекция (Collection) | А. Приведение данных из разных источников к единому формату, извлечение полей. |
| 2. Нормализация и парсинг (Parsing) | Б. Добавление контекстной информации (например, геолокация по IP, данные об угрозах). |
| 3. Обогащение (Enrichment) | В. Сбор сырых данных с источников (агентами или напрямую). |
| 4. Корреляция (Correlation) | Г. Объединение событий по правилам для выявления сложных инцидентов. |
| 5. Визуализация и отчетность (Visualization) | Д. Представление данных на дашбордах, создание отчетов. |

Задание № 4. Установите соответствие между типом внутренней угрозы и примером аномалии, которую может обнаружить UEBA.

| **Тип внутренней угрозы** | **Пример аномалии, которую может обнаружить UEBA** |
|---|---|
| 1. Скомпрометированная учетная запись | А. Попытка доступа к большому количеству ресурсов, не характерных для роли пользователя, в нерабочее время. |
| 2. Нелояльный сотрудник (инсайдер) | Б. Загрузка необычно большого объема данных на внешний ресурс. |
| 3. Вредоносное ПО (Malware) | В. Последовательные аутентификации с одной учетной записи на множестве разных систем в короткий промежуток времени. |
| 4. Перемещение «боком» (Lateral Movement) | Г. Наличие на хосте процессов, подозрительно взаимодействующих с командным центром (C&C). |

Задание № 5. Расположите шаги по интеграции глобальных аналитических данных в процесс расследования инцидента.

А. Ручная или автоматическая блокировка обнаруженных индикаторов (IP, доменов) на периметре.
Б. Автоматический поиск (Hunting) по историческим данным на предмет ранее незамеченных компрометаций.
В. Подписка на актуальные каналы данных об угрозах (Threat Intelligence Feeds) в форматах STIX/TAXII.
Г. Обогащение внутренних событий безопасности из SIEM контекстом из TI-платформы.
Д. Верификация срабатывания (True/False Positive) и оценка воздействия на инфраструктуру.
Е. Корреляция: автоматическое создание инцидента при совпадении внутреннего события с индикатором из TI.

**Перечень заданий открытого типа**

Задание № 1. Назовите тип машинного обучения, требующий размеченных данных для обучения.
Задание № 2. Какой метод классификации и регрессии основан на построении древовидной структуры решений?
Задание № 3. Какой уровень анализа обрабатывает данные сетевых потоков (например, NetFlow) и метаданные пакетов?
Задание № 4. Дополните предложение, вставляя пропущенное слово:
В архитектуре ELK компонент _____ отвечает за прием, парсинг и преобразование логов перед отправкой в Elasticsearch.
Задание № 5. Дополните предложение, вставляя пропущенное слово:
Фаза _____ в UEBA необходима для формирования эталонного профиля нормальной активности без генерации ложных срабатываний.

**Фор*мируемая компетенция: ПК-4***

**Перечень заданий закрытого типа**

Задание № 1. Какой способ машинного обучения используется для обнаружения аномалий, когда неизвестно, что является нормальным, а что нет?
а) Обучение с учителем
б) Обучение без учителя
в) Обучение с подкреплением
г) Глубинное обучение

Задание № 2. Какой метод машинного обучения основан на идее нахождения гиперплоскости, максимально разделяющей классы?
а) Дерево решений
б) Метод опорных векторов (SVM)
в) Метод k-ближайших соседей (k-NN)
г) Наивный байесовский классификатор

Задание № 3. Установите соответствие между стандартом/протоколом и его назначением в контексте сбора логов и аналитики угроз.

| Стандарт/протокол | Назначение |
|---|---|
| 1. Syslog | А. Стандартный язык и формат для представления данных об угрозах (тактики, инструменты, индикаторы). |
| 2. CEF (Common Event Format) | Б. Протокол для транспортировки данных об угрозах (на основе HTTPS). |
| 3. STIX (Structured Threat Information eXpression) | в**)** Открытый стандартный формат для унификации данных безопасности от разных вендоров. |
| 4. TAXII (Trusted Automated eXchange of Indicator Information) | Г. Стандартизированный, расширяемый формат логов, предложенный компанией ArcSight. |
| 5. OCSF (Open Cybersecurity Schema Framework) | Д. Стандартный протокол для передачи сообщений о событиях в IP-сетях. |

