ТЕЛЕКОММУНИКАЦИИ

АЛЕКСАНДР КОРЯКОВ

1. **ДМИТРИЙ ПЕТРОВ,**
   генеральный директор ООО «Комфортел»

2. **АЛЕКСАНДР ЛОГИНОВ,**
   директор макрорегионального филиала «Северо-Запад» ПАО «Ростелеком»*

3. **АНДРЕЙ ГУК,**
   генеральный директор ООО «Обит»

В ГОЛОСОВАНИИ ТАКЖЕ УЧАСТВОВАЛИ

НИКОЛАЙ БЕЛОЗЕРОВ,
генеральный директор ООО «П.А.К.Т.»

СЕРГЕЙ ГЕРАСИМЕНКО,
исполнительный директор компании NewLink

АЛЕКСЕЙ ГОРБУНОВ,
руководитель макрорегиона «Северо-Запад» компании «Манго Офис»

АЛЕКСАНДР КРЫЛОВ,
генеральный директор SkyNet

ЕКАТЕРИНА КУДРЯШОВА,
с января 2023 года — региональный директор Западного региона ПАО «Вымпелком»

АЛЕКСАНДР СОЛОВЕНЧУК,
с февраля 2023 года директор филиала МТС в Санкт-Петербурге и Ленинградской области

АНДРЕЙ СУХОДОЛЬСКИЙ,
генеральный директор ООО «Смарт Телеком»

СЕРГЕЙ ТИМОШИН,
директор макрорегиона «Северо-Запад» Tele2 (дочернее общество ПАО «Ростелеком»)*

МАКСИМ ТОКАРЕНКО,
с апреля 2023 года — директор отделения по Санкт-Петербургу и Ленинградской области ПАО «Мегафон»

МАКСИМ ШЕВЧЕНКО,
с 1 марта 2023 года — межрегиональный директор Северо-Запада АО «ЭР-Телеком Холдинг»

* *Включены оба игрока, так как ежегодно жюри указывает на недостаток в списке одного из них. При условии четкого соблюдения условия: голос участника за сотрудника аффилированной компании не учитывается*

ИНТЕЛЛЕКТ НА СТРАЖЕ ИНФОРМАЦИИ

ЭКСПЕРТЫ РОССИЙСКОЙ ГРУППЫ IT-КОМПАНИЙ О ТРЕНДАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ.

МАТВЕЙ КИСЛИНСКИЙ («Ъ-ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ», №194 ОТ 18.10.2023)

Любая новая и перспективная технология всегда сталкивается с тем, что в какой-то момент ее начинают использовать как во благо, так и наоборот. Искусственный интеллект не стал исключением и нашел свое применение и у хакеров. Защищать инфраструктуру от вредоносного программного обеспечения и других атак штатному IT-специалисту будет сложно, поэтому компании все больше задействуют искусственный интеллект для борьбы со злоумышленниками. Эксперты российской группы IT-компаний «Ланит» рассказывают о трендах искусственного интеллекта в кибербезопасности.

ЕВГЕНИЙ ПАВЛЕНКО

ИИ СМОЖЕТ АДАПТИРОВАТЬ ИСПОЛЬЗУЕМЫЕ ТАКТИКИ И ТЕХНИКИ, ОБУЧАЯСЬ НА ПРОШЛЫХ РЕЗУЛЬТАТАХ

Согласно данным аналитической компании IDC, расходы на искусственный интеллект (ИИ) в 2023 году в Европе достигнут $34,2 млрд, что составляет 20,6% мирового объема инвестиций в эти технологии. Аналитики отмечают, что больше всего средств вкладывается в банковскую сферу (15,7%), сферу услуг (11,2%) и ритейл (10,9%).

В то же время инвестиции в развитие искусственного интеллекта в кибербезопасности также демонстрируют положительную динамику. Так, по данным Markets & Markets, сейчас объем мирового рынка ИИ в этой сфере достигает $22,4 млрд, а к 2028 году прогнозируется его увеличение до $60,6 млрд. Аналитики связывают такой финансовый подъем с повышенной уязвимостью сетей Wi-Fi, вызванной огромным количеством мобильных и смарт-устройств. Самый высокий среднегодовой темп роста до 2028 года будет наблюдаться в Азиатско-Тихоокеанском регионе, куда входят Китай, Россия, США и другие страны. В Markets & Markets подчеркивают, что в связи с популярностью перехода бизнеса на облачные серверы злоумышленники вынуждены адаптироваться и использовать новые способы кибератак: программы-вымогатели, вредоносное ПО для мошенничества с рекламой, DDoS, ботнеты, трояны и др.

Мошенники уже больше трех лет задействуют ИИ в собственных целях. Так, в конце 2020 года аналитики компании Trend Micro, специализирующейся на кибербезопасности, совместно с Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия и Европолом подготовили доклад «Злонамеренное использование и злоупотребление искусственным интеллектом». В нем указано, что технологии ИИ чаще всего применяются для создания дипфейков, которые заменяют голос или изображение одного человека на другого. Также искусственный интеллект используют для повышения эффективности вредоносного ПО.

ИИ В ЦЕНТРАХ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ Искусственный интеллект в центрах управления безопасностью (SOC) применяется во многих направлениях: для автоматизации процессов и отдельных действий, разгрузки аналитиков от ручной работы, а также в принятии некоторых решений, объясняет директор центра мониторинга и противодействия кибератакам IZ:SOC компании «Информзащита» Александр Матвеев. По его словам, применение ИИ может значительно упростить работу SOC, например увеличит скорость обработки инцидентов и уменьшит количество рутинных задач, которые отнимают много времени и зачастую мешают глубже погружаться в суть. «Автоматизация и, как следствие, упрощенный процесс первичной обработки позволят аналитикам больше концентрироваться на самих инцидентах»,— отмечает он.

Господин Матвеев подчеркивает, что ИИ вряд ли полностью заменит человека, однако может стать инструментом для решения задач: «Все упирается в вопрос доверия к ИИ и принятым им решениям, которые могут привести к драматическому исходу». Насколько бы ни была обученной модель ИИ, она рано или поздно столкнется с чем-то, что отсутствовало в данных для обучения, поэтому еще рано говорить о том, что ИИ заменит сотрудников SOC.

По прогнозу Александра Матвеева, вероятность того, что компании целиком перейдут на ИИ в кибербезопасности, крайне мала. «Многие уже частично применяют или планируют использовать функционал ИИ для решения и упрощения конкретных задач, а также для автоматизации отдельных процессов. Это позволяет не только экономить ресурсы, но и предоставляет определенное конкурентное преимущество»,— отмечает он, добавляя, что рано или поздно большинство компаний заместят с помощью ИИ все больше функций, которые сейчас выполняются аналитиками вручную. Среди перспективных направлений для искусственного интеллекта господин Матвеев называет прогнозирование атак, в том числе тех, о которых достоверно еще неизвестно, планирование реагирования на инциденты, поддержку в восстановлении скомпрометированных систем и т. д.

ИИ В СИМБИОЗЕ С ЧЕЛОВЕКОМ Искусственный интеллект способен значительно ускорить работу, автоматизируя задачи пентеста (анализ системы на наличие уязвимостей), говорит директор центра информационной безопасности «Ланит-Интеграции» Николай Фокин. ➔ 16