СТРАХОВАНИЕ*

ЕВГЕНИЙ ПАВЛЕНКО

1. **АЛЕКСЕЙ КУЗНЕЦОВ,**
генеральный директор страховой группы «Капитал-Полис»

2. **ИВАН ДЕМЧУК,**
с января 2023 года — генеральный директор АО «Страховая компания „Гайде“»

3. **ВЛАДИМИР ХРАБРЫХ,**
директор филиала СПАО «Ингосстрах» в Санкт-Петербурге

В ГОЛОСОВАНИИ ТАКЖЕ УЧАСТВОВАЛИ

ВИТАЛИЙ БАТОВ, директор Санкт-Петербургского филиала группы «АльфаСтрахование»

СЕРГЕЙ БЕЖЕНКОВ, генеральный директор АО «СК „Двадцать первый век“»

ЕВГЕНИЙ ДУБЕНСКИЙ, заместитель генерального директора АО «Зетта Страхование»

СЕРГЕЙ ДУДИН, директор Северо-Западного окружного филиала СК «Согласие»

РОМАН КОЛЫВАНОВ, директор Санкт-Петербургского филиала АО «ГСК „Югория“»

МИХАИЛ КРИВЦОВ, директор Северо-Западного филиала ПАО «САК „Энергогарант“»

КОНСТАНТИН КУДРЯВЦЕВ, директор Северо-Западного регионального центра САО «РЕСО-Гарантия»

ОЛЕГ КЯЛВИЯЙНЕН, директор филиала АО «Объединенная страховая компания» в Санкт-Петербурге

ИГОРЬ ЛАППИ, генеральный директор АО «Совкомбанк Страхование»

ТАТЬЯНА НИКИФОРОВИЧ, вице-президент по развитию бизнеса СК «Ренессанс-страхование»

КИРИЛЛ ПАВЛОВ, директор филиала ПАО «СК „Росгосстрах“» в Санкт-Петербурге и Ленинградской области

ВЛАДИМИР ПЫСТИН, старший вице-президент — директор Санкт-Петербургского филиала страхового дома ВСК

ВАЛЕНТИН СМЫШЛЯЕВ, директор филиала страховой компании «Макс» в Санкт-Петербурге

МАРИНА УРАЛЬСКАЯ, директор Санкт-Петербургского филиала АО «Согаз»

ДМИТРИЙ ФИЛАТОВ, директор Северо-Западного филиала ООО «Британский страховой дом»

КАНДИДАТУРЫ, ПРЕДЛОЖЕННЫЕ В ХОДЕ ГОЛОСОВАНИЯ

АНАТОЛИЙ КУЗНЕЦОВ,
президент Союза страховщиков Санкт-Петербурга и Северо-Запада

* *САО «Медэкспресс» в этом году не включено в список номинантов из-за процесса реструктуризации, который закончился осенью 2023 года*

12 → По его словам, применение ИИ не только сокращает время тестирования безопасности, генерации сценариев атак, анализа собранных данных, верификации уязвимостей, создания отчетов, но и позволяет проводить более частые и комплексные проверки в большем масштабе. «Для крупных и динамичных инфраструктур это действительно важно, здесь можно привести в качестве примера генеративные модели ИИ. PentestGPT может выступать ассистентом специалиста при проведении пентеста (метод оценки безопасности IT-систем средствами моделирования атаки.— **„Ъ“**)»,— отмечает эксперт.

Господин Фокин уверяет, что использование хорошо обученного ИИ позволяет повысить качество пентеста и избежать погрешностей, которые сопряжены с человеческим фактором. Искусственный интеллект, продолжает он, способен дать более высокую точность, снижая ложные срабатывания и выстраивая векторы атак на основе реальных достижений. «Модели, обученные на больших наборах данных, потенциально позволяют распознавать закономерности и выявлять уязвимости, которые могут быть неочевидны для ИБ-специалистов»,— поясняет господин Фокин. Он считает, что ИИ со временем сможет адаптировать используемые тактики и техники, обучаясь на прошлых результатах, в зависимости от угроз и окружения инфраструктуры, в котором он находится. «Применение искусственного интеллекта позволит снизить общие затраты на пентест и получить силу тысяч пентестеров в одной автоматизированной системе, а также сократить время на исправление обнаруженных уязвимостей за счет их более качественной приоритизации»,— добавляет эксперт.

При этом директор центра информационной безопасности «Ланит-Интеграции» отмечает, что использование ИИ при атаках на инфраструктуру сопряжено с некоторыми рисками: в отличие от человека, он не осознает возможных последствий и может не соблюдать ограничения при тестировании, поскольку не способен оценить риск воздействия на бизнес-процессы. «ИБ-специалист обладает творческой силой, интуицией и, возможно, не в 100% случаев, но лучше понимает контекст задачи. Поэтому, на мой взгляд, предпочтительный сценарий — сочетание возможностей ИИ и квалифицированных специалистов»,— дополняет он.