Задание № 4. Установите соответствие между методом машинного обучения и типичной задачей в кибербезопасности.

| Метод машинного обучения | Типичная задача в кибербезопасности |
|---|---|
| 1. Классификация | А. Разделение сетевых подключений на группы для выявления новых типов атак. |
| 2. Кластеризация | Б. Прогнозирование всплеска подозрительной активности на основе исторических данных. |
| 3. Обнаружение аномалий (Anomaly Detection) | В. Маркировка файла как вредоносного или доброкачественного. |
| 4. Анализ временных рядов (Time Series Analysis) | Г. Выявление редких и подозрительных действий пользователя, отклоняющихся от его профиля. |

Задание № 5. Расположите этапы развертывания и работы системы UEBA в хронологическом порядке.

А. Наблюдение за системой в режиме обучения для формирования базовых поведенческих профилей.

Б. Настройка сбора необходимых данных о действиях пользователей, хостов и приложений.

В. Расследование инцидента, оценка уровня риска и принятие мер реагирования.

Г. Непрерывный мониторинг и генерация оповещений при отклонении от базовых профилей или выявлении известных вредоносных паттернов.

Д. Развертывание и тонкая настройка алгоритмов машинного обучения для обнаружения аномалий.

**Перечень заданий открытого типа**

Задание № 1. Назовите тип машинного обучения, используемый для обнаружения скрытых структур в данных без предварительных меток.

Задание № 2. Какой метод группирует объекты в кластеры по схожести их характеристик?

Задание № 3. Какой уровень анализа фокусируется на процессах, вызовах реестра и файловой активности на конечной точке?

Задание № 4. Дополните предложение, вставляя пропущенное слово:

Система _____ анализирует отклонения в поведении пользователей и сущностей от базового профиля для выявления инсайдерских угроз.

Задание № 5. Дополните предложение, вставляя пропущенное слово:

Для пересылки событий с рабочих станций Windows в центральное хранилище часто настраивают _____.

**Фор*мируемая компетенция: ПК-6***

**Перечень заданий закрытого типа**

Задание № 1. Какой уровень многоуровневого машинного обучения отвечает за анализ поведения пользователей и хостов?

а) Сетевой уровень

б) Уровень приложений

в) Поведенческий уровень

г) Сигнатурный уровень

Задание № 2. Какой уровень многоуровневого машинного обучения отвечает за анализ сетевого трафика и выявление аномалий в потоках данных?

а) Сетевой уровень

б) Уровень приложений

в) Поведенческий уровень

г) Сигнатурный уровень

Задание № 3. Установите соответствие между компонентом системы мониторинга политик сегментации и его функцией.

| **Компоненты системы мониторинга политик сегментации** | **Функции** |
|---|---|
| 1. Сетевой брэдмауэр / NGFW | А. Применение правил фильтрации трафика между сетевыми сегментами, ведение логов. |
| 2. Система предотвращения вторжений (IPS) | Б. Анализ и блокировка аномального или вредоносного трафика на стыке сегментов. |
| 3. Прокси-сервер | В. Мониторинг и фильтрация веб-трафика, контроль доступа к внешним ресурсам. |
| 4. SIEM-система | Г. Корреляция логов доступа из разных источников для выявления нарушений политик. |
| 5. Средства контроля доступа к данным (DLP) | Д. Контроль и предотвращение утечки конфиденциальных данных за пределы сегмента. |

Задание № 4. Установите соответствие между способом машинного обучения и его ключевой характеристикой.

| **Способ машинного обучения** | **Ключевая характеристика** |
|---|---|
| 1. Обучение с учителем (Supervised Learning) | А. Модель учится на данных без заранее известных ответов, выявляя скрытые структуры. |
| 2. Обучение без учителя (Unsupervised Learning) | Б. Алгоритм взаимодействует со средой, получая награду или штраф за действия, чтобы выработать оптимальную стратегию. |
| 3. Обучение с подкреплением (Reinforcement Learning) | В. Модель запрашивает у «учителя» (оператора) метки для наиболее неопределенных данных, повышая эффективность обучения. |
| 4. Активное обучение (Active Learning) | Г. Модель обучается на размеченном наборе данных, где каждому примеру соответствует правильный ответ. |

Задание № 5. Расположите этапы развертывания централизованной системы сбора логов в домене Windows.

