Конспект лекции

С.С. Жумажанова, П.С. Ложников

Этика и правовые проблемы искусственного интеллекта

Технологии ИИ в задачах защиты информации

ТЕХНОЛОГИИ ИИ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

В последнее время в связи с повышением значимости информационной безопасности (ИБ) различных объектов информатизации отмечается достаточно активное применение методов ИИ в процессе решения задач по обеспечению защиты информации. В современных условиях информационная составляющая оказалась на первом плане, и в мире идёт самая жестокая борьба за умы и интеллект. Эксперты считают, что информационные войны с развитием ИИ выходят на совершенно новый уровень. Использование новых технологий способствует роботизации процессов при ведении информационного и дезинформационного противоборства. Это, в свою очередь, может привести к возникновению кризисных явлений невероятных масштабов.

В сфере информационной безопасности применение ИИ начиналось (в начале 2000-х) с построения систем, облегчающих работу специалистов определенного профиля, в частности вирусных аналитиков. Есть глобальные компании, анализирующие в Сети колоссальный объем информации, которая может указать на новые угрозы или, например, предсказать атаки нулевого дня. У этих компаний есть системы, которые собирают массивы данных, анализируют их с помощью технологии класса ИИ, выявляют закономерности, проводят кластеризацию данных и прогнозируют угрозы.

ИИ пришел в индустрию безопасности позже, чем в другие отрасли. В некоторых отраслях, где применим ИИ никто не пытается послать искусственные данные, чтобы обмануть систему ИИ. В них, как правило, строились модели, базирующиеся на доказанных законах природы или социологии.

В настоящее время специалисты делят продукты, предназначенные для обеспечения информационной безопасности, применяющие технологии поведенческого анализа и предиктивной аналитики, на 9 типов (рис. 1).

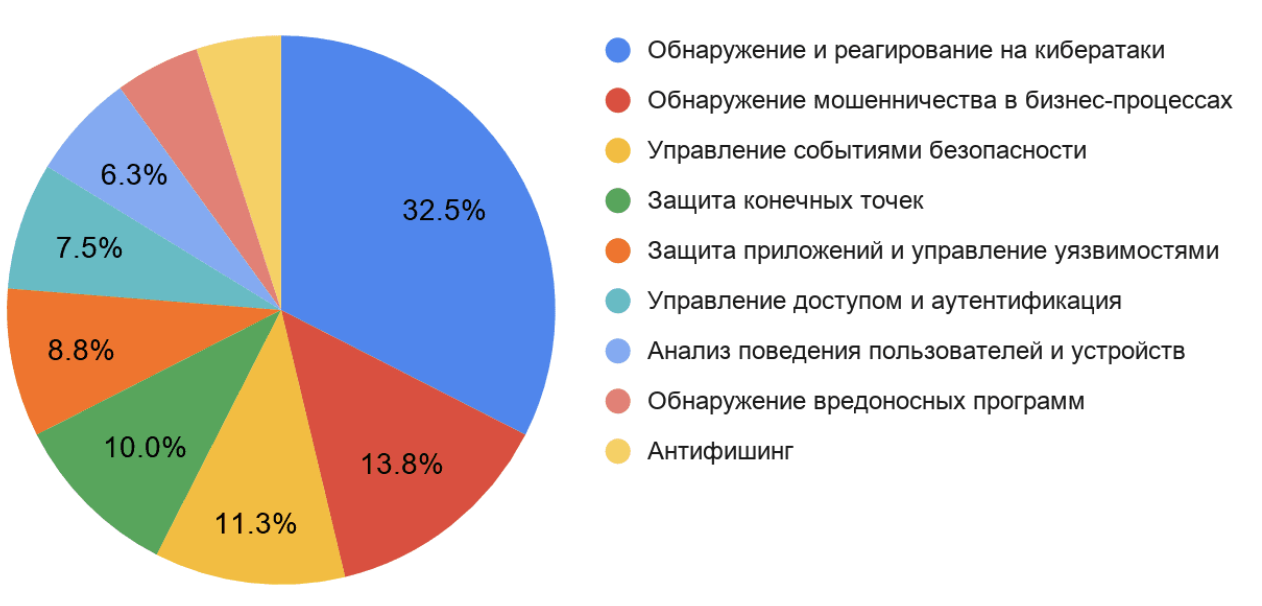


Рис.1. Распределение продуктов с применением технологий ИИ по сценариям использования

Машинное обучение для автоматизированного обнаружения угроз. Машинное обучение может отслеживать и регистрировать модели использования сети среди сотрудников в организации и своевременно предупреждать руководителей об обнаружении аномального поведения. Улучшение аутентификации с помощью ИИ (поведенческая биометрия на базе ИИ). При использовании интеллектуальной модели безопасности RBA злоумышленнику недостаточно просто знать пароль к системе.

