DOI 10.37882/2223-2966.2023.12-2.11

РОЛЬ И МЕСТО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

THE ROLE AND PLACE OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF CYBERSECURITY

A. Ermolaev
V. Velikanov

Summary. This article presents a study and analysis of current trends and opportunities for the use of artificial intelligence in the field of cybersecurity. The paper examines the impact of artificial intelligence on cybersecurity in several aspects: from cyberattacks, cyber defense, as well as the impact of artificial intelligence on the labor market in this sector of the IT industry.

The section devoted to the role of artificial intelligence in cyber attacks analyzes modern cyber threats in which cybercriminals use IT solutions based on artificial intelligence to conduct cyber attacks. Specific cases and ways of using artificial intelligence to bypass information systems protection systems are considered.

In the section that reveals the importance of artificial intelligence in the field of cyber defense, innovative methods of using artificial intelligence to prevent cyber attacks are analyzed; machine learning technologies for improving the security of information systems are considered.

Keywords: artificial intelligence (AI); machine learning; cybersecurity; information security; neural network.

Ермолаев Алексей Сергеевич
QA-инженер, ООО Интернет-агентство «ИНТЕРВОЛГА»;
Магистрант, Волгоградский государственный технический университет
alexey.0994@mail.ru.
Великанов Василий Викторович
Кандидат экономических наук, доцент, Волгоградский государственный технический университет
helen901@mail.ru

Аннотация. В данной статье представлено исследование и анализ современных тенденций и возможностей использования искусственного интеллекта в сфере кибербезопасности. В работе рассматривается влияние искусственного интеллекта на сферу кибербезопасности в нескольких аспектах: со стороны кибератаки, киберзащиты, а также влияния искусственного интеллекта на рынок труда в данном секторе ИТ-отрасли.

В разделе, посвященном роли искусственного интеллекта в кибератаках, анализируются современные киберугрозы, в которых киберпреступники используют ИТ-решения, функционирующие на основе искусственного интеллекта, для проведения кибератак. Рассматриваются конкретные случаи и способы применения искусственного интеллекта для обхода систем защиты информационных систем.

В разделе, раскрывающем значение искусственного интеллекта в области киберзащиты, анализируются инновационные методы применения искусственного интеллекта для предотвращения кибератак; рассматриваются технологии машинного обучения для повышения защищенности информационных систем.

Ключевые слова: искусственный интеллект (ИИ); машинное обучение; кибербезопасность; информационная безопасность; нейронная сеть.

Введение

Популярность использования возможностей искусственного интеллекта (ИИ) ширится во многих отраслях, в том числе и в сфере кибербезопасности. Объем и сложность технологий, применяемых киберпреступниками, постоянно растут, требуя всё новых подходов и решений для противодействия этой угрозе. Указанные обстоятельства привели к активному внедрению инструментов искусственного интеллекта в область кибербезопасности, причем роль ИИ в этой сфере становится все более значимой.

В ближайшем будущем ИИ, построенный на основе машинного обучения, станет неотъемлемой частью всех систем кибербезопасности. Эта необходимость обусловлена тем, что обеспечение кибербезопасности связано с переработкой больших объемов данных, для операций с которыми важна высокая скорость выполнения операций и реагирования, а роль человека хоть и является в целом незаменимой, но при решении определенных задач искусственный интеллект действует иной раз заметно успешнее человеческого.

Роль ИИ в кибератаках

Рост популярности использования искусственного интеллекта в кибербезопасности обусловлен не только использованием ИИ-технологий при защите от кибератак. Наряду с этим также участилось использование ИИ при проведении самих кибератак.

Изначально технологии искусственного интеллекта способствовали повышению уровня безопасности корпоративных сетей, но злоумышленники смогли быстро адаптировать эти технологии под свои цели. В ходе кибератак взломщики могут изменять параметры информационных систем или разрабатывать новые программы и инструменты на основе искусственного интеллекта для нарушения целостности таких систем. В подобных

атаках искусственный интеллект используется с целью проникновения в сети и системы быстрее, чем организация сможет идентифицировать атаку и отреагировать на эти факты должным образом. Также киберпреступники научились использовать искусственный интеллект для сбора информации о том, каким образом компаниям удается предотвращать атаки на их вычислительные мощности и базы данных.

Использование ИИ при кибератаках не ограничено задействованием технологий искусственного интеллекта лишь для проникновения в сети и системы. Множество различных инструментов позволяют разрабатывать всё новые способы для киберагрессии.