А. Настройка групповых политик (GPO) для включения расширенного аудита на контроллерах домена и рабочих станциях.

Б. Установка и настройка агентов сбора (например, Winlogbeat) или настройка Windows Event Forwarding.

В. Определение критичных источников событий: контроллеры домена, файловые серверы, серверы приложений.

Г. Развертывание и конфигурация центрального сервера (например, Elastic Stack: Elasticsearch, Logstash, Kibana).

Д. Проверка полноты сбора, создание дашбордов и правил корреляции для ключевых событий безопасности.

Е. Настройка конвейера обработки логов (парсинг, нормализация, обогащение) на центральном сервере.

**Перечень заданий открытого типа**

Задание № 1. Назовите тип обучения, при котором модель взаимодействует со средой, получая награды за правильные действия.

Задание № 2. Какой популярный алгоритм кластеризации основан на минимизации расстояний до центроидов?

Задание № 3. Какой подход объединяет данные с сетевого, хостового и пользовательского уровней для выявления сложных атак?

Задание № 4. Дополните предложение, вставляя пропущенное слово:

Многоуровневый подход повышает точность обнаружения за счет _____ недостатков одного уровня данными другого.

Задание № 5. Дополните предложение, вставляя пропущенное слово:

Вредоносный IP-адрес, хэш файла или домен являются примерами _____ компрометации (IoC).

## 4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

***Формируемая компетенция: ПК-2***

**Перечень заданий закрытого типа**

Задание № 1. Какой из перечисленных источников глобальных аналитических данных по угрозам предоставляет информацию об известных вредоносных IP-адресах и доменах?
а) Национальный институт стандартов и технологий (NIST)
б) Открытые источники угроз (Open Source Threat Intelligence)
в) Внутренние логи безопасности
г) Базы данных уязвимостей (CVE)

Задание № 2. Какой формат обмена данными об угрозах используется для структурированного представления информации об индикаторах компрометации?
а) XML
б) STIX (Structured Threat Information Expression)
в) JSON
г) CSV

Задание № 3. Какой подход используется для моделирования поведения при внутренних угрозах и основан на построении профилей нормального поведения пользователей?
а) Сигнатурный анализ
б) Динамический анализ вредоносного ПО
в) Статический анализ кода
г) Анализ поведения пользователей и сущностей (UEBA)

Задание № 4. Какой показатель является ключевым при моделировании поведения для выявления внутренних угроз?
а) Количество попыток входа в систему
б) Отклонение от нормального поведения (аномалии)
в) Количество отправленных электронных писем
г) Время, проведенное в сети

Задание № 5. Какой протокол является стандартным для сбора и передачи логов в системе сбора событий безопасности?
а) HTTP
б) Syslog
в) FTP
г) SMTP

Задание № 6. Какой компонент системы сбора событий безопасности отвечает за хранение и индексацию логов?
а) База данных логов
б) Агент сбора логов
в) Анализатор логов
г) Визуализатор логов

Задание № 7. Установите соответствие между конкретным методом машинного обучения и задачей в области анализа событий безопасности, для которой он наиболее применим.

| **Метод машинного обучения** | **Задача** |
|---|---|
| 1. K-ближайших соседей (k-NN) | А. Классификация сетевых пакетов на основе исторических данных о легитимном и вредоносном трафике. |
| 2. Дерево решений (Decision Tree) | Б. Обнаружение новых, ранее неизвестных типов атак путем группировки похожих событий в логиах. |
| 3. Метод опорных векторов (SVM) | В. Интерпретируемое принятие решений о блокировке активности на основе набора правил, извлеченных из данных. |
| 4. Кластеризация k-средних (k-Means) | Г. Нахождение оптимальной границы разделения между классами в высокоразмерном пространстве признаков для обнаружения аномалий. |

Задание № 8. Установите соответствие между уровнем анализа в многоуровневой системе МО и типом данных или признаков, которые на нем обрабатываются.

| Уровень анализа | Тип данных или признак |
|---|---|
| 1. Сетевой уровень | Последовательность системных вызовов, изменения в реестре, запуск процессов. |
| 2. Уровень хоста (Endpoint) | Б. Геолокация входа, частота обращений к ресурсам, отклонения от персональной поведенческой базы. |
| 3. Пользовательский и сущностный уровень (UEBA) | В. Потоки NetFlow, протоколы, объемы трафика, аномальные порты. |
| 4. Уровень приложения | Г. Логи веб-сервера, аномальные SQL-запросы, параметры API-вызовов. |

Задание № 9. Расположите этапы жизненного цикла модели машинного обучения для задач обнаружения угроз в правильной последовательности.

