Как искусственный интеллект изменит представление об информационной и компьютерной безопасности в ядерной сфере

Митчелл Хьюз

Искусственный интеллект (ИИ) и технологии машинного обучения потенциально способны произвести революцию в мире выступая в качестве двигателя беспрецедентного прогресса и инноваций и меняя наш подход к созданию, потреблению и использованию информации. Технологии ИИ будут становиться все более совершенными, что будет приводить к трансформации целых отраслей, позволит оптимизировать различные процессы и даже может повлиять на наш образ жизни. Ядерный сектор не является здесь исключением, и можно ожидать, что преимущества ИИ найдут применение во многих процессах и операциях на ядерных и радиологических установках.

В то же время, стремительное развитие ИИ порождает массу различных рисков. Злоумышленники могут задействовать ИИ для организации более изощренных и целенаправленных атак или использовать его уязвимости для нарушения целостности компьютерных сетей или систем и доступа к закрытой информации на ядерных и радиологических установках.

Выгоды с точки зрения информационной и компьютерной безопасности

МАГАТЭ готовится к грядущим переменам, обусловленным распространением ИИ, укрепляя международное сотрудничество в этой области, чтобы все страны могли воспользоваться открывающимися возможностями и в то же время принять меры к смягчению рисков. Опираясь на такие механизмы сотрудничества, как технические совещания и проекты координированных исследований (ПКИ), МАГАТЭ поддерживает разработку и применение методов ИИ с учетом их особенностей, а также поиск контрмер и способов защиты от злоумышленников.

Возможно, самым значительным преимуществом ИИ в плане информационной и компьютерной безопасности является снижение зависимости от анализа оператором и необходимости его вмешательства. Системы с поддержкой ИИ могут работать круглосуточно и без выходных, выполняя мониторинг компьютерных сетей и систем на наличие угроз. Благодаря автоматизации этих задач у специалистов по физической ядерной безопасности появляется время для того, чтобы сосредоточиться на задачах более стратегического характера и эффективнее реагировать на инциденты, как только они произошли.

«Возможности ИИ в плане адаптивного обучения могут быть использованы для повышения информационной и компьютерной безопасности за счет быстрого выявления угроз и автоматического предоставления экспертам-людям необходимой информации для координации действий по реагированию, — рассказывает доцент Технологического института Джорджии в Соединенных Штатах Америки Фань Чжан, который участвовал в ПКИ, призванном поддержать исследования в области укрепления компьютерной безопасности. — Это не заменит штатных работников, а скорее позволит формировать ресурсы и аналитические выкладки, благодаря которым действия по раннему обнаружению и реагированию в области компьютерной безопасности станут реально осуществимыми».

Используя передовые алгоритмы машинного обучения, ИИ поможет также повысить эффективность защиты от кибератак на ядерных и радиологических установках за счет выявления аномальных данных в компьютерных системах. Оснащенные элементами ИИ системы безопасности могут непрерывно отслеживать и анализировать огромное количество данных, чтобы определить, является ли какая-либо активность аномальной на фоне нормальной эксплуатации установки. Кибератаки могут предусматривать передачу поддельных данных, чтобы предумышленно ввести в заблуждение операторов ядерных установок. В этом случае системы с элементами ИИ могут использоваться для предупреждения сотрудников, отвечающих за управление атомной электростанцией, о малейших отклонениях от нормальной эксплуатации. Создавая предпосылки для повышенной ситуационной осведомленности, ИИ также обеспечивает возможность раннего обнаружения преступных действий и подсказывает необходимые шаги для реагирования на инциденты.

Проблемы, требующие решения

Преимущества, которые дает применение ИИ на ядерных и радиологических установках, в значительной степени зависят от того, как было выполнено обучение систем ИИ. ИИ сведущ только в тех пределах, в которых представлены обучающие данные для его работы, и если он не располагает правильными исходными данными, им можно манипулировать, чтобы получать ложные показания и результаты. Это остается серьезным препятствием на пути к его применению в сфере физической ядерной безопасности. Даже с учетом последних достижений в технологии ИИ, использовать его в качестве замены человека не представляется целесообразным. Физическая защита, учет и контроль материалов и непосредственные измерения — все эти важнейшие направления работы для

обеспечения физической ядерной безопасности требуют участия человека.

