ГИБРИДНЫЕ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И АНАЛИЗ СЕТЕВОГО ТРАФИКА ДЛЯ ПРОТИВОДЕЙСТВИЯ СОВРЕМЕННЫМ УГРОЗАМ

Лукьянец Софья Евгеньевна, студент
E-mail: marlagastrolerha@gmail.com

Донской государственный технический университет
г. Ростов-на-Дону, РФ

Аннотация. В данной статье подробно анализируются гибридные системы защиты сетевого трафика, которые сочетают в себе традиционные подходы к обеспечению безопасности, такие как настройка межсетевых экранов и современные методы, основанные на искусственном интеллекте. Рассматриваются наиболее распространенные виды угроз, которые можно встретить при работе с сетевым трафиком, включая атаки типа *DDoS*, *SQL*-инъекции и *Zero-day* атаки. Была предложена архитектура гибридной системы, использующая кроссплатформенные инструменты, такие как *Wireshark* и *Suricata*, для обеспечения лучшей совместимости с большим спектром операционных систем, таких как *Windows*, *Linux* и др. В рамках данной архитектуры представлена оценочная система, использующая различные метрики для оценки эффективности защиты, которые применяются в исследованиях киберсистем, например, точность и время реагирования. Статья подчеркивает важность интеграции традиционных методов и искусственного интеллекта для создания более стойких и надежных решений для защиты сетевого трафика при условии постоянного роста количества и сложности киберугроз. Данная работа может представлять интерес для системных администраторов, инженеров сетевой безопасности и исследователей, стремящихся повысить надежность сетей и усовершенствовать уже существующие решения.

Ключевые слова. Гибридные системы, сетевая безопасность, искусственный интеллект, сигнатурный анализ, киберугрозы.

Введение

В нынешнее время информационные технологии подвержены высокому количеству кибератак, сложность которых возрастает с каждым днем. Традиционные подходы не всегда могут справиться с адаптивными кибератаками, что приводит к утечкам данных, выводу из строя оборудования и финансовым потерям. В связи в этим необходима эффективная защита, которая сможет обеспечить комплексный подход, включающий в себя традиционные методы защиты и методы, только получившие развитие в этой сфере.

Актуальность данной темы обусловлена стремительным ростом киберугроз, которые наносят значительный ущерб корпоративным сетям, из-за чего появляется потребность в новых методах борьбы с ними [4].

Целью данной работы является реализация архитектуры гибридной системы, основанной на сигнатурном анализе с использованием искусственного интеллекта, а также оценочная система для анализа эффективности использования данных систем.

Основная часть

Среди современных угроз сетевой безопасности можно выделить самые популярные и вредоносные атаки такие как: *DDoS*-атаки, *SQL*-инъекции, *Zero-day* атаки. Данные угрозы чаще всего сочетают в себе несколько методов и имеют высокую адаптивность к мерам противодействия [4].

Перед рассмотрением мер защиты стоит разобрать некоторые конкретные угрозы. *Zero-day* атаки – эксплуатация ранее неизвестных уязвимостей в программном обеспечении [2]. *DDoS*-атаки нацелены на отказ функционирования системы, за счет перегрузки нелеги-

тимным трафиком. Они могут быть нацелены либо на всю инфраструктуру, либо на отдельные каналы. Существует классификация *DDoS*-атак по модели *OSI* по механизму воздействия, по протоколам [4].

SQL-инъекции – это уязвимости, которые позволяют с помощью фрагментированного вредоносного кода получать сведения из баз данных. Среди атак, связанных с *SQL*-инъекциями, различают: числовые, строковые, слепые, *out-of-band, second-order* [2].

Для предотвращения данных атак и других киберугроз, связанных с сетевым трафиком, необходимы соответствующие методы. Существуют проверенные технические меры, которые рекомендовано использовать, например, настройка межсетевых экранов, а также организационные методы, такие как обновление политик [1]. Совокупность данных методов имеет большую эффективность, однако они не всегда могут обеспечить защиту от новых угроз. В связи с этим возникает потребность в использовании новых подходов, таких как интеграция искусственного интеллекта с существующими системами защиты. Комбинация традиционных методов и ИИ позволяет создавать гибридные системы, которые будут использовать уже проверенные механизмы и при этом адаптироваться к новым видам атак, что является перспективным решением для защиты сетевого трафика [4].

Гибридные системы уже описывались в других работах и применяются в настоящем время. Они отличаются друг от друга в зависимости от целей и методов, использованных в них [3].