А. Развертывание модели в рабочую среду и интеграция с SIEM.

Б. Сбор и предобработка журналов событий безопасности (логов).

В. Разметка данных (например, присвоение меток «нормально»/«атака») для обучения.

Г. Тестирование модели на новых, невиданных ею данных (тестовой выборке).

Д. Обучение выбранного алгоритма (например, случайного леса) на подготовленных данных.

Е. Анализ признаков (Feature Engineering) и создание обучающей выборки.

Задание № 10. Расположите этапы обработки данных в многоуровневой системе обнаружения угроз в порядке их выполнения.

А. Агрегация и корреляция меток/оценок риска с сетевого, хостового и пользовательского уровней.

Б. Применение специализированных моделей МО для анализа поведения пользователей и сущностей (UEBA).

В. Предобработка и извлечение признаков из сетевого трафика (например, длительность сессии, количество пакетов).

Г. Сбор сырых данных с разных уровней: NetFlow, логи с серверов, события аутентификации.

Д. Применение моделей для анализа активности на хостах (процессы, вызовы реестра).

Е. Принятие финального решения о наличии комплексной атаки и генерация инцидента.

**Задания открытого типа**

Задание № 1. Какой стандартизированный структурированный язык используется для описания информации об угрозах?

Задание № 2. Назовите класс решений, анализирующий отклонения в поведении пользователей, хостов и приложений от базовых профилей.

Задание № 3. Какой популярный открытый стек технологий используется для сбора, обработки, хранения и визуализации логов?

Задание № 4. Назовите самый важный журнал на контроллере домена для отслеживания событий входа, доступа и изменений политик.

Задание № 5. Дополните предложение, вставляя пропущенное слово:

Для обнаружения сложных целевых атак данные с _____ уровня (трафик) коррелируют с данными с хостового уровня (процессы).

Задание № 6. Дополните предложение, вставляя пропущенное слово:

Протокол _____ используется для безопасного обмена структурированными данными об угрозах в формате STIX.

***Формируемая компетенция: ПК-4***

**Задания закрытого типа**

Задание № 1. Какой механизм используется для реализации политик сегментации в компьютерных сетях?

а) Виртуализация

б) Межсетевые экраны (брандмауэры)

в) Шифрование данных

г) Резервное копирование

Задание № 2. Какой инструмент используется для мониторинга соблюдения политик сегментации?

а) Антивирусное программное обеспечение

б) Система обнаружения вторжений (IDS)

в) Система управления базами данных

г) Система управления конфигурациями

Задание № 3. Какой компонент системы сбора событий безопасности домена отвечает за сбор логов с контроллеров домена?

а) Агент сбора логов на контроллере домена

б) Сервер сбора логов

в) База данных логов

г) Консоль управления

Задание № 4. Какой тип логов является наиболее важным для сбора с контроллеров домена?

а) Логи безопасности (Security logs)

б) Логи приложений

в) Системные логи

г) Логи оборудования

Задание № 5. Какой алгоритм машинного обучения часто используется для кластеризации и может помочь в обнаружении аномалий?
а) Линейная регрессия
б) Наивный байесовский классификатор
в) Дерево решений
г) k-средних (k-means)

Задание № 6. Какой из перечисленных методов машинного обучения является примером обучения с подкреплением?
а) Обучение агента в среде для максимизации награды
б) Классификация изображений
в) Кластеризация данных
г) Обнаружение выбросов

Задание № 7. Установите соответствие между форматом/стандартом обмена данными об угрозах и его основным назначением.

| **Формат /стандарт обмена данными** | **Основное назначение** |
|---|---|
| 1. STIX (Structured Threat Information eXpression) | А. Специфичный, но гибкий XML-формат для описания индикаторов компрометации. |
| 2. TAXII (Trusted Automated Exchange of Indicator Information) | Б. Открытая платформа для совместного использования, хранения и корреляции данных об угрозах. |
| 3. OpenIOC | В. Язык и сериализация для детального описания тактик, техник, процедур (TTP), инструментов и индикаторов. |
| 4. MISP (Malware Information Sharing Platform & Threat Sharing) | Г. Протокол для безопасного обмена данными в формате STIX. |