Еще одной проблемой, связанной с применением ИИ в сфере физической ядерной безопасности, является понимание того, как и почему моделью ИИ было принято то или иное решение или выдан определенный прогноз. «Одними из самых значительных проблем с моделями ИИ являются их прозрачность и объяснимость — то есть когда люди могут понять логику предложенных ИИ решений или прогнозов. Часто бывает трудно понять, как эти модели приходят к тому, чтобы представить свои выводы, и это усложняет вопрос о доверии к таким результатам и обеспечении их достоверности, — говорит начальник Секции управления информацией Отдела физической ядерной безопасности МАГАТЭ Скотт Первис. — Это становится особенно проблематичным, когда эти модели заменяют собой датчики, предназначенные для непосредственных измерений, и человеческий опыт, накапливаемый с учетом уникальных характеристик каждой установки. Из-за этого становится практически невозможным дать какие-либо гарантии целостности системы, если нет предварительного глубокого и всестороннего понимания алгоритмов ИИ, чтобы представлять, как и почему принимаются соответствующие решения».

Руководящие материалы МАГАТЭ по обеспечению компьютерной безопасности в интересах физической ядерной безопасности включают в себя примеры положительной практики, касающейся системы сдержек и противовесов с участием человека, и дают операторам установок рекомендации о том, какие процессы могут быть автоматизированы за счет ИИ, а какие должны и далее оставаться под надзором человека, по крайней мере, до тех пор, пока не будут изучены риски, связанные с этой быстро развивающейся технологией. Они также являются важным ресурсом, который может служить подспорьем для стран при реализации первоочередных мер компьютерной безопасности для обнаружения кибератак, их предотвращения и реагирования на них.

Кроме того, МАГАТЭ разработало ПКИ для поддержки исследовательских работ в области укрепления компьютерной безопасности. Соответствующий ПКИ под названием «Совершенствование анализа инцидентов в сфере компьютерной безопасности на ядерных установках» объединил усилия исследователей из 13 стран, работающих над совершенствованием средств компьютерной безопасности на ядерных установках, включая методы на основе ИИ, в целях выявления аномалий, являющихся признаком целенаправленных кибератак.

Гонка технологий, связанных с внедрением ИИ

ИИ продемонстрировал свою способность приносить пользу там, где ядерные технологии используются в мирных целях. По мере того, как он все чаще находит

ИИ может также повысить эффективность защиты от кибератак на ядерных и радиологических установках за счет выявления аномальных данных в компьютерных системах. (Изображение: AdobeStock)

применение для улучшения процессов и операций на ядерных и радиологических установках, должна также расти и осведомленность о рисках, обусловленных его широким внедрением. Реализуя на практике преимущества ИИ, организации должны предусмотреть надежную программу обеспечения компьютерной безопасности в интересах физической ядерной безопасности.

Для этого требуется фундаментальная смена парадигмы, определяющей наши взгляды на аспекты доверенности и секретности. Необходимо учитывать каждую потенциальную точку отказа в системе, включая даже те, которые не связаны с ее системной архитектурой. Злоумышленники могут использовать ИИ для создания более изощренного вредоносного ПО, автоматизации кибератак, вскрытия систематических ошибок и уязвимостей в моделях или обхода мер безопасности путем имитации поведения добропорядочных пользователей. Эта гонка вооружений между защищающимися и нападающими будет требовать постоянных инноваций и адаптации к новым реалиям.

Более широкое внедрение технологий ИИ для укрепления мер компьютерной безопасности на ядерных установках может дать значительные преимущества, включая более эффективное обнаружение угроз, применение упреждающих мер безопасности, снижение зависимости от вмешательства оператора и улучшение реагирования на инциденты. Используя преимущества искусственного интеллекта и одновременно нейтрализуя его риски, организации могут значительно повысить свой уровень компьютерной безопасности перед лицом эволюционирующих киберугроз.