ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Мирзаева М.Б.[1], Абдазимов С.З.[2]

[1] *Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, г.Ташкент, Узбекистан, malikamirzaeva01@gmail.com;*
[2] *Академия МВД Республике Узбекистан, г.Ташкент, Узбекистан, saidazimov@gmail.com*

Abstract. The article examines a form of cyber-attack that uses disguised email as a weapon and the most serious cyber threats in the world, as well as advances in powerful tools in the field of artificial intelligence. Also, as data becomes more complex, machine learning helps you understand how easy it is to master many of the mechanical, simple aspects of security. The possibility of focusing on more intuitive, strategic aspects of the work of specialists will also be considered.

В настоящее время особую актуальность представляют всесторонние исследования, с различных точек зрения (этической, социальной, экономической, правовой), посвященные вопросам внедрения технологий искусственного интеллекта в самых разных сферах жизнедеятельности общества. Важно выявить возможности и угрозы, определить предельные границы применения искусственного интеллекта на практике. искусственный интеллект является вспомогательным, но ценным инструментом, который может выполнять и совершенствовать большое количество различных операций, осуществляемых в вузе, помогать в организации эффективного учебного процесса и выстраивании необходимых коммуникаций. Эффективное использование технологий ИИ в сфере высшего образования позволит осуществлять подбор наиболее оптимальной стратегии обучения, адаптированной под индивидуальные способности и потребности студентов и потребности рынка труда Искусственный интеллект (ИИ) быстро проникает в экосистему корпоративной безопасности, привнося широкий спектр передовых возможностей в то, что быстро становится ключевым аспектом успешной цифровой бизнес-модели.

Но хотя может показаться заманчивым просто бросить искусственный интеллект на цифровую стену, чтобы увидеть, где он работает, более мудрые бизнес-лидеры не торопятся, чтобы выяснить, где его можно использовать наиболее эффективно и как он должен сочетаться с обычными операциями, чтобы не мешать в целом.

По статистикам известно, что самые популярные приложения безопасности для искусственный интеллект включают защиту сети, конечных точек и самих данных. Свыше 80 % ИТ-руководителей, опрошенных в 2021 году, считают, что сети вызывают наибольшее беспокойство, за ними следуют 78 % по безопасности данных и 59 % по конечным точкам.

Фишинг, форма кибератаки, в которой в качестве оружия используется замаскированная электронная почта, считается одной из самых серьезных киберугроз во всем мире [1]. Цель фишинга – обмануть получателя электронной почты, заставив его поверить в то, что сообщение является законным, и убедить его выдать форму своей личности – будь то данные кредитной карты или данные для входа в бизнес. Только в первом квартале 2021 года во всем мире было обнаружено более 171 тысячи уникальных фишинговых сайтов, и только в первый месяц 2021 года были атакованы сотни известных брендов и законных организаций.

Небольшой спад в глобальных расходах на кибербезопасность. Предприятия и частные лица тратят средства на решение безопасности для противодействия киберпреступлениям, таким как фишинговые атаки [4]. В последние годы мировые расходы на кибербезопасность росли, и ожидается, что они продолжат расти в 2021 году, хотя и скомпрометированными темпами из-за воздействия пандемии коронавируса (COVID-19).

Искусственный интеллект привносит ряд мощных инструментов в эти конкретные приложения, но, возможно, не более, чем его способность просеивать огромные объемы данных в поисках шаблонов, которые указывают либо на потенциальное, либо на фактическое нарушение безопасности [2]. Кроме того, искусственный интеллект находит применение в таких областях, как управление идентификацией и доступом, а также в защите ресурсов, которые все чаще предоставляются за пределами традиционного брандмауэра: в облаке и на границе Интернета вещей (IoT).

Более того, что среды данных становятся все более сложными, машинному обучению легче взять на себя многие механические, обыденные аспекты безопасности, позволяя специалистам-людям сосредоточиться на более интуитивных, стратегических аспектах работы. Это может быть особенно эффективно при предотвращении DDoS-атак, которые пытаются вывести системы из строя, бомбардируя их запросами, возможно, с тысяч компьютеров. До того, как Amazon сообщила о DDoS-атаке со скоростью 2,3 терабит в секунду (Тбит/с) в феврале 2020 года, GitHub сообщил о самой крупной атаке в истории в 2019 году, когда на сервис попало более 1,45 Тбит/с в течение 15 минут.

Искусственный интеллект также становится важным активом в разработке программного обеспечения для кибербезопасности. В рамках новой модели разработки DevOps искусственный интеллект можно использовать для оценки уязвимостей и быстрого обновления кода. Это позволяет организациям внедрять новые уровни защиты и новые исправления для существующих уязвимостей по мере появления новых угроз.