Задание № 8. Установите соответствие между концепцией/инструментом сегментации и его описанием.

| **Концепция/инструмент сегментации** | **Описание** |
|---|---|
| 1. Микросегментация | А. Подход, при котором доступ к ресурсам предоставляется только после строгой проверки контекста (идентичность, устройство, др.) для каждого запроса, независимо от местоположения в сети. |
| 2. Межсетевой экран следующего поколения (NGFW) | Б. Детализированное разделение сети на очень маленькие сегменты (вплоть до одной рабочей нагрузки) с индивидуальными политиками доступа. |
| 3. Zero Trust (Никому не доверяй) | В. Устройство, которое применяет политики безопасности на границе сегментов, анализируя трафик на уровне приложений и используя данные об угрозах. |
| 4. Аудит SACL (System Access Control List) | Г. Механизм Windows для журналирования попыток доступа (успешных/неуспешных) к файлам, папкам и другим объектам, критичный для мониторинга соблюдения политик. |

Задание № 9. Расположите шаги по интеграции глобальных аналитических данных в процесс расследования инцидента.

А. Ручная или автоматическая блокировка обнаруженных индикаторов (IP, доменов) на периметре.
Б. Автоматический поиск (Hunting) по историческим данным на предмет ранее незамеченных компрометаций.
В. Подписка на актуальные каналы данных об угрозах (Threat Intelligence Feeds) в форматах STIX/TAXII.
Г. Обогащение внутренних событий безопасности из SIEM контекстом из TI-платформы.
Д. Верификация срабатывания (True/False Positive) и оценка воздействия на инфраструктуру.
Е. Корреляция: автоматическое создание инцидента при совпадении внутреннего события с индикатором из TI.

Задание № 10. Расположите этапы развертывания и работы системы UEBA в хронологическом порядке.
А. Наблюдение за системой в режиме обучения для формирования базовых поведенческих профилей.
Б. Настройка сбора необходимых данных о действиях пользователей, хостов и приложений.
В. Расследование инцидента, оценка уровня риска и принятие мер реагирования.
Г. Непрерывный мониторинг и генерация оповещений при отклонении от базовых профилей или выявлении известных вредоносных паттернов.
Д. Развертывание и тонкая настройка алгоритмов машинного обучения для обнаружения аномалий.

**Задания открытого типа**

Задание № 1. Какая современная концепция безопасности предполагает, что доверие никогда не предоставляется по умолчанию, а постоянно проверяется.
Задание № 2. Назовите встроенную в Windows технологию для централизованной пересылки событий с компьютеров домена на сервер-коллектор.
Задание № 3. Назовите фазу работы UEBA, в которой система изучает нормальную активность без генерации оповещений.
Задание № 4. Назовите протокол для безопасного обмена данными в формате STIX.
Задание № 5. Дополните предложение, вставляя пропущенное слово:
Метод _____ позволяет модели самостоятельно находить скрытые структуры и аномалии в неразмеченных потоках логов.
Задание № 6. Дополните предложение, вставляя пропущенное слово:
Метод _____ хорошо интерпретируется и используется для построения прозрачных правил обнаружения на основе древовидной структуры.

***Формируемая компетенция: ПК-6***

**Перечень заданий закрытого типа**

Задание № 1. Какой стандарт де-факто используется для обмена данными об угрозах в реальном времени?
а) STIX/TAXII
б) XML/RSS
в) JSON/HTTP
г) CSV/FTP

Задание № 2. Какой подход к машинному обучению используется в многоуровневых системах для комбинирования результатов с разных уровней?
а) Ансамблевое обучение
б) Объединение данных (Fusion)
в) Уменьшение размерности
г) Увеличение данных

Задание № 3. Какой показатель эффективности системы моделирования поведения при внутренних угрозах является наиболее важным?
а) Количество обнаруженных угроз
б) Соотношение истинно положительных и ложноположительных срабатываний
в) Скорость обработки событий
г) Количество отслеживаемых пользователей