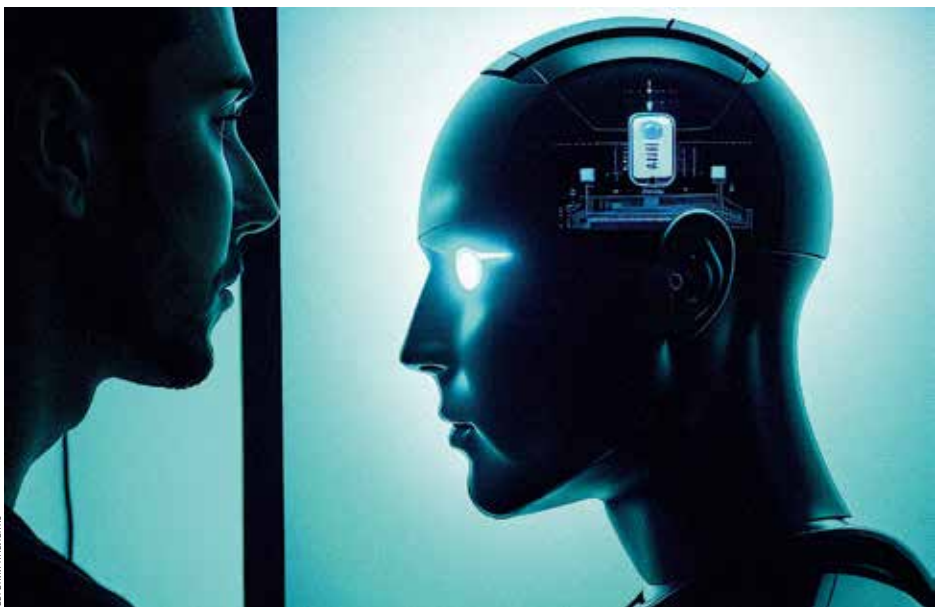
Среди перспектив применения ИИ в пентестах Николай Фокин отмечает несколько направлений: создание систем, способных адаптироваться к ландшафту и контексту, а также совершенствоваться по результатам достижений, автоматизация и симуляция сложных сценариев атак, повышение точности алгоритмов, а также более быстрое развитие инструментария для пентеста благодаря накоплению большого объема данных. ИИ хорошо справляется и с задачей обнаружения уязвимостей нулевого дня — искусственный интеллект может анализировать поведение систем и выявлять аномалии, связанные с возможностью эксплуатации. Отдельно стоит отметить вовлечение все большего числа специалистов по безопасности во взаимодействие с ИИ и его обучение.

ИИ НА СТРАЖЕ ИНФОРМАЦИИ Детекция аномалий (обнаружение уязвимостей) способна выявлять различные типы вредоносных активностей, которые не могут быть определены общепринятыми методами. Традиционные методы детекции аномалий опираются на заранее известные паттерны вредоносной активности, например, на сигнатуры вирусов, говорит руководитель практики анализа данных центра компетенций больших данных и искусственного интеллекта «Ланит» Владислав Балаев. По его словам, шаблоны вредоносного поведения ищутся по уже выявленным ранее типам атак. «Методы детекции аномалий основаны на том, что создается модель типичного поведения системы. Далее происходит анализ действий системы, который позволяет понять, насколько ее поведение отличается от обычного»,— поясняет он, добавляя, что традиционные методы ищут паттерны подозрительной активности в работе системы, а методы детекции аномалий создают картину нормального поведения, где любые признаки отклонения считаются вредоносными.

Среди преимуществ методов детекции аномалий господин Балаев отмечает способность выявлять новые, ранее не случавшиеся типы вредоносной активности. Среди недостатков — частые сработки на легитимные события, которые отличаются от обычного поведения: перезагрузка системы, обновление ПО, смена пользователей, перепрошивка сетевых устройств.

Искусственный интеллект представляет собой совокупность математических методов, которые используются для выделения аномалий, объясняет эксперт. По его словам, ИИ вместе с современными MLOps-практиками дает возможность автоматизировать обработку больших объемов данных ИБ. На них обучаются модели машинного обучения, позволяющие выявлять скрытые закономерности между различными показателями работы информационных систем. «Благодаря этому повышается эффективность обработки данных о работе информационных систем, что в конечном счете увеличивает точность и полноту выявляемых атак и вредоносной активности»,— подчеркивает господин Балаев.

Среди главных перспектив развития технологий детекции аномалий с использованием ИИ эксперт называет следующие тренды: способность выявлять нелинейные сложные зависимости между различными компонентами информационных систем и обнаружение неизвестных ранее типов вредоносной активности. «Эти методы не являются панацеей и обладают рядом недостатков, самым большим из которых является наличие ложных срабатываний, требующих фильтрации результатов и тонкой настройки системы. Однако благодаря своим преимуществам, несмотря на описанные выше нюансы использования, детекция аномалий является необходимым звеном для обеспечения комплексной защиты системами обнаружения вторжений»,— заключает господин Балаев. ■



ЕВГЕНИЙ ПАВЛЕНКО

ИСПОЛЬЗОВАНИЕ ОБУЧЕННОГО ИИ ПОЗВОЛЯЕТ ИЗБЕЖАТЬ ПОГРЕШНОСТЕЙ, КОТОРЫЕ СОПРЯЖЕНЫ С ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ

НЕЙРОСЕТИ