УДК 004.9 *DOI 10.55421/3034-4689_2026_29_9_83*

А. В. Каляшина, Ю. Н. Смирнов

ИНТЕЛЛЕКТУАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ СЕТЕВЫХ АТАК

Ключевые слова: информационная безопасность, веб-ресурсы, сетевой трафик, интеллектуальная система, машинное обучение.

Целью исследования является повышение информационной безопасности клиентских ресурсов для компаний, занимающихся разработкой и хостингом веб-решений. В статье представлены результаты реинжиниринга информационной системы мониторинга веб-ресурсов и разработки интеллектуальной информационной системы для автоматического обнаружения и классификации кибератак. Объект исследования – процессы мониторинга сетевой безопасности и анализа трафика веб-ресурсов, предмет исследования – методы машинного обучения для мультиклассовой классификации сетевых атак на основе наборов данных. Проведя анализ бизнес-процессов нескольких предприятий, работающих в сфере информационной безопасности, авторы сделали вывод о том, что существующая система мониторинга клиентских веб-ресурсов фиксирует лишь факт недоступности сайта, не определяя причины сбоев и не предоставляя инструментов оперативного реагирования. Авторами создан интеллектуальный модуль, способный в автоматическом режиме анализировать сетевые данные, выявлять аномалии и классифицировать их по типам атак с применением технологий машинного обучения. Функциональная модель подсистемы отображает последовательность действий, которые выполняются системой — от момента перехвата сетевого пакета до применения мер реагирования и записи инцидента. Основные источники данных для системы – сетевые журналы проверяемых сайтов, системные логи и результаты HTTP-запросов. Выходные массивы предназначены для хранения и передачи результатов анализа трафика, формирования уведомлений об атаках и аномалиях, последующего анализа в подсистемах визуализации, а также для пополнения обучающей выборки при дообучении модели машинного обучения. Они обеспечивают трассируемость всех решений системы защиты и позволяют восстанавливать полную картину инцидента. В ходе работы спроектирована и реализована интеллектуальная модель классификации сетевого трафика на основе алгоритма XGBoost. Модель показала очень высокие результаты: точность порядка 97%, практически полное распознавание основных атак (DDoS, DoS, PortScan, Botnet

A. V. Kalyashina, Yu. N. Smirnov

INTELLIGENT INFORMATION SYSTEM FOR DETECTION AND CLASSIFICATION OF NETWORK ATTACKS

Keywords: Information security, web resources, network traffic, intelligent system, machine learning.

The aim of this study is to improve the information security of client resources for companies developing and hosting web solutions. This article presents the results of reengineering a web resource monitoring information system and developing an intelligent information system for the automatic detection and classification of cyberattacks. The object of this study is network security monitoring and web resource traffic analysis, and the subject of this study is machine learning methods for multi-class classification of network attacks based on datasets. After analyzing the business processes of several companies working in the field of information security, the authors concluded that the existing web resource monitoring system only records the fact of site unavailability, without determining the cause of failures or providing tools for rapid response. The authors created an intelligent module capable of automatically analyzing network data, identifying anomalies, and classifying them by attack type using machine learning technologies. The functional model of the subsystem displays the sequence of actions performed by the system—from the moment a network packet is intercepted to the application of response measures and recording of the incident. The primary data sources for the system are network logs of the websites being monitored, system logs, and HTTP request results. Output arrays are used to store and transmit traffic analysis results, generate attack and anomaly notifications, perform subsequent analysis in visualization subsystems, and supplement the training set for further training of the machine learning model. They ensure traceability of all security system decisions and enable the reconstruction of a complete picture of the incident. During the project, an intelligent network traffic classification model based on the XGBoost algorithm was designed and implemented. The model demonstrated very high results: approximately 97% accuracy and almost complete recognition of major attacks (DDoS, DoS, PortScan, Botnet).