Задание № 4. Какой компонент системы сбора событий безопасности домена отвечает за корреляцию событий и генерацию оповещений?
а) Агент сбора
б) Хранилище логов
в) Движок корреляции
г) Визуализатор

Задание № 5. Какой метод мониторинга политик сегментации позволяет обнаруживать попытки несанкционированного доступа между сегментами?
а) Анализ трафика в реальном времени
б) Аудит журналов доступа
в) Сканирование портов
г) Тестирование на проникновение

Задание № 6. Какой из перечисленных факторов является критическим при создании системы сбора событий безопасности домена?
а) Количество серверов в домене
б) Масштабируемость и производительность системы сбора логов
в) Тип операционной системы на рабочих станциях
г) Количество пользователей в домене

Задание № 7. Установите соответствие между форматом/стандартом обмена данными об угрозах и его основным назначением.

| **Формат/стандарт обмена данными об угрозах** | **Основное назначение** |
|---|---|
| 1. STIX (Structured Threat Information eXpression) | А. Специфичный, но гибкий XML-формат для описания индикаторов компрометации. |
| 2. TAXII (Trusted Automated Exchange of Indicator Information) | Б. Открытая платформа для совместного использования, хранения и корреляции данных об угрозах. |
| 3. OpenIOC | В. Язык и сериализация для детального описания тактик, техник, процедур (TTP), инструментов и индикаторов. |
| 4. MISP (Malware Information Sharing | Г. Протокол для безопасного обмена данными в формате |

| | |
|---|---|
| Platform & Threat Sharing) | STIX. |

Задание № 8. Установите соответствие между типом аномального поведения, выявляемого UEBA, и его интерпретацией с точки зрения внутренней угрозы.

| **Аномальное поведение** | **Интерпретация** |
|---|---|
| 1. Кража данных (Data Exfiltration) | А. Необычно высокий объем исходящего трафика, массовая загрузка файлов на внешние ресурсы или в облако. |
| 2. Скомпрометированные учетные данные (Compromised Credentials) | Б. Входы в систему из географически невозможных локаций, множественные неудачные попытки входа с последующим успехом. |
| 3. Вредоносные инсайдеры (Malicious Insider) | В. Регулярный доступ к конфиденциальным данным вне рабочего времени, попытки обхода средств контроля. |
| 4. Перемещение внутри сети (Lateral Movement) | Г. Последовательные подключения с одной учетной записи к множеству различных серверов в короткий промежуток времени. |

Задание № 9. Расположите этапы развертывания централизованной системы сбора логов в домене Windows.

А. Настройка групповых политик (GPO) для включения расширенного аудита на контроллерах домена и рабочих станциях.

Б. Установка и настройка агентов сбора (например, Winlogbeat) или настройка Windows Event Forwarding.

В. Определение критичных источников событий: контроллеры домена, файловые серверы, серверы приложений.

Г. Развертывание и конфигурация центрального сервера (например, Elastic Stack: Elasticsearch, Logstash, Kibana).

Д. Проверка полноты сбора, создание дашбордов и правил корреляции для ключевых событий безопасности.

Е. Настройка конвейера обработки логов (парсинг, нормализация, обогащение) на центральном сервере.

Задание № 10. Расположите этапы реализации и мониторинга политик микросегментации в корпоративной сети.

А. Внедрение правил сегментации на межсетевых экранах, коммутаторах или средствах микросегментации.

Б. Анализ бизнес-процессов и приложений для определения требуемых потоков трафика между сегментами.

В. Регулярный пересмотр и адаптация правил на основе данных мониторинга и изменений в инфраструктуре.

Г. Составление детальной карты сети и инвентаризация всех систем, их ролей и взаимосвязей.

Д. Активное мониторинг логов межсетевых экранов и системы сбора событий на предмет нарушений или попыток обхода политик.

Е. Разработка матрицы доступа (кто, к кому, на каких портах) и проектирование границ сегментов.

**Задания открытого типа**

Задание № 1. Назовите конкретные наблюдаемые артефакты, такие как вредоносные IP-адреса, домены или хэши файлов.

Задание № 2. Какая тактика атакующего заключается в перемещении между узлами внутри сети для расширения доступа.

Задание № 3. Назовите стандартный протокол для пересылки системных сообщений и логов в IP-сетях.

