Институт статистических
исследований и экономики знаний

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ТРЕНДЫ | РАЗРАБОТКИ | ЧЕЛОВЕЧЕСКИЙ КАПИТАЛ
ИНФРАСТРУКТУРА | ИСПОЛЬЗОВАНИЕ | ЭФФЕКТЫ

№ 7 / 2024

Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ в очередном выпуске новой серии информационно-аналитических материалов «Искусственный интеллект» представляет обзор трендов применения бизнесом решений на основе искусственного интеллекта (ИИ) в целях цифровой безопасности.

Оценки основаны на результатах обследования 2.5 тыс. организаций 20 отраслей экономики (обрабатывающая промышленность, торговля, финансы и страхование, транспорт и логистика, ИТ-отрасль, телекоммуникации и др.), проведенного ИСИЭЗ НИУ ВШЭ в конце 2023 г.

Настоящий выпуск подготовлен в рамках проекта «Мониторинг технологического развития искусственного интеллекта в Российской Федерации» тематического плана научно-исследовательских работ, предусмотренных Государственным заданием НИУ ВШЭ.

ИИ ДЛЯ КИБЕРБЕЗОПАСНОСТИ: ТРЕНДЫ И ВОСТРЕБОВАННОСТЬ

В 2023 г., по данным InfoWatch, в мире зафиксировано 11 549 утечек данных (порядка 30 ежедневно), на каждую из них в среднем приходилось более 4 млн записей персональных данных. На рост количества атак (+61.6% к 2022 г.) влияет, в том числе, распространение технологий ИИ (генеративных моделей, дипфейков, ботов, усложнение техник социальной инженерии и др.).

Решения на основе ИИ также помогают предотвращать атаки злоумышленников: перспективные методы машинного обучения применяются для определения поддельных данных (включая аудио- и видео-), выявления и прогнозирования действий нарушителей, в целом более эффективной защиты электронных систем, информационных сетей и различных устройств (компьютеров, серверов, мобильных телефонов). По некоторым оценкам, внедрение инструментов ИИ и автоматизации сокращает время реагирования на инциденты кибербезопасности с 2.3 дней до 58 минут.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ИИ В КИБЕРБЕЗЕ

Среди ИИ-инструментов обеспечения цифровой безопасности наиболее популярны **системы прогнозирования новых угроз**, обученные обнаруживать закономерности на данных о ранее совершенных атаках. Разработка таких систем предполагает создание базы угроз, и ключевой задачей тут становится анонимизация персональных и коммерческих данных (обезличивание обучающих датасетов). При эксплуатации системы прогнозирования важной задачей, наряду с предотвращением утечки данных, является также недопущение искажений внутренней логики ее ИИ-модели.

Минимизировать возможности киберугроз со стороны внутренних нарушителей (инсайдеров) позволяют методы **поведенческой аналитики** сотрудников. Их применение считают необходимым 87% руководителей подразделений по информационной безопасности крупнейших мировых компаний. Согласно InfoWatch, с утечкой данных по вине увольняющихся сотрудников сталкивались 73% организаций. «Лидирует» в данном отношении сфера образования, где подобные происшествия случались в 95% организаций. С компрометацией конфиденциальных и корпоративных данных по вине действующих и бывших сотрудников только за последние годы столкнулся целый ряд транснациональных корпораций (Google, Tesla, Disney и др.), а также Пентагон. Поскольку частым следствием утечек является финансовый и репутационный ущерб, крупные компании уделяют повышенное внимание мониторингу поведенческих паттернов персонала (отслеживание по критериям аномального вывода информации, нетипичных внешних коммуникаций, снижения производительности и иной активности) и автоматизированной оценке рисков, включая профилирование пользователей и рейтингование подозрительных сотрудников.