Эксперимент, демонстрирующий возможности злонамеренного использования искусственного интеллекта, провели специалисты компании IMB. За основу был взят вирус-вымогатель Wanna Cry. Вредоносное приложение DeepLocker оснастили искусственным интеллектом, содержащим вирус Wanna Cry. Во время видеозвонка DeepLocker сканировал лица собеседников, далее он находил и распознавал нужного человека с помощью встроенной ИТ-процедуры, а затем заражал его компьютер вирусом WannaCry, который незаметно шифровал файлы и в дальнейшем использовался для вымогательства. Компания IBM создала эту программу, для того чтобы продемонстрировать потенциальные угрозы для сферы информационной безопасности.

Переход компаний на дистанционный режим работы увеличил масштабы использования инструментов аудио- и видеосвязи. Такая ситуация предоставила мошенникам широкие возможности для сбора образцов голоса и портретных изображений пользователей, которые могут быть использованы для создания фейк-контента, направленного на манипулирование людьми.

В отчете под названием «Social Engineering. Blurring reality and fake» (2020) инициативная группа экспертов-страховщиков компании CyberCube, специализирующаяся на киберугрозах, выделила три новые тенденции, которые, по их прогнозам, окажут значительное влияние на положение дел в этой области к 2025 году:

1. Подделка голоса индивида (deep voice mimicry). Создание правдоподобного и убедительного голоса может быть достигнуто за счет использования технологий искусственного интеллекта, машинного обучения и нейронных сетей. Эти передовые технологии позволяют генерировать голоса, очень похожие на человеческую речь.
2. Масштабное социальное профилирование (social profiling at scale). Создание комплексного профиля человека, как правило, на основе данных его социальных сетей или похищенной личной информации.
3. Подделка видео с помощью технологии «mouth mapping», которая позволяет имитировать артикуляцию человека при говорении.

Использование искусственного интеллекта во вредоносных целях открывает перед киберпреступниками широкие возможности. Это позволяет быстро и с большим охватом проводить кибератаки, что приводит к возрастанию атакующей мощи и зачастую застает информационные сети врасплох, не оставляя им времени на адекватную реакцию. Для противодействия этой новой угрозе необходимо тщательно исследовать, изучать и анализировать тактику действий злоумышленников, что позволит разработать надежные средства обеспечения кибербезопасности, способные предотвращать атаки с использованием искусственного интеллекта в будущем.

Можно выделить следующие области кибератак с применением ИИ:

1. Анализ. Это процесс извлечения ценной информации из данных или моделей. Исследование атакуемой модели машинного обучения для определения ключевых факторов, влияющих на ее производительность (например, на точность классификации). Этого можно достичь с помощью объясняющих методов, таких как LIME и SHAPLEY. Понимание того, как функционирует атакуемая модель, позволяет разработать более эффективные атаки или стратегии сокрытия вторжения. В тех случаях, когда атакуемая модель недоступна, аналогичные эксперименты можно проводить на ее реплицированной версии.

Методы машинного обучения могут использоваться для эксплуатации уязвимостей в системах биометрической аутентификации. К ним относятся такие методы, как подмена голоса, портрета и т.п.

2. Прогнозирование. Машинное обучение используется для составления прогнозов на основе прошлых данных. Например, атака может включать в себя определение того, какие кнопки были нажаты на смартфоне путем анализа движения (вибрации). Другой пример — прогнозирование конфиденциальной информации о пользователях социальных сетей с целью поиска уязвимых мест для потенциальных атак, а также поиска уязвимых мест программного обеспечения.
3. Поиск. Задача отыскания конкретной информации или объектов по определенным критериям. Например, это может быть идентификация человека путем анализа изображений с различных взломанных камер, поиск потенциальных инсайдеров путем изучения публикаций в социальных сетях с использованием семантического анализа

или обобщение и реферирование документов при сборе данных из общедоступных источников.
4. Генерация. Создание контента с помощью ИИ. К числу наступательных применений этой технологии относятся фальсификация медиаданных, подбор паролей и модификация трафика. Например, модификация трафика предполагает проведение атаки против системы машинного обучения, используемой для обнаружения вторжений, с целью скрыть реальные вторжения. Еще одним видом наступательного ИИ в этой категории являются «дипфейки». Они подразумевают создание реалистичных медиафайлов с помощью методов глубокого обучения и могут использоваться для моделирования чьего-то голос или изображения для фишинговых атак.
5. Принятие решений. Различные задачи, такие как разработка стратегического плана или координация атаки. Например, искусственный интеллект может быть использован для управления сетью автономных ботов и выработки оптимальной стратегии атак на сеть. Стоит отметить, что автоматизированные атаки могут осуществляться и без машинного обучения, однако использование обучения с дополняющими его элементами нападения доказало свою эффективность. Согласно отчету Microsoft, хотя использование ИИ в кибератаках на начальном этапе будет ограничено более опытными хакерами, но впоследствии оно может распространится на всю ИТ-систему мира благодаря расширению взаимодействия взломщиков и коммерциализации ИТ-инструментов. Эти инструменты включают в себя распространенные тактики, используемые злоумышленниками для обхода защитных систем (так указано в атласе MITRE).