Задание № 4. Назовите самый важный журнал на контроллере домена для отслеживания событий входа, доступа и изменений политик.

Задание № 5. Дополните предложение, вставляя пропущенное слово:

Для обучения модели классификации вредоносного трафика требуется набор данных с метками, что характерно для подхода _____ (машинного) обучения.

Задание № 6. Дополните предложение, вставляя пропущенное слово:

Алгоритм _____ используется для разделения объектов на группы по схожести и часто применяется для первичной кластеризации событий безопасности.

## 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-2 | **Задания закрытого типа** | |
| | 1. | в |
| | 2. | б |
| | 3. | 1-В, 2-А, 3-Б, 4-Г, 5-Д |
| | 4. | 1-А, 2-Б, 3-Г, 4-В |
| | 5. | В Г Е Д Б А |
| | **Задания открытого типа** | |
| | 1. | Обучение с учителем |
| | 2. | Дерево решений |
| | 3. | Сетевой уровень |
| | 4. | Logstash |
| | 5. | обучения |
| ПК-4 | **Задания закрытого типа** | |
| | 1. | б |
| | 2. | б |
| | 3. | 1-Д, 2-Г, 3-А, 4-Б, 5-В |
| | 4. | 1-В, 2-А, 3-Г, 4-Б |
| | 5. | Б А Д Г В |
| | **Задания открытого типа** | |
| | 1. | Контрольное Обучение |
| | 2. | Кластеризация |
| | 3. | Хостовый уровень |
| | 4. | UEBA |
| | 5. | WEF |
| ПК-6 | **Задания закрытого типа** | |
| | 1. | в |
| | 2. | а |
| | 3. | 1-А, 2-Б, 3-В, 4-Г, 5-Д |
| | 4. | 1-Г, 2-А, 3-Б, 4-В |
| | 5. | В А Г Е Б Д |
| | **Задания открытого типа** | |
| | 1. | Обучение с подкреплением |
| | 2. | К-средних |
| | 3. | Многоуровневое обнаружение / |
| | 4. | компенсации |
| | 5. | индикатора |

## КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

| Формируемые компетенции | № задания | Ответ |
|---|---|---|
| ПК-2 | **Задания закрытого типа** | |
| | 1. | б |
| | 2. | б |
| | 3. | г |
| | 4. | б |
| | 5. | б |
| | 6. | а |
| | 7. | 1-А, 2-В, 3-Г, 4-Б |
| | 8. | 1-В, 2-А, 3-Б, 4-Г |
| | 9. | Б В Е Д Г А |
| | 10. | Г В Д Б А Е |
| | **Задания открытого типа** | |
| | 1. | STIX |
| | 2. | UEBA |
| | 3. | ELK-стек |
| | 4. | Журнал безопасности |
| | 5. | сетевого |
| | 6. | TAXII |
| ПК-4 | **Задания закрытого типа** | |
| | 1. | б |
| | 2. | б |
| | 3. | б |
| | 4. | а |
| | 5. | г |
| | 6. | а |
| | 7. | 1-В, 2-Г, 3-А, 4-Б |
| | 8. | 1-Б, 2-В, 3-А, 4-Г |
| | 9. | В Г Е Д Б А |
| | 10. | Б А Д Г В |
| | **Задания открытого типа** | |
| | 1. | Zero Trust / Нулевое доверие |
| | 2. | Windows Event Forwarding / WEF |
| | 3. | Обучение / Baseline establishment |
| | 4. | TAXII |
| | 5. | обучения без учителя / unsupervised learning |
| | 6. | дерева решений / decision tree |
| ПК-6 | **Задания закрытого типа** | |
| | 1. | а |
| | 2. | б |
| | 3. | б |
| | 4. | в |
| | 5. | б |
| | 6. | б |
| | 7. | 1-В, 2-Г, 3-А, 4-Б |
| | 8. | 1-А, 2-Б, 3-В, 4-Г |

| | | |
|---|---|---|
| | 9. | В А Г Е Б Д |
| | 10. | Г Б Е А Д В |
| | **Задания открытого типа** | |
| | 1. | Индикаторы компрометации / IoC |
| | 2. | Lateral movement / Боковое перемещение |
| | 3. | Syslog |
| | 4. | Журнал безопасности / Security Log |
| | 5. | с учителем / supervised |
| | 6. | k-средних / k-means |