Введение

Вопросы применения методов машинного обучения для обнаружения компьютерных атак активно обсуждаются в последние годы. По данной тематике опубликовано множество работ[1-4]. В работе [2] сформулированы направления исследований в области информационной безопасности. Одна из важнейших задач – применение методов искусственного интеллекта и машинного обучения. В работе [3] особенно выделяется задача разработки новых наборов данных, которые содержат современные типы кибератак. Также в этой статье проведен анализ общедоступных наборов данных, формализованы требования к создаваемым наборам данных для обучения: разнородности представленных атак, наличия полной конфигурации сети, полного сетевого взаимодействия, разнородности протоколов и др. Сформирован публичный набор данных

CICIDS2017, который впоследствии получил широкое распространение в исследовательских проектах. [1]

В работах [4,8] приведен опыт применения нейронных сетей для обнаружения информационных атак, представлен обзор 34 общедоступных наборов данных с указанием их отличительных особенностей, используемых сценариев атак, имеющихся недостатков. Предложена методология оценки применимости наборов данных к различным задачам информационной безопасности. Среди проанализированных наборов данных для использования в практических задачах авторы рекомендуют наборы CICIDS 2017, CIDDS-001, UGR-16 и UNSW-NB15.

Для компаний, занимающихся разработкой и хостингом веб-решений, критически важными являются вопросы обеспечения информационной безопасности клиентских ресурсов. Согласно статистике специализированных центров мониторинга киберугроз, количество DDoS-атак на российские компании выросло на 35-40% в 2024 году по сравнению с предыдущим периодом. Атаки на веб-приложения (SQL-инъекции, XSS, брутфорс) составляют до 25% от всех инцидентов безопасности [5].

Данное научное исследование посвящено реинжинирингу информационной системы мониторинга веб-ресурсов и разработке интеллектуальной информационной системы (ИИС) для автоматического обнаружения и классификации кибератак

Объект исследования – процессы мониторинга сетевой безопасности и анализа трафика веб-ресурсов.

Предмет исследования – методы машинного обучения (XGBoost) для мультиклассовой классификации сетевых атак на основе наборов данных CICIDS2017 и CSECICIDS2018 [6], [8].

Цель работы – создание интеллектуальной информационной системы (ИИС), обеспечивающей классификацию 9 типов атак (DDoS, BruteForce и др.)

Решаемые задачи: анализ требований и действующей информационной системы (ИС); проектирование архитектуры ИИС (IDEF0, ER-модели); разработка и обучение нейросетевой модели; реализация в Kaggle Notebook с оценкой результатов.

Проектирование интеллектуальной информационной системы

Проведя анализ бизнес процессов нескольких предприятий, работающих в сфере информационной безопасности, авторы сделали вывод о том, что существующая система мониторинга клиентских веб-ресурсов фиксирует лишь факт недоступности сайта, не определяя причины сбоев и не предоставляя инструментов оперативного реагирования. Для решения этой проблемы необходим переход от реактивного к проактивному управлению подобными инцидентами [7].

Задачи и цели исследования:

1. Автоматизация анализа инцидентов – разработка интеллектуального модуля WebGuard-AI, способного в режиме реального времени классифицировать типы веб-атак на основе анализа сетевого трафика.

2. Интеграция анализа трафика в процесс мониторинга - к существующему процессу проверки доступности сайтов добавить этап интеллектуального анализа, с помощью которого система не только определяет, доступен ли ресурс, но и может выявлять DDoS, брутфорс, SQL-инъекции и другие типы атак

3. Внедрение стандартов интеллектуального управления инцидентами [2], [8].

4. Повышение уровня автоматизации принятия решений [1], [9].

5. Интеграция с внутренней системой поддержки клиентов - при обнаружении атак система должна автоматически создать задачу в CRM, тем самым обеспечивая прозрачность и контроль всех этапов обработки инцидента

В результате проектирования ИИС WebGuard-AI предприятие получает не просто инструмент мониторинга, а интеллектуальную платформу поддержки решений в области кибербезопасности, способную адаптироваться к динамическим угрозам и обеспечивать устойчивую работу клиентских веб-ресурсов [10].

Структура ИИС имеет модульный характер и включает несколько взаимосвязанных компонентов:

1) Модуль сбора данных
2) Модуль предварительной обработки данных
3) Интеллектуальный модуль анализа
4) Модуль обработки результатов
5) Система уведомлений
6) База данных
7) Веб-интерфейс
8) Модуль интеграции с существующей системой мониторинга.

