Искусственный интеллект: оружие против компаний или способ борьбы с хакерами

Д. ХОМУТОВ,
директор компании Ideco

В 2023 г. 83 % компаний отметили, что нейросети являются неотъемлемой частью их рабочих процессов. Ожидается, что российский рынок ИИ увеличится еще на 38,1 % до 2030 г. Однако в связи с широким распространением инноваций растут и угрозы взлома AI. Мошенники все чаще используют уязвимости машинных алгоритмов с целью получения выгоды.

Нейросети являются не только мощным защитным механизмом от кибератак, но и инструментом для их создания. Атакующий код, направленный на искусственный интеллект, быстро распространяется, что приводит к взломам личных данных как простого пользователя интернета, так и организаций, в том числе и из сферы ритейла.

Защитные методы от данной угрозы, напротив, на данный момент ограничены. Подобная “лазейка” позволяет мошенникам управлять целостностью систем машинного обучения, их конфиденциальностью и доступностью.

Кибератаки с использованием искусственного интеллекта эксперты предсказывали еще несколько лет назад. В 2019 г. более 80 % ИБ-специалистов были уверены, что AI увеличит масштаб угроз, а 66 % ожидали беспрецедентные взломы, сгенерированные нейросетями. Сейчас фактически проигрывается этот сценарий.

Злоумышленники используют совершенные технологии для создания крупных атак, так как ИИ легко справляется с большим объемом данных. Нейронные сети в том числе нередко используются для фишинговых взломов. Более того, Россия вошла в топ-10 стран по количеству DDoS-атак, которые перегружают целевые системы и создают масштабные кампании фишинга, отправляя получателям множество зараженных электронных писем.

Кроме того, AI используется хакерами в социальной инженерии для генерации зараженных электронных писем и ссылок с целью обмана пользователей и получения их личных данных. В 2023 г. компании назвали самой распространенной сетевой угрозой спам-рассылку — эту проблему отметили 47 % опрошенных в исследовании года. Более того, каждый день в мире отправляется свыше 122 млрд хакерских сообщений — это 85 % мирового почтового трафика. Такие показатели подчеркивают важность защиты своей учетной записи от мошенников.

Лучший способ обезопасить компанию — внедрить обучение кибербезопасности и ИИ для сотрудников на постоянной основе. Так как с каждым днем угрозы становятся все изощреннее, всей команде организации необходимо быть осведомленными о новых хакерских уловках. Обучение является важной составляющей любого рабочего процесса, тем более в России наблюдается нехватка квалифицированных киберспециалистов. Только 3,5 % в полной степени соответствуют текущим требованиям для работника этой сферы. Посредством обучения возможно улучшить навыки специалистов и, следовательно, сократить количество атак более чем на 70 %.

Помимо обучения сотрудников, следует принять дополнительные меры для повышения общей IT-безопасности компании. В первую очередь необходимо разработать улучшенные алгоритмы обучения AI с учетом его возможных уязвимостей. Это поможет сделать ИИ-модель устойчивее и надежнее на 87 %. Также для слаженной работы нейронной сети необходимо заниматься ее “тренировкой”. Это процесс, в ходе которого на специально созданных атаках нейросеть учится защищаться от подобных киберопасностей в будущем.

Хакерские угрозы постоянно развиваются — все чаще мошенники прибегают к новейшим технологиям. По этой причине необходимо непрерывно совершенствовать искусственный интеллект с целью развития технологий и усиления безопасности. Обновление и улучшение моделей помогут быть на шаг впереди злоумышленников и снизят число взломов на 84 %. Кроме того, необходимо постоянно обновлять программное обеспечение до последней доступной версии. Эта мера также помогает сократить число кибератак более чем на 90 %.

На данный момент автоматизированные электронные письма и чат-боты — два наиболее распространенных варианта использования ИИ в повседневной деловой коммуникации.

Статью целиком читайте в бумажной версии журнала