Учитывая актуальность кроссплатформенных инструментов для обеспечения возможности работы системы на разных операционных системах при построении собственного решения было решено использовать следующие элементы:

1. Сбор данных. Для него используются инструменты фиксации сетевого трафика, например, *Wireshark, Tcpdump, Zeek*. Данные можно сохранять в хранилищах для дальнейшего анализа, например, *Elasticsearch* [1].
2. Сигнатурный анализ. Для проверки трафика на известные угрозы можно использовать *Suricata*. Эта система использует базы правил для нахождения атак [2].
3. Анализ искусственным интеллектом. Использование *LSTM*, реализованное через библиотеку *TensorFlow*, позволяет выявлять аномалии [5].
4. Система реагирования. Для известных угроз *Suricata* блокирует трафик через *API* межсетевых экранов, например, *Nftables*. Для системы оповещения можно использовать *SIEM* систему – *Graylog* [1].
5. Обновление баз сигнатур. Для переобучения модели необходимо обновлять данные. Это реализуется не только автоматически в ходе работы, но вручную, используя открытые источники, например, *MITREATT&CK* и БДУ ФСТЭК [5].



Рис. 1. Схема работы архитектуры

На данной схеме, представленной на рис. 1, трафик поступает в блок сбора данных, после чего фиксирует пакеты и сохраняет их в хранилище. Далее идет параллельная обработка данных. В блоке сигнатурного анализа проверяется трафик на известные угрозы по сигнатурам, а в блоке ИИ анализа происходит поиск аномалий. Результаты объединяются, уже известные угрозы блокируются, а при обнаружении аномалий происходит оповещение администратора. Модель обучается на основе новых данных, после этого система обновляется.

Для проверки эффективности работы гибридной системы предлагается модель оценки, разработанная для данной архитектуры. Она включает в себя следующие метрики, которые применяются в исследованиях кибербезопасности:

1. Точность обнаружения.
2. Время реагирования.
3. Процент ложных срабатываний.
4. Количество снижения инцидентов.

Таблица 1

Метрики оценочной системы

Метрика	Отлично (20–25)	Хорошо (15–19)	Удовлетворительно (6–14)	Плохо (0–5)
Точность	85–100 %	75–84 %	60–74 %	< 60 %
Время реагирования	< 3 с	3–10 с	10–40 с	> 40 с
Ложные срабатывания	< 5%	6–15 %	16–25 %	>25 %
Снижение инцидентов	> 50 %	35–50 %	20–34 %	<20 %

Таким образом максимальной суммой баллов будет являться значение 100. Система, у которой будет больше 80 баллов, будет считаться высокоэффективной, 60–79 – эффективной, 35–59 – удовлетворительной и меньше 40 баллов – неэффективной.

Отметим, что несмотря на преимущества гибридных систем, они не могут обеспечить идеальную защиту, т. к. невозможно обнаружить все уязвимости в системе, всегда остается вероятность ошибок [3].

В рамках данной статьи рассмотрены гибридные системы, которые сочетают в себе традиционные методы защиты трафика и искусственный интеллект. Предложена архитектура, которая основана на кроссплатформенных приложениях. Она имеет большой потенциал в развитии защиты сетевого трафика из-за сочетания сигнатурного анализа с искусственным интеллектом. В рамках реализованной архитектуры рассматривается оценочная система, включающая метрики: точность, время реагирования, ложные срабатывания и снижение инцидентов, что поможет в дальнейшем усовершенствовать архитектуру гибридной системы для защиты сетевого трафика и повысить эффективность системы.

Библиографический список

1. Борисовская, О. В. Мониторинг и классификация сетевого трафика в целях обнаружения и предотвращения нагрузочных сетевых атак / О. В. Борисовская, А. А. Борисовская, Д. В. Маяков // Инновации и инвестиции. – 2023. – № 9. – С. 186–190.

2. Бутырский, И. Ф. Кибератаки на сайты организаций, сигнатурный анализ этих атак и противодействие им / И. Ф. Бутырский, Н. В. Петрищев // Электронный журнал: наука, техника и образование. – 2023. – № S1(41). – С. 32–41.

3. Гибридная интеллектуальная система обнаружения атак на основе комбинации методов машинного обучения / В. И. Васильев, А. М. Вульфин, В. Е. Гвоздев, Р. Р. Шамсутдинов // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9, № 3(34).

4. Ермак, К. К. Методы защиты от кибератак: современные подходы и технологии / К. К. Ермак // Международный студенческий научный вестник. – 2025. – № 1. – С. 4.

5. Спиридонов, В. А. Технология анализа сетевого трафика и автоматической оптимизации на основе искусственного интеллекта / В. А. Спиридонов // Экономика и качество систем связи. – 2022. – № 3(25). – С. 81–88.