Одним из ярких примеров автоматизации наступательных действий с использованием ИИ является размещение ботов в социальных сетях. Другой пример, приведенный в ряде исследований, связан с автоматизированным тестированием на проникновение (penetration test) на основе использования методов ускоренного обучения.

Выше мы рассмотрели, как машинное обучение может использоваться для выявления фишинговых атак. Однако важно отметить, что машинное обучение может применяться и для генерации фишинговых атак. Цель таких атак — обойти защиту системы путем создания некого заманчивого контента, побуждающего пользователя перейти по вредоносным ссылкам или установить вредоносное программное обеспечение в свою систему. Наступательные действия в этом контексте могут включать в себя подбор паролей, запутывание исходного кода программ, маскировку трафика и управление сетью ботов. Компания Microsoft даже организовала отдельный семинар, посвященный изучению наступательных технологий ИИ. Кроме того, Национальная комиссия по безопасности в области искусственного интеллекта США (National Security Commission on Artificial Intelligence, NSCAI) опубликовала обширный доклад, посвященный атакам с использованием ИИ.

Роль ИИ в защите от киберугроз

Возрастающая сложность и вместе с тем рост общего числа киберпреступлений требуют новых подходов в борьбе с этим злом. Внедрение инструментов искусственного интеллекта становится приоритетной задачей в этой борьбе.

Обнаружение угроз является первой линией обороны в кибербезопасности. Традиционные методы основаны на аналитической работе ИТ-специалистов, которые просматривают огромные массивы данных для выявления возможных угроз. Колоссальное количество информации превращает эту задачу в весьма продолжительный и трудоемкий процесс. Искусственный интеллект может не только нарастить скорость обработки данных, но и повысить точность обнаружений за счет машинного обучения, тем самым увеличив эффективность систем обеспечения кибербезопасности.

Вторая линия обороны — это прогнозирование и предотвращение кибератак. Искусственный интеллект, используя машинное обучение, позволяет системам безопасности обучаться на прошлых инцидентах, а затем использовать наработанные методы для прогнозирования и предотвращения кибератак в будущем. Возможность прогнозирования особенно полезна для выявления уязвимостей т.н. «нулевого дня» (уязвимости, о которых ещё никому неизвестно). Прогнозируя уязвимости нулевого дня до их эксплуатации, ИИ может существенно помочь человеку в разработке защитных алгоритмов и предотвратить несанкционированное проникновение в систему.

Система реагирования на кибератаки — это третья линия обороны. Автоматизированные системы быстрого реагирования, работающие на базе искусственного интеллекта, могут оперативно реагировать на обнаруженные угрозы и принимать меры по дальнейшей защиты системы. Например, может инициироваться изоляция пораженной системы или блокировка IP-адресов, с которых ведется атака. Быстрая реакция на атаки позволит значительно снизить ущерб, наносимый вредоносными кодами. После этого ИИ может проанализировать атаку, выявить источник и закономерности ее развертывания, что поможет укрепить защиту системы и разработать более надежную стратегию профилактики подобных инцидентов.

Можно выделить следующие направления, касающиеся использования машинного обучения для защиты от кибератак:

1. Обнаружение попыток взлома.
2. Расстановка приоритетов для предупреждения о потенциальной атаке.
3. Обнаружение активности вредоносных программ.
4. Идентификация living off the land (LoLt) атаки, при которой злоумышленник использует легитимное программное обеспечение для выполнения вредоносных действий.
5. Автоматизация действий по реагированию и смягчению последствий, после совершенной атаки для предотвращения дальнейшего распространения вредоносного кода.

Для эффективного и безопасного использования искусственного интеллекта в сфере кибербезопасности, нужно учитывать несколько важных обстоятельств:

1. Необходимо обеспечить защиту данных и алгоритмов искусственного интеллекта от взлома. Злоумышленники могут производить атаку на саму систему искусственного интеллекта, изменяя алгоритмы её работы для того, чтобы обойти защитные алгоритмы. В этих целях необходимо проводить регулярные проверки на возможные уязвимости.
2. Систему защиты на основе искусственного интеллекта необходимо постоянно обучать на различных типах кибератак, используя актуальные данные. ИИ не сможет эффективно обнаруживать новые типы атак, если он не будет обучен.
3. Необходимо учитывать правовые и этические нормы в отношении использования ИИ в кибербезопасности. Принятие решений на основе ИИ может привести к нарушению прав человека на приватность в сети. Компаниям нужно разрабатывать этические и правовые стандарты, которые будут регулировать работу искусственного интеллекта в области кибербезопасности.