Для эффективного функционирования ИИС каждая подсистема выполняет определённый набор задач, направленных на обеспечение автоматизации процессов мониторинга, анализа событий и реагирования на инциденты безопасности.

В проектируемой ИИС используются современные методы машинного обучения, что позволяет различать обычную активность и потенциальные сетевые атаки с высокой точностью [11].

Классификация применимости технологий искусственного интеллекта в различных подсистемах [12]:

1) Подсистемы без применения ИИ (технического типа):
- Сбор данных
- Хранение в базе данных
- Интеграционные компоненты
2) Подсистемы с частичным применением ИИ:
- Предобработка данных (очистка, фильтрация выбросов)
- Система уведомлений (контекстный анализ приоритетности инцидентов)

Аналитический модуль (прогнозирование динамики атак)

3) Подсистемы с полным применением ИИ:

- Интеллектуальный модуль анализа трафика (основная ML-модель)

- Подсистема принятия решений, использующая результаты анализа модели

Таким образом, наибольшая роль технологий искусственного интеллекта реализуется в ядре системы WebGuard-AI, где выполняются задачи машинного обучения по классификации сетевых угроз и принятие интеллектуальных решений о характере событий. Остальные подсистемы обеспечивают поддержку и передачу данных, создавая единую интеллектуальную экосистему мониторинга и защиты веб-ресурсов предприятия.

Система формирует замкнутый контур обмена информацией: данные проходят через сбор, обработку, анализ, принятие решений и обратную связь, обеспечивая постоянное совершенствование модели и точности детектирования сетевых атак.

Разработка подсистемы «Интеллектуальный анализ трафика»

В процессе реинжиниринга и проектирования ИИС предприятия выявлена необходимость автоматизации анализа сетевого трафика для выявления и классификации кибератак на клиентские веб-ресурсы [13]. Действующий механизм мониторинга фиксирует только факт доступности или недоступности сайта, не определяя причины инцидента. Это ограничивает эффективность реагирования и не позволяет своевременно обнаруживать вредоносную активность [14].

Целью разработки данной подсистемы является создание интеллектуального модуля, способного в автоматическом режиме анализировать сетевые данных, выявлять аномалии и классифицировать их по типам атак с применением технологий машинного обучения.

Задача «Обнаружение и классификация сетевых атак» подсистемы «Интеллектуальный анализ трафика» функционирует в составе интеллектуальной информационной системы защиты WebGuard-AI.

Подсистема интеллектуального анализа трафика интегрируется в действующую систему мониторинга предприятия и будет функционировать в серверном окружении [15]. Основные источники данных – сетевые журналы проверяемых сайтов, системные логи и результаты HTTP-запросов. Все данные поступают на обработку через API в формате CSV, JSON или потоковых сообщений [16]. Функциональная модель подсистемы отображает последовательность действий, которые выполняются системой — от момента перехвата сетевого пакета до применения мер реагирования и записи инцидента. Функциональная модель построена на основе нотации BPMN 2.0 и показывает взаимодействие всех основных элементов модуля анализа трафика в составе системы защиты WebGuard‑AI [17]. Как правило, существующие процессы включают множество последовательных этапов взаимодействия между техническим специалистом, менеджером и клиентом, что увеличивает время реакции на атаку и снижает эффективность защиты. Кроме того, отсутствие автоматизированной классификации угроз приводит к повышенной нагрузке на персонал.

Внедрение системы WebGuard‑AI автоматизирует ключевые этапы обнаружения и реагирования на атаки: от мониторинга трафика и классификации инцидентов средствами машинного обучения до автоматической блокировки источников атак и оповещения администратора. На рис. 1 представлена BPMN‑диаграмма бизнес‑процесса, которая демонстрирует сокращение количества ручных операций, параллельное выполнение задач мониторинга доступности и анализа инцидентов, а также прозрачный цикл обратной связи для дообучения модели на основе разметки администратора.

Целевой процесс значительно снижает время реакции на инциденты за счёт автоматизированной детекции и классификации атак с использованием модели XGBoost, параллельного мониторинга доступности защищаемых ресурсов и автоматического формирования команд на блокировку. Участие специалиста сводится к контролю за срабатываниями системы, анализу истории инцидентов и периодическому дообучению модели на размеченных данных, что обеспечивает постоянное повышение точности детекции.