Это может быть особенно эффективно в таких областях, как антивирусное программное обеспечение, говорит разработчик систем искусственного интеллекта USM Systems [3]. Традиционное программное обеспечение должно регулярно обновляться и обновляться по мере появления в цепочке новых вирусов. Проблема в том, что к моменту появления патча новый вирус мог уже поразить критически важные системы. Антивирус требует регулярного обновления сигнатур, это может происходить несколько раз в день, чтобы не отставать от доступных поправок поставщика к известным и новым вирусам. AV-движок также требует обновления, однако чаще всего это происходит ежемесячно или периодически в течение года.

Однако в рамках парадигмы разработки, основанной на искусственный интеллект, после того как система настроена и механизм искусственный интеллект знает, что является нормальным и чего следует ожидать, расширенные инструменты обнаружения аномалий могут отслеживать поведение программы на предмет необычной активности. Затем это запускает процесс быстрой аналитики с последующим удалением и смягчением последствий. И все это происходит, даже если вредоносное ПО не имеет никаких контрольных цифровых подписей прошлых атак. Например, часто такие приложения, как MS Outlook, могут рассматриваться как аномалия в зависимости от операции. Это требует некоторого взаимодействия со стороны конечного пользователя (например, внесения приложения в белый список).

Еще одна область, в которой искусственный интеллект помогает конечным пользователям, – это платформа электронной почты. В настоящее время существуют безопасные системы электронной почты на основе ИИ, как локальные, так и облачные, которые помогают при составлении электронных писем. Это гарантирует, что вы отправляете сообщения правильному получателю, и предотвращаете ложные электронные письма и утечку данных.

Кроме того, это автоматически предотвратит отправку конфиденциальных файлов внешним получателям или даже посоветует использовать соответствующую классификацию и уровень шифрования. Этот процесс также не позволит вам ответить на электронное письмо с потенциально опасной ссылкой, например, на фишинговое электронное письмо, при этом искусственный интеллект будет работать не покладая рук, а не полагаться на то, что пользователи всегда сделают правильный выбор.

Наиболее эффективное использование искусственный интеллект в качестве защитного киберинструмента – противопоставить его правонарушениям, поддерживаемым искусственный интеллект, – по сути, вести огонь огнём. Ключевой проблемой являются боты, управляемые искусственным интеллектом, которые ползают по сетям и другой инфраструктуре в поисках уязвимостей. Эти крошечные объекты, состоящие из автоматизированного кода, составляют теперь большую часть интернет-трафика и могут делать что угодно: от кражи учетных данных до прерывания обмена важными данными. Вот почему многофакторная аутентификация является обязательной [5].

Компании не могут бороться с автоматизированными угрозами только с помощью человеческих действий», – Почему? Потому что, чтобы по-настоящему различать хороших ботов (таких как парсеры поисковых систем), плохих ботов и людей, предприятия должны использовать искусственный интеллект и машинное обучение для всестороннего понимания трафика своего веб-сайта». В этом отношении искусственный интеллект – всего лишь последний виток в продолжающихся кибервойнах. По мере того, как в канал внедряются новые технологии, они принимаются как белыми, так и черными шляпами, чтобы одержать верх.

Некоторые из других полезных областей использования искусственный интеллект в бизнесе сосредоточены на анализе поведения конечных пользователей и внутренних угрозах. Программа узнает, к каким файлам обращаются регулярно и в каких отделах. Примером этого может быть искусственный интеллект, обнаруживший пользователя из отдела ИТ или маркетинга, пытающегося получить доступ к файлу отдела кадров и сообщить о событии. Для сотрудников, которые отправили уведомление, но все еще работают, можно создать часы, чтобы определить, происходит ли доступ к файлам, их перемещение или экспорт.

Однако основная проблема остается: черные шляпы могут одерживать огромные победы в краже данных, нарушении процессов и сеять откровенный страх среди населения на довольно регулярной, хотя и временной основе, но белые шляпы сталкиваются с многочисленными и разнообразными препятствиями в их отслеживании. вниз, разоблачая их сети и привлекая их к ответственности. Пока не появится что-то, что разрушит эту реальность, ожидайте, что ИИ будет одновременно и помощником, и препятствием для безопасности данных и инфраструктуры.

Литература

1. Лэнс Джеймс. Фишинг. Техника компью-терных преступлений. ISBN (EAN): 978-5-477-00572-7, 1-59749-030-X. -M.2008.

2. Mirzaeva M.B. study of neural networks in telecommunication systems. International Conference on Information Science and Communications Technologies Applications, Trends and Opportunies: ICISCT 2021. Tashkent – 2021. 3p

3. Best AI Mobile App Development Company in USA Europe (usmsystems.com).

4. Категории фишинговых атак на копье в 2020 году по типу атаки. Интернет"Киберпреступность и безопасность. https://translated.turbopages.org/

5. Mirzaeva M.B., Sobirov M.A. Estimates of Efficiency and Control Methods of Communication Network Functioning. (IJATCSE) ISSN: 2278-3091, Volume 9, Issue-4, July – August 2020. –P.5736-5740, https://doi.org/10.30534/ijatcse /2020/228942020