УДК 004.8:004.056

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ ОРГАНИЗАЦИИ

С.Г. Михайловский

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Нарушители в настоящее время используют искусственный интеллект (ИИ) для автоматизации и улучшения кибератак на информационные системы организаций. ИИ сканирует системы, находит уязвимости и реализует кибератаки. Он помогает нарушителям без особых усилий получать данные, взламывать учетные записи и распространять вредоносное ПО. Машинное обучение (МО) и ИИ помогает нарушителям усовершенствовать свои методы, обойти защиту и имитировать обычное поведение пользователей. В статье раскрывается использование искусственного интеллекта, машинного обучения в обнаружении распределенных кибератаках типа DDoS (Distributed Denial of Service).

Ключевые слова: искусственный интеллект; платформы безопасности; байесовский алгоритм; DDoS-атака; машинное обучение; система обнаружения, модель обнаружения.

USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TO DETECT ATTACKS ON AN ORGANIZATION'S INFORMATION SYSTEM

S.G. Mikhailovsky

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Violators are currently using artificial intelligence (AI) to automate and improve cyber attacks on organizations' information systems. AI scans the system, finds vulnerabilities and implements cyber attacks. It helps violators effortlessly obtain data, hack accounts, and distribute malware. Machine learning (MO) and AI help violators improve their methods, bypass security, and mimic normal user behavior. The article reveals the

use of artificial intelligence and machine learning in detecting distributed cyber attacks such as DDoS (Distributed Denial of Service).
Keywords: artificial intelligence; security platforms; Bayesian algorithm; DDoS attack; machine learning; detection system. detection model.

Введение

DDoS – это вид кибератаки, при которой нарушители используют множество распределенных ресурсов для нанесения ущерба целевым объектам, что приводит к недоступности услуг для легитимных пользователей. Основными целями таких кибератак являются информационные системы организаций, пропускная способность сетей и другие критически важные ресурсы. DDoS-атаки считаются одними из самых распространенных и разрушительных кибератак, могут характеризоваться большим объемом трафика за короткий период времени, небольшим объемом трафика на протяжении длительного времени или значительным объемом трафика на протяжении длительного времени, и их сложно обнаружить, так как трафик, создаваемый во время атаки, часто не отличается от обычного сетевого трафика. В связи с развитием облачных вычислений, Интернета вещей (IoT) и технологий искусственного интеллекта DDoS-атаки продолжают эволюционировать, что делает их обнаружение и предотвращение все более сложной задачей, в том числе из-за невозможности отличить реальный траффик от нелегитимного. Методы классификации с помощью машинного обучения могут быть использованы для различения разных видов пакетов. Пакеты, классифицированные как атакующий трафик, будут отброшены. Некоторые признаки, позволяющие обнаружить DDoS-атаку, включают количество пакетов, средний размер пакета, разницу во временном интервале, разницу в размере пакета, количество байт, скорость передачи пакетов и битрейт.

Применение искусственного интеллекта для предотвращения DDoS-атак

Основные методы ИИ включают машинное обучение, распознавание речи и обработку естественного языка. Алгоритмы МО используются для обнаружения DDoS-атак и защиты от них, с акцентом на обнаружение аномалий. Основные методы включают байесовские алгоритмы, нейронные сети и машины опорных векторов для классификации и регрессии.

ИИ и МО применяются для обнаружения кибератак, используя подходы глубокого обучения, как показано на рисунке 1. Обнаружение DDoS-атак решает задачу классификации последовательностей, преобразуя обнаружение пакетов в обнаружение окон [1]. Подход включает CNN (Convolutional Neural Network), RNN (Recurrent Neural Network) и полностью связанные слои, причем RNN изучает объекты на входе от CNN.