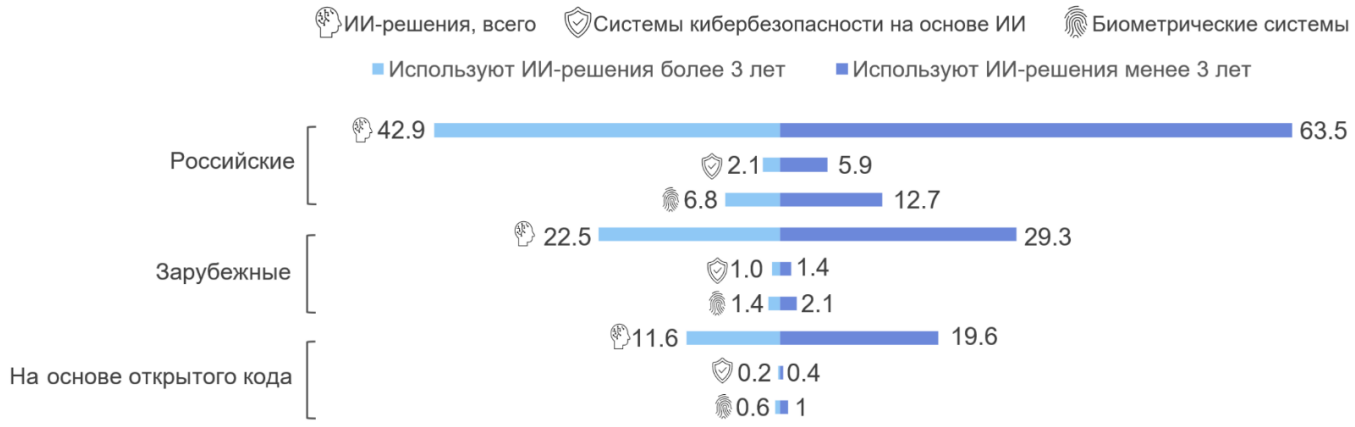
Набирают популярность **ИИ-решения для блокировки ботов** на основе анализа их активности. В 2023 г. боты сгенерировали почти половину сетевого трафика (49.6%), причем треть общего трафика (32%) – вредоносные боты, используемые для атак на сайты компаний, кражи конфиденциальных данных, мошеннических операций, нанесения вреда репутации конкурентов и др.

Генеративные модели могут, среди прочего, анализировать уязвимости кода, собирать расширенный контекст событий в сфере информационной безопасности, генерировать на основе идентификаторов пояснения по обнаруженным угрозам, выявлять неявные связи в системе. Для обнаружения фишинговых сообщений применяется функция выявления текста, написанного с помощью ИИ.

ВОСТРЕБОВАННОСТЬ В РОССИИ

Согласно результатам обследования организаций, проведенного ИСИЭЗ НИУ ВШЭ, отечественные инструменты ИИ в целом более востребованы у организаций, использующих такие технологии менее трех лет (63.5%). Вдвое чаще «новички» используют российские ИИ-системы кибербезопасности (5.9%) и системы биометрии (12.7%) (рис. 1). У зарубежных вендоров эти два класса решений приобретаются существенно реже (1.4% и 2.1% соответственно).

Рис. 1. Доля организаций, использующих ИИ-решения в области кибербезопасности, по типу вендора (в % от числа обследованных организаций – пользователей ИИ)



