СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

Е.В. Гайкевич, М.Г. Рогов

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

Современные антивирусные программы используют множество сложных технологий для обнаружения и предотвращения вирусных угроз. К основным компонентам и методам, используемым в современных антивирусах, относят сигнатурное обнаружение, поведенческий анализ и эвристику, облачные технологии, защиту в реальном времени, санбоксинг и виртуализацию [1].

Программы анализируют поведение системы и приложений, автоматически блокируют или инициируют проверки при обнаружении отклонений, указывающих на вредоносную активность [2].

Наиболее традиционным методом обнаружения вирусов является сигнатурное обнаружение. Антивирус сравнивает файлы на компьютере пользователя с базой данных вирусных сигнатур – уникальных строк кода или шаблонов, ассоциированных

с известными вирусами. Если обнаруживается совпадение, файл считается зараженным и принимаются соответствующие меры.

Современные угрозы часто используют эксплойты для эксплуатации уязвимостей, требуя непрерывного обновления антивирусов. Искусственный интеллект и машинное обучение помогают разрабатывать новые методы обнаружения вирусов, предоставляя антивирусам возможность анализировать большие и разнообразные наборы данных, учиться на примерах прошлых атак и непрерывно адаптироваться к новым угрозам [3].

Эффективность антивирусных программ улучшается благодаря интеграции ИИ и машинного обучения, что делает их неотъемлемым элементом современной информационной безопасности.

Использование нейросетей в разработке вредоносного ПО позволит создавать целенаправленные атаки, оптимизировать распространение вирусов и даже разрабатывать новые типы атак. Эти возможности делают искусственный интеллект мощным инструментом в руках злоумышленников.

Искусственный интеллект может обучаться на гораздо больших и разнообразных наборах данных, чем это возможно при традиционных подходах. Это позволяет антивирусным программам обнаруживать сложные угрозы, основываясь на поведенческих шаблонах и аномалиях, которые трудно заметить обычным сканированием.

Использование машинного обучения при разработке антивирусных программ является целесообразным не только с точки зрения улучшения работы с имеющимися проблемами, но и для предсказания новых угроз на основе анализа поведения существующих.

Список литературы

1. Вредоносные программы [Электронный ресурс]. – Режим доступа: https://www.calameo.com/read/006720537f97cf50b7288. – Дата доступа: 23.04.2024.

2. Introduction to Antivirus – Tryhackme [Электронный ресурс]. – Режим доступа: https://nehrunayak.medium.com/introduction-to-antivirus-tryhackme-3bdbdc6d8ab8. – Дата доступа: 23.04.2024.

3. How cybercriminals try to bypass antivirus protection [Электронный ресурс]. – Режим доступа:https://www.kaspersky.com/resource-center/threats/combating-antivirus. . – Дата доступа: 23.04.2024.