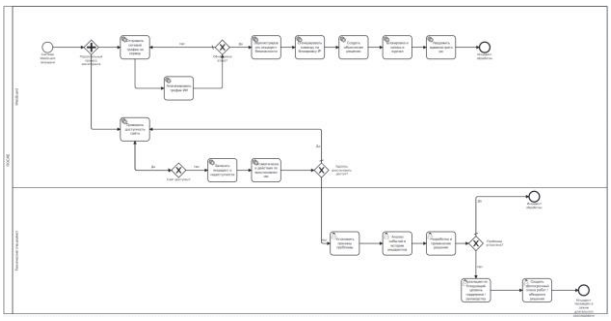

Рис. 1 – Бизнес-процесс обнаружения и реагирования на атаки

Fig. 1 – Business process for attack detection and response

Процесс обнаружения и классификации сетевых атак в системе WebGuard‑AI реализуется в виде следующей последовательности этапов [16]:

1. Инициализация системы мониторинга.

При запуске сервис загружает конфигурационные файлы, устанавливает соединения с источниками логов и базой данных, а также инициализирует обученную ML‑модель (XGBoost) и объект SHAP‑explainer. Запускается основной цикл опроса и обработки данных в режиме реального времени.

2. Захват данных (Data Ingestion).

От распределённых агентов сбора на сервер поступают потоки сырых данных (строки логов веб-серверов, сетевая телеметрия)

3. Предварительная обработка данных.

Входные данные проходят первичную очистку и нормализацию

4. Извлечение признаков (Feature Engineering).

Для каждого агрегированного потока формируется вектор признаков, необходимый для работы модели:

– вычисление статистических метрик (среднее, дисперсия размера пакета);

– расчёт энтропии URL для выявления DGA‑доменов и туннелирования;

– кодирование категориальных признаков (Label Encoding);

– масштабирование числовых значений (Min‑Max Scaling) для приведения к диапазону.

5. Передача в модуль машинного обучения (AI Core – XGBoost).

Подготовленный вектор признаков подаётся на вход ансамблю решающих деревьев. Модель вычисляет распределение вероятностей принадлежности текущей сессии к одному из известных классов атак (от 0 до 7, согласно таксономии CIC‑IDS2017).

6. Классификация и принятие решения.

Система анализирует выход модели:

– полученная вероятность атаки P(Attack) сравнивается с порогом уверенности τ (Confidence Threshold);

– P(Attack)≥τ, событие классифицируется как инцидент;

– определяется конкретный тип атаки (например, Class 1: HTTP Flood) на основе класса с максимальной вероятностью.

7. Реагирование (Active Response).

В случае подтверждения инцидента автоматически выполняются защитные действия:

– генерация правила блокировки для межсетевого экрана (бан IP‑адреса или подсети);

– отправка управляющей команды на API веб‑сервера для принудительного сброса соединения;

– Включение режима JS‑Challenge (CAPTCHA) для подозрительных клиентов с пограничным уровнем риска.

8. Фиксация инцидента.

Информация об атаке сохраняется для аудита и анализа:

– создаётся запись в таблице инцидентов базы данных PostgreSQL с сохранением всех метаданных (время, тип атаки, источник, уверенность модели);

– сохраняется образец «сырого» запроса или пакета, инициировавшего срабатывание, для последующего изучения.

9. Уведомление и отчетность.

Система информирует персонал о произошедшем инциденте:

– администратор безопасности получает мгновенное уведомление с краткими деталями атаки;

– обновляются показатели на дашбордах мониторинга в реальном времени.

Для выполнения задачи «Обнаружение и классификация сетевых атак» используются различные документы и файлы, которые фиксируют исходные данные (входные документы) и результаты анализа (выходные документы). Эти документы формируют информационную основу для последующей визуализации угроз, регистрации инцидентов и документального подтверждения действий системы защиты.

Первичные входные документы представляют собой машинные и текстовые файлы, содержащие параметры сетевого трафика и настройки безопасности. Эти данные являются исходной информацией для анализа и классификации.

