УДК 004.8

Шушакова А.А.
Уфимский университет науки и технологий, Уфа

Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

НЕКОТОРЫЕ НОВЫЕ ВИДЫ АТАК НА МОБИЛЬНЫЕ И IOT-УСТРОЙСТВА С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ И ПРОТИВОДЕЙСТВИЕ ИМ

Аннотация. В статье рассматриваются некоторые новые виды атак на мобильные и IoT-устройства с использованием технологии машинного обучения и способы противодействия.

Ключевые слова: информация, кибератаки на мобильные устройства, машинное обучение в информационной безопасности, IoT-устройства.

Мобильные устройства оказались привлекательной целью для атак как непосредственно на эти устройства, так и на инфраструктуру, с которой они взаимодействуют. По мере развития интеграции технологий искусственного интеллекта с мобильной электроникой (например, т. н. периферийный ИИ) для злоумышленников открываются новые возможности, а для специалистов по защите информации растет сложность управления безопасностью. Помимо ставших уже традиционными атак на мобильные устройства с помощью вредоносного ПО, социальной инженерии и фишинга, киберпреступники стали применять инновационные подходы с использованием технологий машинного обучения, такие как создание персонализированных видео-, аудио- и фото-дипфейков для обмана пользователей [1]. Голосовые ассистенты мобильных устройств и системы распознавания речи становятся уязвимыми, позволяя злоумышленникам подменять голоса легальных пользователей, чтобы получить доступ [2] к личной информации пользователя.

Согласно данным исследования McAfee (компании по разработке антивирусного ПО), проведенного в 2024 г. среди 7000 респондентов, каждый четвертый сталкивался с использованием голосовых дипфейков или знает людей, которые столкнулись с этой проблемой. 72 % из

опрошенных испытывают ежедневное беспокойство по поводу мошенничества с использованием данного типа мошенничества.

Однако атаки с использованием технологий машинного обучения не ограничиваются только мобильными устройствами. IoT-устройства, в силу своей распространенности и часто недостаточной защищенности, также становятся все более привлекательной целью для злоумышленников, использующих машинное обучение для автоматизации поиска уязвимостей и повышения эффективности атак.

Хотя атаки с использованием IoT-ботнетов не являются принципиально новыми (например, печально известный ботнет Mirai, появившийся в 2016 г., использовал сотни тысяч уязвимых устройств для организации масштабных DDoS-атак) [3], наблюдается их эволюция. Злоумышленники используют методы машинного обучения для повышения живучести и эффективности ботнетов. В 2023 г. компания Nokia сообщила о 300-процентном росте DDoS-атак с использованием IoT-устройств в первой половине года. Ботнеты стали основой 90 % сложных многовекторных атак.

Многие IoT-устройства базируются на встроенных системах с легко анализируемой прошивкой. APT-группы все чаще используют автоматизированные инструменты, работающие на основе машинного обучения, для выявления уязвимостей в прошивках IoT-устройств [4]. Это позволяет им находить и эксплуатировать как известные, так и ранее неизвестные уязвимости.

Для эффективной защиты IoT-устройств от атак с использованием машинного обучения необходим многоуровневый подход:

Своевременная установка обновлений безопасности от производителя устройства критически важна для устранения известных уязвимостей. Многие производители, такие как Nest, Philips Hue и Samsung SmartThings, регулярно выпускают обновления для своих устройств.

Замена стандартного пароля, установленного производителем, на сложный и уникальный пароль, а также включение двухфакторной аутентификации, где это возможно, значительно повышает уровень безопасности.

Проведение регулярных проверок безопасности IoT-устройств и сети с использованием специализированных инструментов и сервисов.

Общая тенденция, наблюдаемая как в IoT-экосистеме, так и в сфере мобильных устройств, – это активное использование злоумышленниками машинного обучения для повышения эффективности, персонализации и адаптации атак к конкретным жертвам и условиям. Одним из примеров такого использования является применение генеративных нейросетей для создания дипфейков [5], используемых в атаках социальной инженерии, нацеленных на мобильные устройства.

Для детектирования фейк-изображений применяются методы машинного обучения, программы анализа подлинности видео; для опознания фальшивых профилей, с которых могут размещаться фейки,

применяются ИИ-инструменты поведенческого анализа. Например, программа FakeBuster для выявления дипфейков во время трансляций в Zoom и Skype, сервис Deepware (scanner.deepware.ai) распознает дипфейк-видео. К несовершенствам нейросетевой технологии распознания фейков относятся значительный процент ложных срабатываний и ограниченная эффективность (так, детекторы ИИ-контента, обученные искать определенные маркеры фейков, плохо справляются с другими типами фейков), а также малодоступность ИИ-инструментов распознавания фейков для большинства пользователей мобильных устройств [6]. Резкие движения актера, использующего цифровую дипфейк-маску, могут привести к ее «слетанию», движение рук перед лицом также может создать искажения [7]. Целесообразна избирательность в цифровом дистанционном общении, пониженное доверие сообщениям и звонкам с незнакомых номеров. Есть сервисы и фактчекинговые сайты для проверки подлинности присылаемых через соцсети фото- и видеоматериалов. Так есть сервис Deepfake Detector от Microsoft для детектирования фейковых фото и видео; в России АНО «Диалог регионы» в 2023 г. запустил платформу мониторинга аудиовизуальных дипфейков «Зефир» с помощью «алгоритмической оценки и анализа с помощью искусственного интеллекта», эффективность которой, по заявлению разработчиков, порядка 80 % [6].

Защита мобильных и IoT устройств должна строиться на комплексном подходе, учитывающем современные научно-технические достижения в области защиты информации. Важно быть в курсе новых видов угроз и принимать превентивные меры заранее до того, как нанесен ущерб пользователю.

Список использованных источников:

1. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1(109). С. 178–188.

2. Бондаренко И.С. Информационная безопасность: учебник / И.С. Бондаренко. М.: МИСИС, 2023. 254 с. Электрон. версия. URL: https://e.lanbook.com/book/360344.

3. Будущее киберугроз: IoT-устройства в центре внимания хакеров // Anti-malware. URL: https://www.anti-malware.ru/analytics/ ThreatsAnalysis/ IoT-devices-attacks#part31 (дата обращения: 19.04.2025).

4. Прогнозы по продвинутым угрозам на 2025 г. // SecureList. URL: https://securelist.ru/ksb-apt-predictions-2025/111090/.

5. Конструктивное использование DeepFake технологии // Хабр. URL: https://habr.com/ru/articles/503038/.

6. Миронова Н.Г. Технологии медиабезопасности: методы противодействия фейк-контенту в цифровых медиа // Экономика и право: проблемы, стратегия, мониторинг: колл. монография. Чебоксары:

«Издательский дом «Среда», 2024. 197 с. Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=78769542.

7. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. СПб.: Лань, 2025. 124 с. Электрон. версия. URL: https://e.lanbook.com/book/445250.

Shushakova A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

SOME NEW TYPES OF ATTACKS ON MOBILE AND IOT DEVICES USING MACHINE LEARNING TECHNOLOGIES AND COUNTERACTIONS TO THEM

Abstract. The article discusses some new types of attacks on mobile devices using machine learning technology and ways to counter them.

Keywords: information protection, cyber attacks on mobile devices, machine learning in information security, IoT devices.