УДК 004.8.056:330.34.014

МАШИННОЕ ОБУЧЕНИЕ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: ЗНАЧИМОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ, ОПЫТ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ

А. Ю. Горбукова

студент, Белорусский государственный технологический университет, г. Минск, Беларусь, alinagee@bk.ru

Научный руководитель: **Л. С. Познякова**

ассистент, Белорусский государственный технологический университет, г. Минск, Беларусь, ls.poznyakova@gmail.com

В статье описывается применение машинного обучения в сфере кибербезопасности и защиты персональных данных. Раскрывается тема применения данного вида искусственного интеллекта за рубежом. Описываются перспективы использования машинного обучения в сфере кибербезопасности, а также делаются выводы о том, как внедрение машинного обучения в сферу кибербезопасности может повлиять на безопасность компаний в условиях цифровой экономики.

Ключевые слова: искусственный интеллект; машинное обучение; защита данных; кибербезопасность; цифровая экономика.

MACHINE LEARNING IN THE FIELD OF CYBERSECURITY: IMPORTANCE FOR THE DIGITAL ECONOMY, EXPERIENCE AND PROSPECTS OF USE

A. Y. Gorbukova

student, Belarusian State Technological University, Minsk, Belarus, alinagee@bk.ru

Academic supervisor: **L. S. Poznyakova**

assistant lecturer, Belarusian State Technological University, Minsk, Belarus, ls.poznyakova@gmail.com

The article describes the application of machine learning in the field of cybersecurity and personal data protection. The topic of the application of this type of artificial intelligence abroad is revealed. The prospects of machine learning in the field of cybersecurity are described and also conclusions about how the introduction of machine learning in the field of cybersecurity can affect the security of the digital economy are formulated.

Keywords: Artificial intelligence; machine learning; data protection; cybersecurity; digital economy.

В эпоху формирования и развития цифровой экономики информация и данные становятся ключевыми ресурсами, определяющими успех и конкурентоспособность организаций. Они служат основой для стратегического принятия решений, инноваций и создания добавленной стоимости. Однако с увеличением объемов данных возрастает и необходимость их защиты от киберугроз, которые становятся все более изощренными и разрушительными.

Рост числа кибератак и утечек данных делает очевидной необходимость эффективных решений в области кибербезопасности. В этом контексте машинное обучение открывает новые горизонты для защиты информации. Алгоритмы машинного обучения способны анализировать огромные объемы данных в реальном времени, выявляя аномалии и предсказывая потенциальные угрозы с высокой степенью точности. Это позволяет не только быстро реагировать на инциденты, но и предотвращать их возникновение. Интеграция машинного обучения в системы кибербезопасности становится неотъемлемой частью стратегии защиты данных. В данной статье рассматриваются ключевые аспекты использования машинного обучения для обеспечения безопасности информации в условиях цифровой экономики, а также перспективы и вызовы, связанные с внедрением этих технологий.

За последнее десятилетие роль машинного обучения в обеспечении кибербезопасности постепенно возрастала по мере того, как угрозы организациям становились все более серьезными, а технологии – все более совершенными. Растущая распространенность кибероперaций как экономического и геополитического инструмента означает, что многие организации рискуют стать мишенью хорошо обеспеченных ресурсами злоумышленников и продвинутых постоянных угроз. Очевидным становится тот факт, что компании рискуют повысить свои издержки, связанные с потерей данных и утечкой информации.

Область применения машинного обучения в кибербезопасности чрезвычайно широка. Она охватывает такие задачи, как выявление аномалий и подозрительного поведения, а также обнаружение уязвимостей и устранение известных угроз. Например, Аналитика поведения пользователей и сущностей (UEBA) применяет технологии машинного обучения для анализа данных о поведении и сетевом трафике в режиме реального времени, а также для адекватного реагирования на инциденты [1]. Этот процесс включает в себя повторную аутентификацию пользователя, блокировку атак или оценку уровня риска с последующим уведомлением сотрудников службы информационной безопасности, что позволяет им предпринять необходимые меры.

Другим способом мониторинга систем и сетей на предмет вредоносной активности или нарушения политики является система обнаружения вторжений (IDS). Система предотвращения вторжений (IPS) – это система, связанная с IDS. От первой идеи к более современному виду IDS и IPS пришли в США в 2001 году [2]. Эти системы выполняют обнаружение вторжений и останавливают обнаруженные инциденты. Обе системы используют контролируемые и неконтролируемые методы ML для обнаружения точечных аномалий, контекстуальных аномалий и коллективных аномалий.

Маркетологи активно применяют методы машинного обучения для создания профилей. Ещё шесть лет назад компания «Trustwave» разработала аналитический инструмент с открытым исходным кодом, который использует технологии распознавания лиц для автоматического мониторинга объектов в социальных сетях [3]. Распознавание лиц способствует этому процессу, минимизируя количество ложных срабатываний в результатах поиска и ускоряя обработку данных оператором. Прежде всего, этот инструмент ориентирован на тестировщиков и других профессионалов, которые применяют его для расширения перечня своих целей, например, при анализе сценариев фишинга в социальных сетях. Его ключевым преимуществом является автоматизация процесса сопоставления профилей и возможность генерации отчетов. В условиях, когда индустрия кибербезопасности сталкивается с нехваткой специалистов и быстро эволюционирующими угрозами, крайне важно, чтобы время тестировщиков использовалось с максимальной эффективностью.

На данный момент перспективы развития машинного обучения на постсоветском пространстве огромны. В странах СНГ не так давно вовсе не было решений, связанных с машинным обучением. Уже в 2022 году Центр компетенций НТИ на базе МФТИ оценил рынок искусственного интеллекта в России в 650 миллиардов российских рублей. Аналитики учитывали совокупные доходы компаний, применяющих искусственный интеллект, включая «Яндекс» и VK. Однако выделить из этого объема приложения для обучения или оценить вклад компьютерного зрения и моделей для анализа естественного языка невозможно [4].

Таким образом, внедрение машинного обучения в сферу кибербезопасности является критически важным шагом для повышения уровня защиты информационных систем компаний в условиях развития цифровой экономкии. Машинное обучение позволяет улучшить обнаружение угроз, автоматизировать процессы реагирования и предсказывать потенциальные атаки, что существенно повышает эффективность защиты данных.

Библиографические ссылки

1. *Micah Musser, Ashton Gariott.* Machine Learning and Cybersecurity: Hype and Reality [Электронный ресурс] / CSET (дата обращения: 10.09.2024).

2. Система обнаружения вторжений [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Система_обнаружения_вторжений (дата обращения: 11.09.2024).

3. Mapping Social Media with Facial Recognition: A New Tool for Penetration Testers and Red Teamers [Электронный ресурс]. URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/mapping-social-media-with-facial-recognition-a-new-tool-for-penetration-testers-and-red-teamers/ (дата обращения: 12.09.2024).

4. Искусственный интеллект. Тренды РБК [Электронный ресурс]. URL: https://plus.rbc.ru/news/638ce84d7a8aa9f0b9bff8fd (дата обращения: 13.09.2024).