Входные массивы представляют собой структурированные наборы данных (логи и векторы признаков), которые используются для обучения и функционирования модели машинного обучения (XGBoost) в целях определения типа угрозы и её характеристик. Вся входная информация передается в модуль интеллектуального анализа автоматически через внутренние шины данных или обновляется администратором через панель управления.

Выходные массивы формируются в результате работы подсистемы «Интеллектуальный анализ трафика» и представляют собой совокупность структурированных данных о классифицированных сетевых потоках, выявленных атаках и применённых мерах реагирования. Эти данные используются другими подсистемами WebGuard‑AI: модулем уведомлений, базой данных инцидентов, панелью администратора и подсистемой отчётности.

Выходные массивы предназначены для хранения и передачи результатов анализа трафика, формирования уведомлений об атаках и аномалиях, последующего анализа в подсистемах визуализации, а также для пополнения обучающей выборки при дообучении модели машинного обучения. Они обеспечивают трассируемость всех решений системы защиты и позволяют восстанавливать полную картину инцидента.

Нейросетевая модель решения задачи и технологий искусственного интеллекта. Для реализации интеллектуального модуля классификации сетевых атак выбрана математическая модель градиентного бустинга над решающими деревьями, реализуемая алгоритмом XGBoost [2]. Формально задача сводится к нахождению отображения $F: \mathbb{R}^m \to \mathbb{R}^K$, которое сопоставляет вектору признаков сетевого трафика x вектор оценок принадлежности к одному из K классов атак [17].

Пусть задан обучающий набор данных $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^n$, где $x_i \in \mathbb{R}^{78}$ – вектор признаков -го сетевого потока, а $y_i \in \{0, \dots, K-1\}$ – метка класса. Модель предсказания строится как аддитивная композиция из T функций (решающих деревьев):

$$\hat{y}_i = \phi(x_i) = \sum_{t=1}^{T} f_t(x_i), f_t \in \mathcal{F},$$

где $\mathcal{F} = \{f(x) = w_{q(x)}\}$ – пространство регрессионных деревьев, $q: \mathbb{R}^m \to \{1, \dots, L\}$ – структура дерева, сопоставляющая пример листу, $w \in \mathbb{R}^L$ – вектор весов в листьях, L – количество листьев.

Обучение модели заключается в минимизации регуляризированной целевой функции $\mathcal{L}(\phi)$: [5]

$$\mathcal{L}(\phi) = \sum_{i=1}^{n} l(\hat{y}_i, y_i) + \sum_{t=1}^{T} \Omega(f_t),$$

где $l(\hat{y}_i, y_i)$ – дифференцируемая выпуклая функция потерь (в данной задаче используется Multi-class LogLoss), измеряющая разницу между предсказанием и истинной меткой, а $\Omega(f)$ – слагаемое регуляризации, предотвращающее переобучение модели:

$$\Omega(f) = \gamma L + \frac{1}{2}\lambda \|w\|^2,$$

здесь γ – штраф за сложность (количество листьев), а λ – коэффициент L2-регуляризации весов.

Алгоритм обучается итеративно. На каждом шаге t добавляется новое дерево f_t, которое минимизирует аппроксимацию целевой функции, разложенную в ряд Тейлора второго порядка:

$$\mathcal{L}^{(t)} \approx \sum_{i=1}^{n} \left[l(y_i, \hat{y}_i^{(t-1)}) + g_i f_t(x_i) + \frac{1}{2} h_i f_t^2(x_i) \right] + \Omega(f_t),$$

где g_i и h_i – первая и вторая производные функции потерь по предсказанию на предыдущем шаге соответственно:

$$g_i = \partial_{\hat{y}^{(t-1)}} l(y_i, \hat{y}^{(t-1)}), h_i = \partial^2_{\hat{y}^{(t-1)}} l(y_i, \hat{y}^{(t-1)}).$$

Оптимальный вес w_j^* в листе j для фиксированной структуры дерева $q(x)$ вычисляется аналитически по формуле:

$$w_j^* = -\frac{\sum_{i \in I_j} g_i}{\sum_{i \in I_j} h_i + \lambda},$$

где $I_j = \{i \mid q(x_i) = j\}$ – множество индексов обучающих примеров, попавших в лист j. Качество структуры дерева оценивается с помощью функции Gain, которая показывает уменьшение функции потерь при расщеплении узла:

$$Gain = \frac{1}{2}\left[\frac{(\sum_{i \in I_L} g_i)^2}{\sum_{i \in I_L} h_i + \lambda} + \frac{(\sum_{i \in I_R} g_i)^2}{\sum_{i \in I_R} h_i + \lambda} - \frac{(\sum_{i \in I} g_i)^2}{\sum_{i \in I} h_i + \lambda} \right] - \gamma.$$