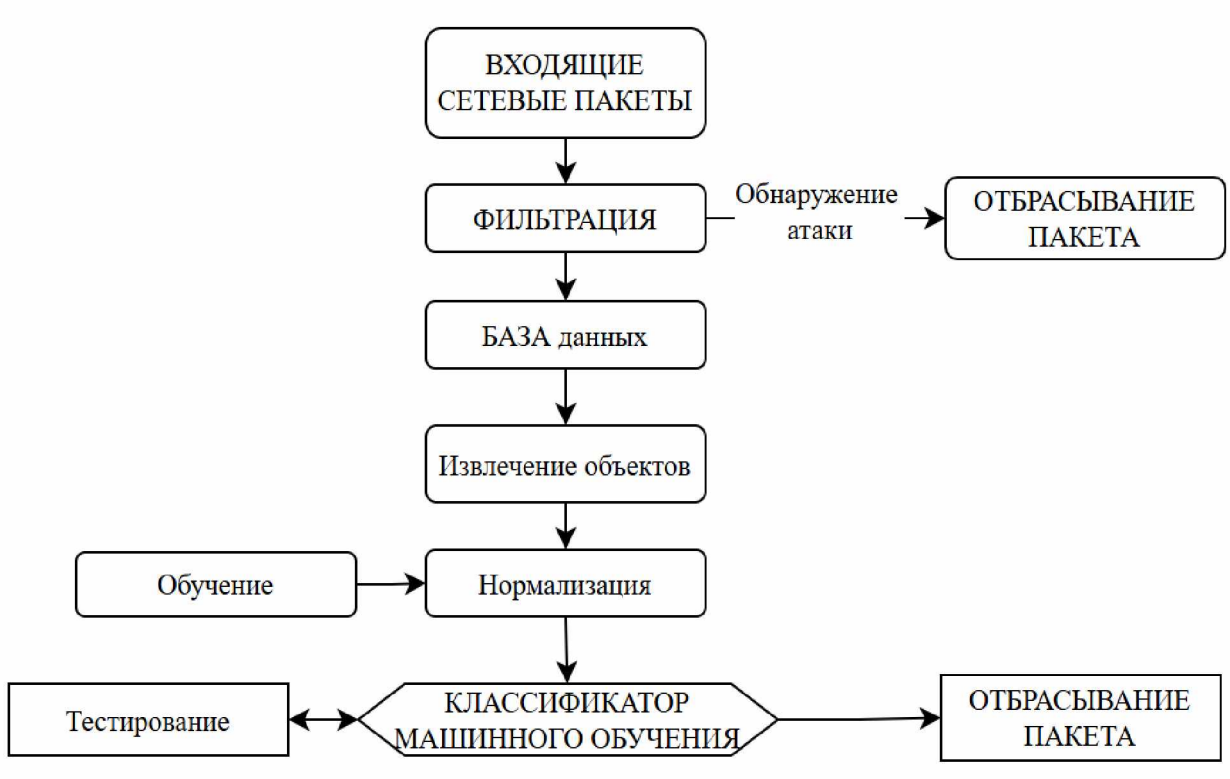

Рис. 1. Архитектура обнаружения DDoS-атак на основе машинного обучения
Fig. 1. DDoS attack detection architecture based on machine learning

На рис. 2 представлено обучение глубоких нейронных сетей с улучшенной устойчивостью к атакам – Deep Defense, представленной в одноименной научной работе, используя LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit) для масштабирования и отслеживания истории пакетов, при этом RNN превосходят random forest, как метод МО в обобщении [3].

