Сычев Д.И. Искусственный интеллект и кибербезопасность: будущие тенденции и вызовы // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 9–14

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ: БУДУЩИЕ ТЕНДЕНЦИИ И ВЫЗОВЫ

Сычев Д.И.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: s.denis_2001@mail.ru

В этой статье исследуется сложная взаимосвязь между искусственным интеллектом (ИИ) и кибербезопасностью с акцентом на будущие тенденции и проблемы, которые могут ждать впереди. В начале представляется краткое введение в ИИ и кибербезопасность, их историческое взаимодействие, после чего следует подробное обсуждение будущих тенденций, включая обнаружение и реагирование на угрозы с помощью ИИ, автоматизированный взлом, роль ИИ в конфиденциальности и защите данных, а также потенциальное влияние квантовые вычисления по искусственному интеллекту и кибербезопасности.
Также в статье рассматриваются потенциальные проблемы, такие как проблемы этики и конфиденциальности, уязвимости из-за чрезмерной зависимости от ИИ, проблемы предвзятости в ИИ и необходимость идти в ногу с последними достижениями в области искусственного интеллекта. Приведены реальные примеры из практики, чтобы проиллюстрировать возможности и сложности внедрения инструмента ИИ в кибербезопасность.

Ключевые слова: Искусственный интеллект, кибербезопасность, безопасность данных.

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: FUTURE TRENDS AND CHALLENGES

Sychev D.I.
St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, Bolshevikov Ave., 22, room 1), e-mail: s.denis_2001@mail.ru

This article explores the complex relationship between artificial intelligence (AI) and cybersecurity with an emphasis on future trends and challenges that may lie ahead. At the beginning, a brief introduction to AI and cybersecurity, their historical interaction is presented, followed by a detailed discussion of future trends, including AI threat detection and response, automated hacking, the role of AI in privacy and data protection, as well as the potential impact of quantum computing on artificial intelligence and cybersecurity.
The article also addresses potential issues such as ethics and privacy issues, vulnerabilities due to over-reliance on AI, issues of bias in AI, and the need to keep up with the latest advances in artificial intelligence. Real-world examples from practice are given to illustrate the possibilities and difficulties of implementing an AI tool in cybersecurity.

Keywords: Artificial intelligence, cybersecurity, data security.

Введение

В эпоху повсеместной цифровизации технологии продолжают развиваться с поразительной скоростью, коренным образом меняя то, как мы живем, работаем и общаемся. Два важнейших аспекта этой технологической революции — искусственный интеллект (ИИ) и кибербезопасность. В то время как ИИ имитирует процессы человеческого интеллекта посредством обучения, рассуждений и исправлений, кибербезопасность направлена на защиту систем, сетей и данных от цифровых атак. Пересечение, на котором встречаются эти две преобразующие технологии, обладает значительным потенциалом для формирования будущего цифровой безопасности. В этой статье рассматриваются развивающиеся связь между ИИ и кибербезопасностью, исследуются их будущие тенденции и проблемы, которые ждут впереди [1-2].

Искусственный интеллект прошел долгий путь с момента своего концептуального зарождения, от простых систем, основанных на правилах, до сложных моделей машинного и глубокого обучения. За прошедшие годы искусственный интеллект проник в различные области, включая кибербезопасность. С ростом взаимосвязанности систем и ростом производства данных, традиционных мер кибербезопасности уже недостаточно. Сложность и изощренность киберугроз растет, а ориентироваться в среде кибербезопасности становится все труднее.

Интеграция искусственного интеллекта в кибербезопасность представляет собой изменение парадигмы в том, как мы обнаруживаем киберугрозы и реагируем на них. Способность ИИ учиться на прошлых инцидентах, адаптироваться к новым ситуациям и делать прогнозы идеально соответствует требованиям современной кибербезопасности. Инструменты искусственного интеллекта могут анализировать огромные объемы данных для обнаружения угроз, автоматизировать реагирование и даже прогнозировать будущие тенденции атак. Несмотря на эти достижения, использование ИИ в кибербезопасности все еще находится на начальной стадии, и множество возможностей еще не изучено.

1. Будущие тенденции

1.1. Обнаружение угроз и реагирование на них с помощью ИИ

В динамичном мире кибербезопасности обнаружение угроз и реагирование на них должны быть быстрыми и точными. Возможности ИИ играют важную роль в достижении этого. Алгоритмы машинного обучения могут анализировать огромное количество данных в режиме реального времени и выявлять закономерности или аномалии, которые могут указывать на угрозу.

