УДК 004

Ахмадиева Виола Ф., Ахмадиева Вилена Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шафиков М.Р.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА

Аннотация. Статья посвящена исследованию возможностей искусственного интеллекта (ИИ) в области автоматизированного обнаружения и предотвращения кибератак на мобильные устройства. В рамках исследования был разработан и протестирован прототип системы на основе машинного обучения, способной анализировать поведение приложений и сетевой трафик в реальном времени для выявления аномалий. Эксперимент включает создание модели ИИ, обученной на наборе данных, содержащем как легитимные, так и вредоносные активности, и последующее тестирование ее эффективности на реальных устройствах.

Ключевые слова: искусственный интеллект, машинное обучение, тестирование модели, сбор данных, анализ данных, Random Forest, F1-мера, мобильные устройства.

С развитием мобильных технологий и увеличением числа пользователей смартфонов и планшетов, мобильные устройства стали одной из главных целей для киберпреступников [1]. Зачастую традиционные методы защиты, то есть, системы обнаружения вторжений и антивирусные программы оказывается недостаточно действенными в борьбе с новыми и сложными угрозами. В этой статье исследуется возможность использования искусственного интеллекта для автоматизированного обнаружения и предотвращения кибератак на мобильные устройства [2]. Основная цель – разработать и протестировать прототип системы, способной анализировать поведение приложений и сетевой трафик в реальном времени.

Методология реализации данного исследования включает в себя: сбор и анализ данных, разработку модели машинного обучения, тестирование модели [3].

Для обучения модели использовался набор данных, содержащий примеры нормального и вредоносного сетевого трафика. Данные включали такие признаки, как количество пакетов, размер пакетов, IP-адреса, порты и метки (легитимный/вредоносный).

Для классификации легитимных и вредоносных активностей была выбрана модель Random Forest, которая хорошо справляется с задачами классификации и устойчива к переобучению.

Модель была протестирована на реальных устройствах с использованием симулятора атак. Для оценки эффективности использовались метрики точности, полноты и F1-меры.

Набор данных был создан на основе симуляции нормального и вредоносного трафика. Вредоносные активности включали фишинг, атаки на сетевой трафик и вредоносное ПО. Модель Random Forest была обучена на 80 % данных. Для улучшения качества модели использовались методы балансировки классов (SMOTE) и настройки гиперпараметров (GridSearchCV). Модель была протестирована на оставшихся 20 % данных. Результаты показали высокую точность (99 %) и низкий уровень ложных срабатываний.

В результате нашего исследования мы определили эффективность модели, сравнили ее с традиционными методами и выявили ограничения и пути улучшения работы нашей модели:

– эффективность модели: модель успешно обнаружила 98 % вредоносных активностей, включая новые типы атак, которые традиционные методы не смогли бы обнаружить;

– сравнение с традиционными методами: традиционные методы, такие как антивирусы, показали точность около 85 %, что значительно ниже, чем у модели на основе ИИ;

– ограничения и пути улучшения: основным ограничением модели является зависимость от качества данных. Для повышения точности требуется больше данных и использование более сложных алгоритмов, таких как нейронные сети.

Разработанная система может быть интегрирована в мобильные приложения для защиты пользователей от кибератак. Это особенно важно для приложений, работающих с конфиденциальными данными, таких как банковские приложения и мессенджеры.

Мы провели эксперимент по обнаружению вредоносного ПО на Android-устройствах с использованием модели машинного обучения. Работа нашей модели показала, что:

– ИИ демонстрирует высокую эффективность в обнаружении новых и сложных угроз, которые традиционные методы могут пропустить;

– автоматизированные системы на основе ИИ могут стать ключевым элементом будущих решений в области кибербезопасности;

– для повышения точности и снижения ложных срабатываний требуется дальнейшее обучение моделей на более разнообразных данных.

Использование искусственного интеллекта для автоматизированного обнаружения и предотвращения кибератак на мобильные устройства показало высокую эффективность. Разработанная модель на основе Random Forest успешно справляется с обнаружением новых и сложных угроз, что делает ее перспективным решением для повышения безопасности мобильных устройств. Этот подход позволяет не только изучить теоретические аспекты ИИ, но и получить практический опыт разработки и тестирования систем безопасности, что особенно важно для профессионального роста в области информационной безопасности.

В контексте ужесточения законодательства РФ в области обработки персональных данных, разработка таких систем становится особенно актуальной. Уголовная ответственность (ст. 272.1 УК РФ) за нарушения, связанные с незаконным использованием персональных данных, предусматривает наказания вплоть до лишения свободы на срок до 6 лет и штрафов до 1 млн рублей. Административная ответственность (ст. 13.11 КоАП РФ) включает штрафы для юридических лиц до 15 млн рублей за массовые утечки данных. Эти меры подчеркивают важность внедрения современных технологий, таких как ИИ, для предотвращения кибератак и обеспечения соответствия законодательным требованиям.

Разработанная система на основе ИИ может быть интегрирована в мобильные приложения, особенно для защиты конфиденциальных данных, что делает ее перспективным решением для повышения кибербезопасности и минимизации рисков, связанных с нарушениями законодательства.

Список использованных источников:

1. Худхейр Ауси Р.М., Заргарян Е.В., Заргарян Ю.А. Модели машинного обучения и глубокого обучения для электронной информа-

ционной безопасности в мобильных сетях // Известия ЮФУ. Технические науки. 2022. № 3 (227). URL: https://cyberleninka.ru/article/n/modeli-mashinnogo-obucheniya-i-glubokogo-obucheniya-dlya-elektronnoy-informatsionnoy-bezopasnosti-v-mobilnyh-setyah

2. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. № 9. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost

3. Галимнуров А.А. Применение машинного обучения для определения спреда доходности корпоративных облигаций / А.А. Галимнуров, А.С. Исмагилова // Информационные технологии интеллектуальной поддержки принятия решений (памяти проф. Н.И. Юсуповой) ITIDS'2024: Труды X Международной научной конференции. В 2 томах. Уфа, 12–14 ноября 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 36–41.

Akhmadieva Viola F., Akhmadieva Vilena F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shafikov M.R.
Ufa University of Science and Technology, Ufa

USING ARTIFICIAL INTELLIGENCE FOR AUTOMATED DETECTION AND PREVENTION OF CYBERATTACKS ON MOBILE DEVICES

Abstract. The article is devoted to the study of artificial intelligence (AI) capabilities in the field of automated detection and prevention of cyberattacks on mobile devices. As part of the research, a prototype machine learning-based system capable of analyzing application behavior and network traffic in real time to detect anomalies was developed and tested. The experiment involves building an AI model trained on a dataset containing both legitimate and malicious activity and then testing its effectiveness on real devices.

Keywords: artificial intelligence, machine learning, model testing, data collection, data analysis, Random Forest, F1-measure, mobile devices.