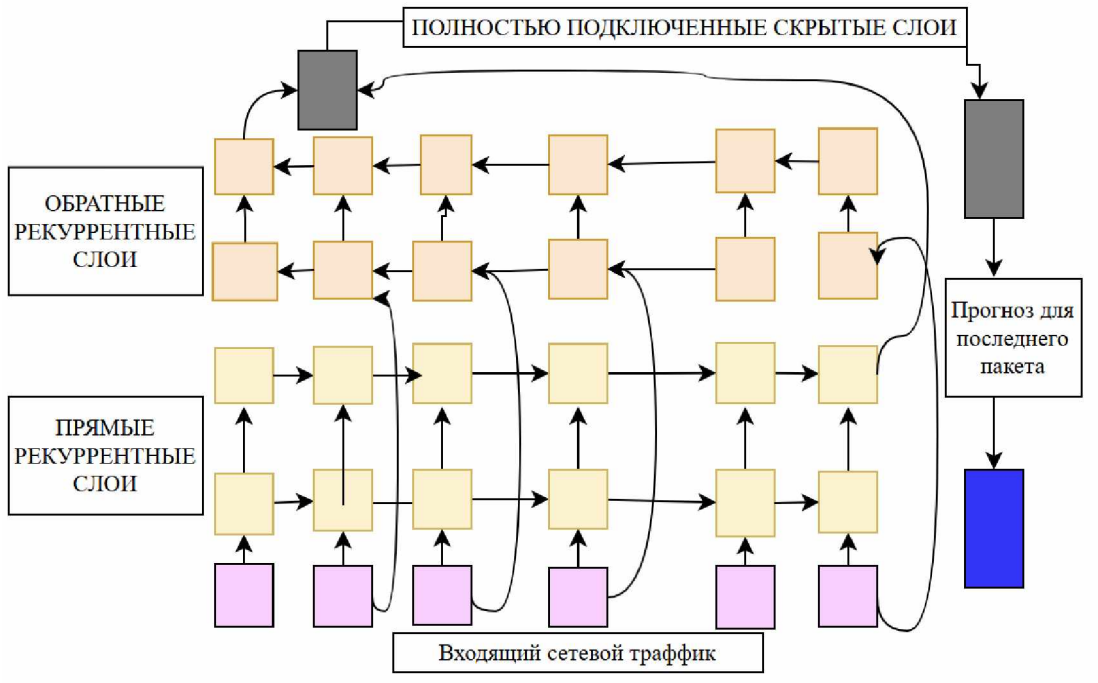

Рис. 2. Общая сетевая архитектура для Deep Defense
Fig. 2. Common network architecture for Deep Defense

Предполагается, что существует более продвинутый подход, в основе которого обнаружение DDoS-атак на основе нейронной сети, состоящая из пяти фазного сборщика пакетов, Hadoop HDFS (Hadoop HDFS (Hadoop Distributed File System, распределенной файловой системы, разработанная для хранения больших объемов данных), конвертера форматов, процессора обработки данных и модуля обнаружения нейронной сети [3].

На рис. 3 отражена архитектура, представляющая систему обнаружения, которая интегрирована с нейронной сетью для обнаружения DDoS-атак по семи параметрам. Система обнаружения может анализировать высокоскоростной и объемный сетевой трафик, а нейронная сеть может эффективно идентифицировать характеристики пакетов [2].