Поскольку задача классификации требует вероятностного ответа, выход ансамбля (сумма весов) преобразуется в вероятности принадлежности к классам с помощью функции Softmax:

$$P(y = k \mid x) = \frac{e^{\hat{y}_k(x)}}{\sum_{j=0}^{K-1} e^{\hat{y}_j(x)}}.$$

Результирующим классом признается тот, для которого вычисленная вероятность $P(y = k \mid x)$ максимальна. Использование данной математической модели обеспечивает высокую обобщающую способность системы за счет сочетания градиентного спуска и механизмов регуляризации, что позволяет эффективно распознавать различные типы сетевых атак на основе полученных из журналов мониторинга признаков.

Обучение и тестирования нейросетевой модели

Этапы обучения:

- Сбор и объединение исходных датасетов.
- Очистка данных: удаление дубликатов, пустых значений и неинформативных колонок.
- Балансировка классов и нормализация признаков.
- Разделение выборки (80% – обучение, 20% – тест).
- Обучение модели XGBoost с контролем переобучения.
- Проверка качества на тестовой выборке и оценка метрик.

Результаты:

- Accuracy – 97.1%
- Precision – 96.5%
- Recall – 97.3%
- F1-score – 0.967
- False positives – <5%

Наиболее важные признаки: Flow Duration, Total Fwd Packets, Flow Bytes/s, Packet Length Std, Fwd IAT Mean.

На рис. 2 отображено изменение значения многоклассовой логарифмической функции потерь (mlogloss) на обучающей выборке (validation_0) и тестовой выборке (validation_1) по итерациям построения деревьев.

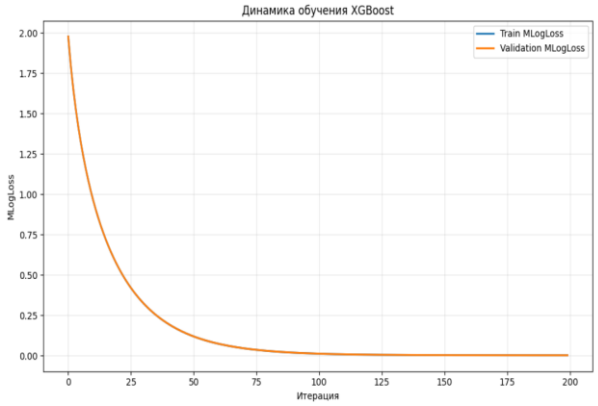

Рис. 2 – Динамика обучения нейронной сети

Fig. 2 – Neural network learning dynamics

Изначально (итерация 0) значение mlogloss составляет около 1.97, что соответствует начальному состоянию модели с почти случайными предсказаниями. К 199-й итерации функция потерь снижается до 0.00092 на train и 0.00118 на test. Монотонное убывание кривых с минимальным разрывом между train и test подтверждает высокое качество обучения, отсутствие переобучения и отличную обобщающую способность модели.

На рис. 3 представлена матрица ошибок.

Матрица ошибок демонстрирует высокую точность модели по всем классам. Диагональные элементы значительно преобладают, что подтверждает правильную классификацию большинства объектов: например, 199 998 из 199 999 для Benign, 40 000 из 40 000 для DDoS и PortScan.

Модель показала устойчивую работу и способность корректно различать различные типы атак с высокой скоростью.