ИИ в предотвращении фишинга: ИИ проанализирует стиль письма, синтаксис и выбор слов для выявления противоречий и предотвращения попадания в ловушку, что позволит пользователю безопасно просматривать и скачивать. ИИ выступает непосредственно против самого ядра фишинговых писем: социальной инженерии. Предиктивная аналитика: прогнозировать атаки и наращивать защиту еще до того, как данные атаки произойдут.

При защите от ИИ с помощью ИИ машинное обучение помогает автоматизировать обнаружение угроз. Особенно это касается новых угроз, от которых не могут защитить традиционные антивирусные системы и брандмауэры. Машинное обучение может на 50–90% сократить количество ложных срабатываний, представляющих серьезную опасность при традиционном обнаружении угроз. В отличие от инструментов обнаружения предыдущего поколения, основанных на сигнатурах, машинное обучение может отслеживать и регистрировать модели использования сети среди сотрудников в организации и своевременно предупреждать руководителей об обнаружении аномального поведения. Согласно статистике, в настоящее время 93% центров по безопасности используют инструменты искусственного интеллекта и машинного обучения для обнаружения угроз.

Основным преимуществом ИИ в кибербезопасности является способность прогнозировать атаки и наращивать защиту еще до того, как данные атаки произойдут. ИИ поможет поддерживать полную видимость всей сетевой инфраструктуры организации и анализировать конечные точки для обнаружения возможных уязвимостей. Уязвимость нулевого дня – программная уязвимость, обнаруженная злоумышленниками до того, как о ней узнали производители программы. ИИ - лучший выбор против уязвимостей нулевого дня, позволяющий быстро создать интеллектуальную защиту еще до того, как эти уязвимости будут использованы злоумышленниками. Кибербезопасность с использованием ИИ можно назвать чем-то вроде цифровой иммунной системы организации, подобно тому, как человеческие антитела атакуют инородные вещества.

Остро встает проблема защиты персональных данных при их обработке с помощью технологий искусственного интеллекта. Одним из методов решения проблемы защиты данных является их **обезличивание**. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ч. 9 ст. 3 Закона № 152-ФЗ). Приказом Роскомнадзора от 5 сентября 2013 г. № 996 к наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

* введение идентификаторов;
* изменение состава или семантики;
* декомпозиция;
* перемешивание.

**Отчуждаемые** от владельца **аутентификаторы** всегда могут быть переданы третьим лицам (умышленно или нет). По этой причине ключ (пароль) можно забыть, потерять, подменить, украсть. Эту проблему пытаются решить с помощью привязки ключей и паролей к биометрическим параметрам человека.

К наиболее изученным динамическим биометрическим образам относят: клавиатурный почерк, особенности воспроизведения рукописного пароля и подписи, характеристики походки, голоса, характер работы с компьютерной мышью, параметры тремора головы, термограмм лица и шеи.

К статическим биометрическим образам относятся образы отпечатка пальца, геометрии ладони, радужной оболочки глаза (радужки), сетчатки, трехмерного «изображения» лица или черепа, ДНК (дезоксирибонуклеиновая кислота) и другие.

**Список источников**

1. 93% of security operations center employing ai and machine learning tools to detect advanced threats | 2020-10-30 | Security magazine [electronic resource]. URL: [https://www.securitymagazine.com/articles/93779-of-security-operations-center-employing-ai-and-machine-learning-tools-to-detect-advanced-threats#:~:text=cyber%20security%20news-,93%25%20of%20security%20operations%20centers%20employing%20ai%20and%20machine,tools%20to%20detect%20advanced%20threats&text=these%20findings%20indicate%20that%20as,to%20address%20gaps%20in%20security](https://www.securitymagazine.com/articles/93779-of-security-operations-center-employing-ai-and-machine-learning-tools-to-detect-advanced-threats%23:~:text=cyber%20security%20news-,93%25%20of%20security%20operations%20centers%20employing%20ai%20and%20machine,tools%20to%20detect%20advanced%20threats&text=these%20findings%20indicate%20that%20as,to%20address%20gaps%20in%20security).
2. Ложников П.С. Биометрическая защита гибридного документооборота: монография / Новосибирск: изд-во СО РАН, 2017. — 130 с.
3. Применение технологий искусственного интеллекта в информационной безопасности [electronic resource]. URL: <https://www.anti-malware.ru/analytics/technology_analysis/using-artificial-intelligence-technologies-in-information-security>.