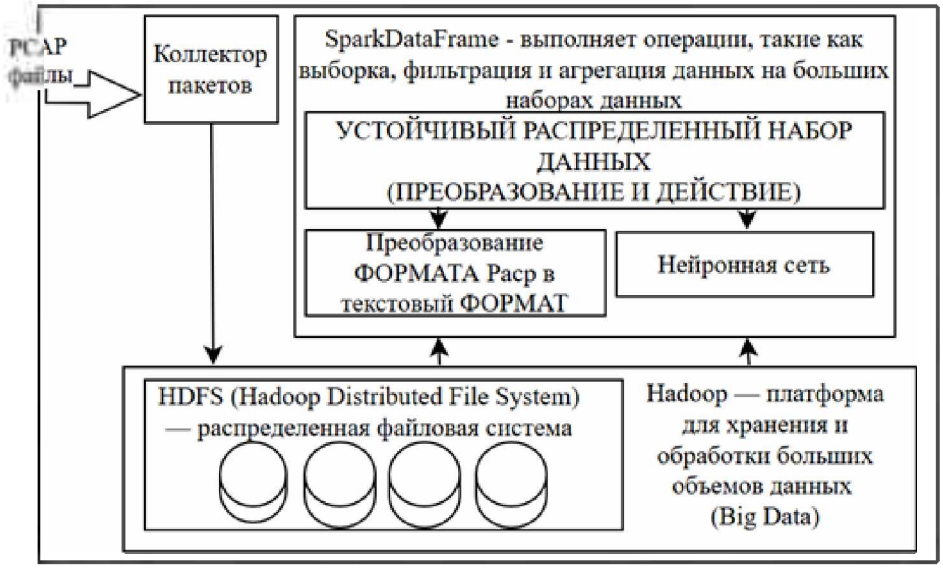

Рис. 3. Архитектура системы обнаружения
Fig. 3. Architecture of the detection system

В настоящее время предлагается более продвинутая концепция машинного обучения для противостояния к подобным кибератакам, в основе которой предположение, что все узлы модели обладают способностью к независимому обучению. Хорошо известный алгоритм кумулятивной суммы используется для обнаружения огромного объема трафика. Для распознавания структуры обычного трафика используются классификаторы и детекторы, такие как байесовский (Naive Bayes) алгоритм [2]. Каждый узел имеет алгоритм, который сравнивает накопленную сумму средних значений за каждую единицу времени с характерным пороговым значением для классификации сообщения. Этот механизм может остановить и избежать DDoS-атаки на ранней их стадии.

Одной из основных моделей обнаружения и смягчения последствий DDoS-атак может быть модель, использующая алгоритм машинного обучения, указанная на рис. 4.

Модель состоит из системы онлайн-мониторинга OMS (Online Monitoring System), модуля обнаружения мошеннического трафика и алгоритма ограничения скорости на основе интерфейса. OMS использует автоматизированные инструменты и скрипты для мониторинга ухудшения качества и предоставления измерений воздействия DDoS. Модуль обнаружения ложного трафика включает алгоритм проверки количества переходов для проверки подлинности входящего пакета. Он создает легитимные записи с указанием IP и количества переходов для обнаружения потенциальных кибератак. Алгоритм проверки количества переходов заключается

в проверке подлинности пакета. HCF-SVM (Hop Count Filtering – Support Vector Machine) обучается и обновляется с учетом IP-адреса источника и соответствующего количества переходов [2].