Эти модели ИИ становятся все более изощренными, извлекая уроки из каждого взаимодействия и улучшая свои прогностические возможности. Они могут понимать цифровую среду, определять нормальное поведение и отмечать аномалии, которые могут указывать на потенциальные киберугрозы. ИИ также может автоматизировать реагирование на эти угрозы, сокращая время отклика и потенциально предотвращая ущерб.

Отличным примером обнаружения угроз с помощью ИИ является использование аналитики поведения пользователей и объектов (UEBA). Инструменты UEBA используют машинное обучение для понимания нормального поведения пользователей и сущностей в системе. Любое отклонение от этого «нормального» поведения помечается как потенциальная угроза, что позволяет быстро реагировать [3-4].

1.2. Механизмы автоматизированного взлома и защиты на основе ИИ

Искусственный интеллект является мощным инструментом в сфере кибербезопасности. С одной стороны, он способен значительно укрепить безопасность хранения данных, однако, он также может быть использован для автоматизации и уточнения попыток взлома.

Хакерские инструменты на базе ИИ могут выполнять атаки с повышенной скоростью и точностью, что делает их более эффективными и трудными для обнаружения. Эта тенденция вызывает тревогу у специалистов по кибербезопасности, поскольку может привести к увеличению частоты и серьезности кибератак.

Однако, стоит отметить, что ИИ также может сыграть важную роль в разработке передовых защитных механизмов. Например, ИИ можно использовать в «этическом взломе» или «красной команде», когда он используется для проверки систем на наличие уязвимостей, а затем исправляет слабые места, прежде чем злоумышленник успеет ими воспользоваться. Этот упреждающий подход к кибербезопасности может изменить правила игры, потенциально позволяя на шаг опережать злоумышленников.

1.3. ИИ в конфиденциальности и защите данных

Еще одна новая тенденция — роль ИИ в защите данных и конфиденциальности. С ростом ценности данных в современном мире защита личной и конфиденциальной информации никогда не была более важной [5].

ИИ может помочь автоматизировать процесс защиты данных и обеспечить соблюдение правил конфиденциальности, таких как Общий регламент по защите данных (GDPR). Инструменты искусственного интеллекта можно использовать для отслеживания утечек данных, обнаружения несанкционированного доступа к персональным данным и обеспечения того, чтобы методы хранения и обработки данных соответствовали нормативным стандартам.

Кроме того, искусственный интеллект может помочь в разработке более надежных алгоритмов шифрования для защиты данных во время передачи и хранения. Возможность использования ИИ для передовых методов шифрования может стать значительным шагом вперед в обеспечении конфиденциальности и целостности данных.

1.4. Квантовые вычисления и кибербезопасность

Появление квантовых вычислений представляет собой новый рубеж для ИИ и кибербезопасности. Квантовые компьютеры с их необычайной вычислительной мощностью потенциально могут сломать традиционные методы шифрования, что создает значительный риск для кибербезопасности.

Однако квантовая технология также предоставляет возможности для повышения кибербезопасности. Квантовое шифрование, или квантовое распределение ключей, обещает «невзламываемой» системы хранения данных, используя принципы квантовой механики. Это может произвести революцию в области безопасной связи.

Но интеграция квантовых вычислений и ИИ в кибербезопасность все еще находится на ранней стадии, и для полного понимания и использования этого потенциала необходимо провести много исследований [6-8].

2. Вызовы и проблемы

2.1. Вопросы этики и конфиденциальности

Хотя потенциал ИИ для повышения кибербезопасности неоспорим, он также вызывает проблемы этики и конфиденциальности. Например, в своей роли в мониторинге и анализе данных для обнаружения потенциальных угроз ИИ может нарушать права людей на неприкосновенность частной жизни.

Более того, алгоритмы ИИ хороши ровно настолько, насколько хороши данные, на которых они обучаются, и если эти данные содержат предвзятую или конфиденциальную информацию, это может привести к серьезным этическим проблемам. Поэтому крайне важно обеспечить прозрачность и подотчетность систем ИИ, используемых в кибербезопасности.

2.2. Зависимость от ИИ и потенциальных уязвимостей

Поскольку мы все больше полагаемся на ИИ для обеспечения кибербезопасности, мы также подвергаем себя новым уязвимостям. Если система ИИ будет скомпрометирована, результаты могут быть катастрофическими, поскольку злоумышленники могут получить доступ к конфиденциальным данным или контроль над критически важными системами.

Обеспечение безопасности самих систем ИИ является серьезной проблемой. Это включает в себя не только защиту системы от внешних атак, но и обеспечение того, чтобы алгоритмы ИИ не могли быть использованы для злонамеренного поведения.