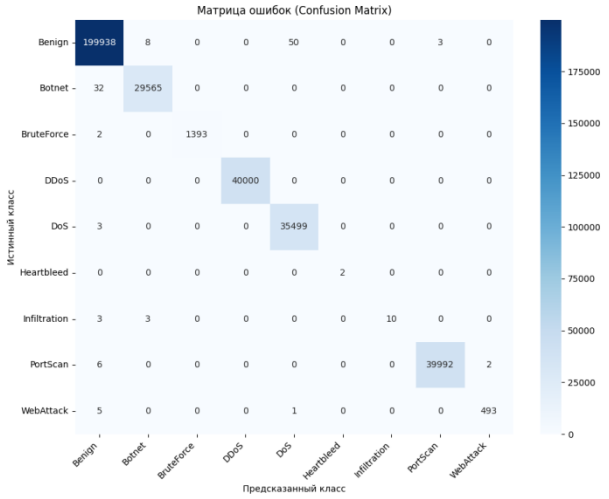

Рис. 3 – Матрица ошибок

Fig. 3 – Confusion matrix

Заключение

Авторами разработан интеллектуальный модуль WebGuard-AI, способный в режиме реального времени классифицировать типы веб-атак на основе анализа сетевого трафика. Благодаря этому процесс диагностики причины сбоя был сокращен с 20-40 минут до 1-2 минут.

К существующему процессу проверки доступности сайтов добавлен этап интеллектуального анализа. Теперь система не только определяет, доступен ли ресурс, но и может выявлять DDoS, брутфорс, SQL-инъекции и другие типы атак

Формализованы этапы жизненного цикла инцидента: обнаружение, классификация, уведомление, реагирование и анализ постфактум. Управление осуществляется с применением ИИ-компонента, который автоматически выставляет приоритеты реагирования в зависимости от типа атаки.

Внедрение моделей машинного обучения позволило минимизировать участие специалистов в рутинных действиях. Система самостоятельно генерирует оповещения, указывает предполагаемые причины инцидента и рекомендует действия для восстановления работоспособности.

При обнаружении атак система автоматически создаёт задачу в CRM, тем самым обеспечивая прозрачность и контроль всех этапов обработки инцидента

Литература

1. А. И. Гетьман, М. Н. Горюнов, А. Г. Мацкевич, Д. А. Рыболовлен, *Труды Института системного программирования РАН*. 5, 33, 83-104 (2021). DOI 10.15514/ISPRAS-2021-33(5).
2. Sharafaldin I., Lashkari A.H., Ghorbani Ali A. In Proc. *of the 4th International Conference on Information Systtms Security and Privacy (ICISSP*), 108-116 (2018).
3. Ring M., Wunderlich S. et al. *Computers & Security*. 86, 147-167 (2019).
4. В. С. Федорова, В. В. Стригунов. *Вестник Тихоокеанского государственного университета.* 2, 73, 71-82 (2024) – DOI 10.38161/1996-3440-2024-2-71-82.
5. М. Н. Горюнов, А. Г. Мацкевич, Д. А. Рыболовлев *Труды Института системного программирования РАН*. – 5, 32, 81-94 (2020)– DOI 10.15514/ISPRAS-2020-32(5)-6.
6. Kanimozhi V., Jacob T.P. *CSE-CIC-IDS2018 using cloud computing. ICT Express*, 5, 3, 211-214 (2019).
7. А. М. Вульфин, В. И. Васильев, С. А. Мандовен *Системная инженерия и информационные технологии*. – 1(10), 7, 105-112 (2025) – DOI 10.54708/2658-5014-SIIT-2025-no1-p105.
8. Болдырихин Н. В., Комоцкий Р. И., Лян Д. И. *Молодой ученый*. 2, 6-9 (2023) .
9. *Кучкарова Н. В. Системная инженерия и информационные технологии*.2(17), 6, 50-65 (2024) .
10. Васильев В. И., Картак В. М. *Системная инженерия и информационные технологии*.2(4), 2, 43-50 (2020).
11. А.В. Каляшина, Ю.Н. Смирнов *Вестник Технологического университета,* 27, 6, 84-89 (2024) – DOI 10.55421/1998-7072_2024_27_6_84.
12. Кириллова А. Д. *Системная инженерия и информационные технологии*.4(13), 5, 77-93 (2023).
13. А. О. Кострикина, К. А. Лазунин. *Проблемы научной мысли*.1, 4, 82-85 (2024).
14. Н. Г. Пархоменко, Б. М. Боташев, П. М. Колобанов Е. С. Григоренко. *Известия ТРТУ*. 4(33). 325-327 (2003).
15. Ю. С. Капусто, О. В. Носов. *Экономика и социум*. 5(48). 538-541 (2018) .
16. V.V. Rykova. *International Journal of Advanced Studies*.3, 10 18-28 (2020) – DOI 10.12731/2227-930X-2020-3-18-29.
17. S. B. Rajasekaran. International Journal of Intelligent Systems and Applications in Engineering. 1, 11, 179-182 (2023) .