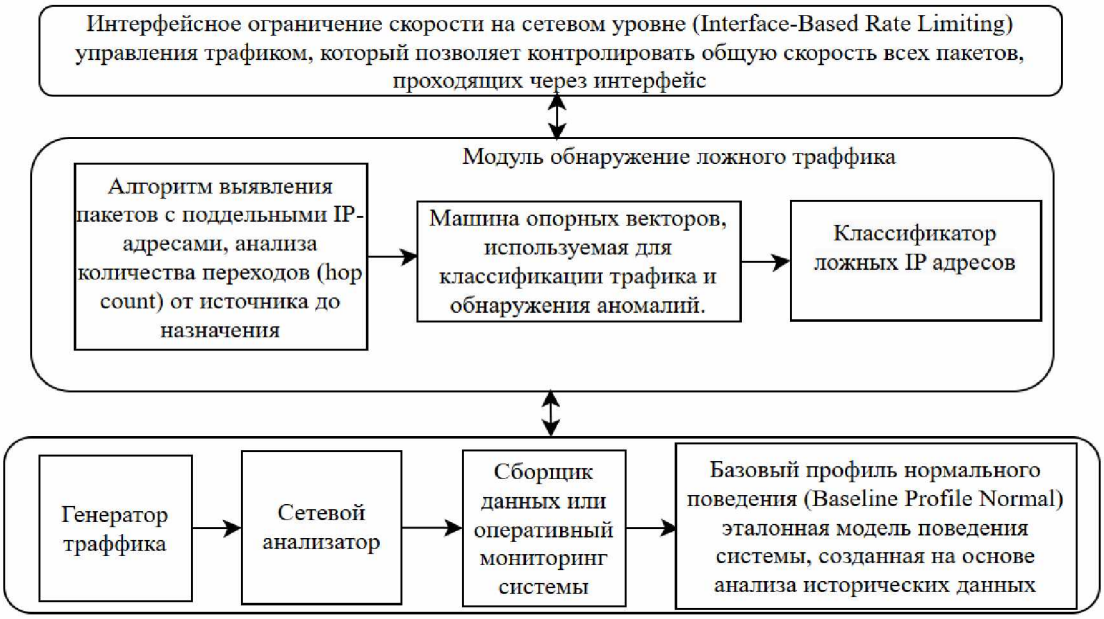

Рис. 4. Моделей обнаружения и смягчения последствий DDoS-атак
Fig. 4. DoS attack detection and mitigation models

Существуют и другие подходы обнаружения DDoS-атак, основанные на машинном обучении и применении ИИ:

1. Система обнаружения DDoS-атак на основе нейронной сети и внедряет в кластер Apache Hadoop и систему HBase. Система имеет архитектуру нейросети, которая обладает способностью адаптироваться к новым типам DDoS-атак. Кластер Hadoop и HBase настроен на обработку огромного трафика, затем нейросетевая модель разработана для обнаружения DDoS-атак;

2. Модель системы на основе ANN (Artificial Neural Network) и статистической информации заголовка пакета для обнаружения DDoS-атаки с усилением DNS [3]. Они классифицируют DNS-трафик с использованием алгоритмов классификации МО, включая дерево решений, многоуровневое восприятие MLP (Multi-Layer Perception), байесовский алгоритм и SVM (Support Vector Machine) метод машинного обучения, который используется для классификации и регрессии данных. Затем осуществляется отбор дерева решений в качестве модели классификации МО для достижения наилучшей эффективности;

3. Система, основанная на простой сетевой архитектуре, которая использует реальный веб-сервер, сервер-приманку и веб-серверы-приманки для отличия трафика DDoS от обычного трафика. В архитектуре используется настроенная система предотвращения вторжений на сетевом шлюзе, которая использует правила, генерируемые случайным деревом алгоритм машинного обучения посредством контролируемого обучения. Дерево решений выбирается для целей выделения вредоносного трафика из нормального трафика. Случайное дерево алгоритма машинного обучения с использованием, маркированного наборов данных, используется для целей минимизации риска формирования ложного положительных трафика.

Заключение

DDoS-атаки по-прежнему остаются существенными угрозами для организаций и людей и могут принести большие убытки. Некоторые методы использования ИИ, такие как алгоритмы МО, могут использоваться для классификации трафика DDoS-атак и обнаружения DDoS-атак, важен в этом вопросе прогресс в обнаружении DDoS-атак с использованием методов МО и ИИ, которые обладают возможностями их обнаружения.

Список использованных источников

1. Воробьева Ю.Н. (2018) Нейросетевая модель выявления DDOS-атак. *Вестник технологического университета*. 21 (2). 94-98.

2. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. (2016) Обнаружение вторжений в компьютерные сети (сетевые аномалии). Москва. Горячая линия-Телеком.

3. Аль-тамими Мохалад Мохсин Абдульхасан. Алзагир Аббас Али Хасан (2024) Повышение сетевой безопасности с помощью подхода глубокого обучения RNN. *Вычислительные нанотехнологии*. 11 (4). 114-122.

References

1. Vorobyeva Yu.N. (2018) Neural network model for detecting DDOS attacks. Bulletin of the Technological University. 21 (2). 94-98.

2. Shelukhin O.I., Sakalema D.J., Filinova A.S. (2016) Intrusion detection in computer networks (network anomalies). Moscow. Hotline-Telecom.

3. Al-tamimi Mohammad Mohsin Abdel Hassan. Alagir Abbas Ali Hassan (2024) Improving network security through the RNN deep learning approach. Computational Nanotechnology. 11 (4). 114-122.

Сведения об авторе

Михайловский С.Г., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mikhailouski@mikhailouski.ru.

Information about the author

Mikhailovsky S.G., Master's student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mikhailouski@mikhailouski.ru.