2.3. Предвзятость ИИ и кибербезопасность

Системы ИИ учатся на данных, на которых они обучаются, и если эти данные содержат предубеждения, ИИ может перенять эти предубеждения, что приведет к несправедливым или неточным результатам. В контексте кибербезопасности это может означать, что определенные типы угроз игнорируются или что невинное поведение помечается как подозрительное.

Преодоление предвзятости в ИИ является серьезной проблемой. Это требует тщательного сбора и обработки данных, тщательного тестирования моделей ИИ и постоянного мониторинга для обеспечения справедливости и точности.

2.4. Задача идти в ногу с достижениями ИИ

ИИ — это быстро развивающаяся область, и идти в ногу с последними разработками может быть сложно. Специалисты по кибербезопасности должны постоянно учиться и адаптироваться, чтобы эффективно использовать ИИ и защищаться от угроз, связанных с ИИ. Этот спрос на постоянное обучение и развитие может стать серьезной проблемой, особенно в сфере, где ставки так высоки.

3. Тематические исследования

Ниже рассматриваются два реальных случая, которые иллюстрируют потенциал и проблемы ИИ в кибербезопасности.

Пример 1: ИИ в обнаружении угроз

Darktrace, ведущая компания искусственного интеллекта в области кибербезопасности, использует машинное обучение для обнаружения киберугроз, реагирования на них и смягчения их последствий в режиме реального времени. Их технология искусственного интеллекта, известная как «Иммунная система предприятия», изучает, что является

нормальным в сети, а затем может идентифицировать и реагировать на необычную активность, которая отклоняется от этого «образца жизни».

Способность системы быстро и автономно реагировать на угрозы оказалась очень эффективной. В одном из случаев он обнаружил и остановил атаку программы-вымогателя за считанные секунды, предотвратив значительную потерю данных и нарушение работы.

Пример 2: ИИ и кибератаки

В 2020 году компания Cybereason, занимающаяся кибербезопасностью, сообщила о кампании кибератак, которую они назвали «кибератакой с использованием ИИ». Злоумышленники использовали ИИ для автоматизации создания вредоносных электронных писем, что позволило им рассылать фишинговые электронные письма в гораздо большем объеме и с более убедительным содержанием, чем это было бы возможно вручную.

Этот случай иллюстрирует возможность использования ИИ киберпреступниками, подчеркивая важность разработки передовых защитных механизмов на основе ИИ.

Вывод

Отношения между ИИ и кибербезопасностью сложны и развиваются. Как было рассмотрено выше, ИИ обладает значительным потенциалом для повышения кибербезопасности, от обнаружения угроз и реагирования до защиты данных и конфиденциальности. Однако мы также должны решать серьезные проблемы, включая проблемы этики и конфиденциальности, потенциальные уязвимости и необходимость идти в ногу с быстрым технологическим прогрессом.

По мере того, как мы движемся в будущее, становится ясно, что ИИ будет играть все более важную роль в кибербезопасности. Непрерывные исследования, инвестиции и бдительность будут иметь решающее значение для использования преимуществ ИИ при одновременном снижении потенциальных рисков и решении проблем.

Кажется, впереди предстоит захватывающий путь, где симбиоз между ИИ и кибербезопасностью будет продолжать переопределять границы возможного в цифровой безопасности.

Список литературы

1. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
2. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
3. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
4. Пестов И. Е., Христофоров Р. О., Швидкий А. А. Анализ подходов к разработке облачных сервисов// Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 752-757.
5. Красов А. В. и др. Построение доверенной вычислительной среды. – 2019.

6. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 438-440.
7. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022. – №. 4s. – С. 92-101.
8. Гельфанд А. М. и др. Интернет вещей (iot): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.

References

1. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. - 2021. - pp. 33-37.
2. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for automation of software testing // Naukosphere. – 2020. – no. 6. - pp. 152-156.
3. Kosov N. A., Timofeev R. S. Comparison of training methods for convolutional neural networks // Actual problems of infotelecommunications in science and education (APINO 2021). - 2021. - pp. 526-530.
4. Pestov I. E., Khristoforov R. O., Shvidkiy A. A. Analysis of approaches to the development of cloud services // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 752-757.
5. Krasov A. V. et al. Construction of a trusted computing environment. – 2019.
6. Gelfand A. M. et al. Applications of big data analytics in critical information infrastructures // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 438-440.
7. Krasov A. V. et al. Actual threats to the security of information in the field of healthcare and ophthalmology // OPHTHALMOSHURGY. – 2022. – no. 4s. - pp. 92-101.
8. Gelfand A. M. et al. Internet of things (iot): threats to security and privacy // Actual problems of infotelecommunications in science and education (APINO 2021). - 2021. - pp 215-220.