References

1. A. I. Getman, M. N. Goryunov, A. G. Matskevich, D. A. Rybolovlen, *Proceedings of the Institute of System Programming RAS*. 5, 33, 83-104 (2021). DOI 10.15514/ISPRAS-2021-33(5)
2. Sharafaldin I., Lashkari A.H., Ghorbani Ali A. *In Proc. of the 4th International Conference on Information Systtms Security and Privacy (ICISSP)*, 108-116 (2018).
3 Ring M., Wunderlich S. et al. *Computers & Security*. 86, 147-167 (2019)
4. V. S. Fedorova, V. V. Strigunov. *Bulletin of Pacific National University*. 2, 73, 71-82 (2024) – DOI 10.38161/1996-3440-2024-2-71-82.
5. M. N. Goryunov, A. G. Matskevich, D. A. Rybolovlev *Proceedings of the Institute of System Programming RAS*. – 5, 32, 81-94 (2020)– DOI 10.15514/ISPRAS-2020-32(5)-6
6. Kanimozhi V., Jacob T.P. *CSE-CIC-IDS2018 using cloud computing. ICT Expres*s, 5, 3, 211-214 (2019).
7. A. M. Vulfin, V. I. Vasiliev, S. A. Mandoven: *Systems Engineering and Information Technologies*. – 1(10), 7, 105-112 (2025) – DOI 10.54708/2658-5014-SIIT-2025-no1-p105.
8. Boldyrikhin N. V., Komotsky R. I., Lyan D. I. *Young Scientist*. 2, 6-9 (2023)
9. Kuchkarova N. V. *Systems Engineering and Information Technologie*s.2(17), 6, 50-65 (2024)
10. Vasiliev V. I., Kartak V. M. *Systems Engineering and Information Technologie*s.2(4), 2, 43-50 (2020)
11. A.V. Kalyashina, Yu.N. Smirnov *Herald of Technological University*, 27, 6, 84-89 (2024) – DOI 10.55421/1998-7072_2024_27_6_84
12. Kirillova A. D. *Systems Engineering and Information Technologies*.4(13), 5, 77-93 (2023)

13. A. O. Kostrikina, K. A. Lazunin. *Problems of Scientific Though*t.1, 4, 82-85 (2024)
14. N. G. Parkhomenko, B. M. Botashev, P. M. Kolobanov E. S. Grigorenko. *Izvestiya TRTU*. 4(33). 325-327 (2003)
15. Yu. S. Kapusto, O. V. Nosov. *Economy and Society*. 5(48). 538-541 (2018)
16. V.V. Rykova. *International Journal of Advanced Studies.*3, 10 18-28 (2020) – DOI 10.12731/2227-930X-2020-3-18-29.
17. S. B. Rajasekaran. *International Journal of Intelligent Systems and Applications in Engineerin*g. 1, 11, 179-182 (2023)

© **А. В. Каляшина** – канд. техн. наук, доцент кафедры Лазерных и аддитивных технологий, Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань, Россия, anna_vik@mail.ru; **Ю. Н. Смирнов** – кандидат физико-математических наук, доцент, заведующий кафедрой «Цифровые системы и модели», Казанский государственный энергетический университет, Казань, Россия, mmite@inbox.ru.

© **A. V. Kalyashina** – PhD (Technical Sci.), Associate Professor of the Department of Laser and Additive Technologies, Kazan National Research Technical University named after A. N. Tupolev, Kazan, Russia, anna_vik@mail.ru; **Yu. N. Smirnov** - PhD (Physical and Mathematical Sci.), Head of the Department of Digital Systems and Models, Kazan State Power Engineering University, Kazan, Russia, mmite@inbox.ru.

Дата поступления рукописи в редакцию – 05.09.26.
Дата принятия рукописи в печать – 19.09.26.