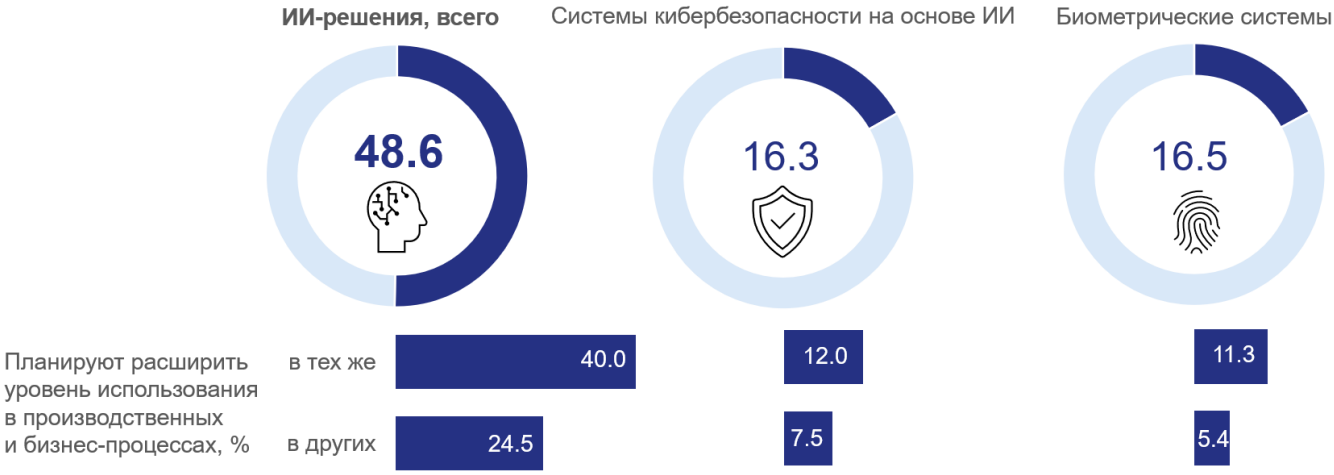
ИСИЭЗ НИУ ВШЭ

Решения на основе открытого кода крайне ограниченно востребованы в системах кибербезопасности и биометрии (0.4 и 1% организаций, использующих ИИ менее трех лет, и 0.2 и 0.6% – среди пользователей с опытом более трех лет соответственно), что связано не только с обработкой корпоративных данных, угрозой их компрометации, но и скрытыми рисками опенсорса. В базе Лаборатории Касперского содержатся данные по более 20 тыс. вредоносным пакетам с открытым исходным кодом в популярных репозиториях[1].

[1] По состоянию на ноябрь 2023 г.

И хотя инструменты на основе ИИ в целом и в частности применяемые для обеспечения безопасности физической и цифровой среды – относительно новое явление в корпоративной цифровой архитектуре, интерес к ним постепенно повышается. Так, среди компаний, использующих ИИ, каждая вторая планирует расширить уровень применения ИИ-решений и примерно каждая шестая намерена шире использовать как системы кибербезопасности, так и более понятные для бизнеса биометрические системы идентификации и аутентификации (16.3 и 16.5% соответственно) (рис. 2). В то же время интеграция подобных систем в ИТ-инфраструктуру компаний происходит с некоторой задержкой. Это объясняется необходимостью проведения дополнительной оценки рисков и угроз при внедрении ИИ, так как подобные системы работают с информацией различной степени доступности. В дополнение к этому компаниям необходимо обеспечить соблюдение требований внутренней политики безопасности и законодательных норм в отношении ИИ, в том числе стандартов, которые только формируются.

Рис. 2. Доля организаций, планирующих продолжать использовать ИИ-решения в области кибербезопасности (в % от числа обследованных организаций – пользователей ИИ)



ИСИЭЗ НИУ ВШЭ

Резюме: Спрос на ИИ-решения в области кибербезопасности со стороны компаний в ближайшие годы будет расти как в России, так и в мире. Этому будет способствовать все большая цифровизация производственных и бизнес-процессов и, в частности, распространение прорывных ИИ-инструментов (генеративного ИИ, мультимодальных нейросетей и др.), сопровождающееся появлением новых угроз. Комплексный подход к укреплению цифровой архитектуры должен предусматривать, помимо применения средств аналитики и защиты, повышение цифровой грамотности персонала и своевременную актуализацию политик безопасности. *Подробнее о том, как компании могут повысить безопасность использования ИИ, читайте в следующем выпуске серии*.

Авторы: **А. И. Фокина, Ю. В. Туровец**

Сайт ИСИЭЗ НИУ ВШЭ
issek.hse.ru

канал в Telegram
t.me/iFORA_knows_how

сообщество во «ВКонтакте»
vk.com/issekhse