Влияние ИИ на рынок труда в секторе кибербезопасности

В условиях быстрого развития технологий в области кибербезопасности появляется потребность в кадровом обновлении отрасли информационной безопасности (ИБ).

Использование искусственного интеллекта позволяет автоматизировать множество рутинных задач. Он отлично справляется с монотонными и трудоемкими процессами, такими как непрерывный мониторинг и анализ журналов регистрации событий в сети. Всё это позволяет специалистам по ИБ сосредоточиться на решении стратегических вопросов более высокого уровня.

Можно выделить несколько новых специальностей, которые помогут в перестройке профиля компетенций специалистов по ИБ.

1. Аналитики обеспечения безопасности искусственного интеллекта. Обязанности данной категории специалистов заключаются в отслеживании алгоритмов искусственного интеллекта, настройке модели ИИ и обеспечении актуальных мер безопасности системы ИИ.
2. Тренеры моделей ИИ. В обязанности тренеров моделей ИИ входит обучение модели ИИ, её контроль и настройка.
3. Пентестеры ИИ. В обязанности пентестеров (этических хакеров) входит проведение тестирования системы искусственного интеллекта на проникновение, а также оценка степени её защищенности.

Несмотря на такую модернизацию, важно подчеркнуть, что ИИ не сможет полностью заменить человека, поскольку специалисты кибербезопасности обладают большим опытом, рациональным мышлением и пониманием контекста, они также легко определяют этическую сторону проблем и способны подходит к поиску ответа на вопрос креативно. Внедрение систем безопасности на основе искусственного интеллекта сможет лишь дополнительно обеспечить надежность систем кибербезопасности, сочетая преимущества ИИ в скорости обработки данных с творческими способностями человека.

Заключение

Резюмируя высказанные выше соображения, можно сделать вывод о том, что технологии искусственного интеллекта в настоящее время стремительно развиваются; внедрение ИИ в системы кибербезопасности может значительно повысить эффективность защиты за счет увеличения скорости и точности обработки данных. Преимущества использования ИИ слишком значительны, чтобы их игнорировать.

Системы искусственного интеллекта продолжат эволюционировать, что в будущем расширит возможности их применения. Добавление новых наборов контекстных данных позволит ИИ принимать более обоснованные решения, а анализируя такие факторы, как сетевой трафик и поведение пользователей, ИИ сможет получать более глубокие знания о системах защиты, а также сможет предсказывать возможные отклонения в использовании каких-либо данных. Всё это будет способствовать развитию кибербезопасности и поможет в будущем конструировать значительно более надежные системы безопасности.

ЛИТЕРАТУРА

1. Искусственный интеллект и машинное обучение в кибербезопасности — прогноз на будущее. — URL: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity (дата обращения: 30.10.2023).
2. Роль и будущее искусственного интеллекта в кибербезопасности. — URL: https://ts2.space/ru/%D1%80%D0%BE%D0%BB%D1%8C-%D0%B8-%D0%B1%D1%83%D0%B4%D1%83%D1%89%D0%B5%D0%B5-%D0%B8%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB-2/ (дата обращения: 30.10.2023).
3. Роль искусственного интеллекта в киберпреступлениях. — URL: https://ir.alfastrah.ru/posts/482 (дата обращения: 30.10.2023).
4. Как ИИ влияет на рабочие места в сфере кибербезопасности и меняет рабочую силу в сфере кибербезопасности? — URL: https://www.cryptopolitan.com/ru/%D0%BA%D0%B0%D0%BA-%D0%B8%D0%B8-%D0%B2%D0%BB%D0%B8%D1%8F%D0%B5%D1%82-%D0%BD%D0%B0-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%83-%D0%B2-%D1%81%D1%84%D0%B5%D1%80%D0%B5-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8/ (дата обращения: 30.10.2023).
5. Влияние искусственного интеллекта на кибербезопасность. — URL: https://ts2.space/ru/%D0%B2%D0%BB%D0%B8%D1%8F%D0%BD%D0%B8%D0%B5-%D0%B8%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82%D0%B0-%D0%BD-10/ (дата обращения: 30.10.2023).
6. Роль искусственного интеллекта в кибербезопасности. — URL: https://vc.ru/dev/621020-rol-iskusstvennogo-intellekta-v-kiberbezopasnosti (дата обращения: 30.10.2023).
7. Роль искусственного интеллекта в обеспечении информационной безопасности. — URL: https://na-journal.ru/6-2023-informacionnye-tekhnologii/5812-rol-iskusstvennogo-intellekta-v-obespechenii-informacionnoi-bezopasnosti (дата обращения: 30.10.2023).
8. Искусственный интеллект и кибербезопасность. — URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost/viewer (дата обращения: 30.10.2023).

Журнал «Современная наука: актуальные проблемы теории и практики»