Международный журнал прикладных наук и технологий "Integral"

Научная статья

Original article

УДК 004.891.3

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

ARTIFICIAL INTELLIGENCE IN THE FIELD OF CYBERSECURITY

Дударев Кирилл Сергеевич, Студент 3-го курса, Передовая Инженерная школа Союзного государства ФГБОУ ВО «Псковский государственный университет» (180000, Россия, Псковская область, г. Псков, пл. Ленина, д.2), тел. +7 8112 20-16-99, dkira2310@gmail.com

Ерофеев Олег Николаевич, Студент 3-го курса, Передовая Инженерная школа Союзного государства ФГБОУ ВО «Псковский государственный университет» (180000, Россия, Псковская область, г. Псков, пл. Ленина, д.2), тел. +7 8112 20-16-99, oleg12122000@yandex.ru

Иванов Николай Александрович, Студент 3-го курса, Передовая Инженерная школа Союзного государства ФГБОУ ВО «Псковский государственный университет» (180000, Россия, Псковская область, г. Псков, пл. Ленина, д.2), тел. +7 8112 20-16-99, n.ivanov.r60@gmail.com

Вертешев Антон Сергеевич, кандидат экономических наук, доцент отделения информационно-коммуникационных технологий, Передовая Инженерная школа Союзного государства ФГБОУ ВО «Псковский государственный университет (180000, Россия, Псковская область, г. Псков, пл. Ленина, д.2) +79532332417, https://orcid.org/my-orcid?orcid=0000-0002-9261-8427, a_verteshev@mail.ru

Dudarev Kirill Sergeevich, 3rd year student, Advanced Engineering School of the Union State, Pskov State University (180000, Russia, Pskov region, Pskov, Lenin Square, 2), tel. +7 8112 20-16-99, dkira2310@gmail.com

Oleg Nikolaevich Yerofeev, 3rd year student, Advanced Engineering School of the Union State, Pskov State University (180000, Russia, Pskov region, Pskov, Lenin Square, 2), tel. +7 8112 20-16-99, oleg12122000@yandex.ru

Ivanov Nikolay Alexandrovich, 3rd year student, Advanced Engineering School of the Union State of Pskov State University (180000, Russia, Pskov region, Pskov, Lenin Square, 2), tel. +7 8112 20-16-99, n.ivanov.r60@gmail.com

Verteshev Anton Sergeevich, PhD in Economics, Associate Professor of the Department of Information and Communication Technologies, Advanced Engineering School of the Union State, Pskov State University (180000, Russia, Pskov Region, Pskov, Lenin Square, 2) +79532332417, https://orcid.org/my-orcid?orcid=0000-0002-9261-8427, a_verteshev@mail.ru

Аннотация: Статья рассматривает роль искусственного интеллекта (ИИ) в обеспечении кибербезопасности, подчеркивая его значимость в современном цифровом мире. Описывая методы использования ИИ, авторы рассматривают машинное обучение, анализ поведения и автоматизированные системы детекции в контексте обнаружения и предотвращения кибератак. Статья также подчеркивает преимущества, такие как улучшенная точность обнаружения и сокращение времени реакции, одновременно обсуждая вызовы, включая этические вопросы и сложность объяснения решений ИИ в кибербезопасности. В целом, статья предлагает глубокий анализ современных тенденций и перспектив развития сферы кибербезопасности с применением искусственного интеллекта.

Abstract: The article examines the role of artificial intelligence (AI) in ensuring cybersecurity, emphasizing its importance in the modern digital world. Describing the methods of using AI, the authors consider machine learning, behavior analysis and automated detection systems in the context of detecting and preventing cyberattacks.

The article also highlights benefits such as improved detection accuracy and reduced reaction time, while discussing challenges including ethical issues and the difficulty of explaining AI solutions in cybersecurity. In general, the article offers an in-depth analysis of current trends and prospects for the development of cybersecurity using artificial intelligence.

Ключевые слова: Искусственный интеллект, кибербезопасность, машинное обучение, анализ поведения, системы детекции вторжений, обнаружение кибератак, преимущества ИИ в безопасности, вызовы кибербезопасности, этические вопросы ИИ, автоматизированная реакция на инциденты.

Keywords: Artificial intelligence, cybersecurity, machine learning, behavior analysis, intrusion detection systems, cyberattack detection, AI security benefits, cybersecurity challenges, AI ethical issues, automated incident response.

Введение

В последние десятилетия цифровая трансформация привела к радикальным изменениям в обществе и бизнесе. С ростом объемов данных и зависимости от цифровых технологий возросли и вызовы в области кибербезопасности. В этой постоянной борьбе с киберугрозами искусственный интеллект (ИИ) выступает в роли надежного союзника, обеспечивая эффективные средства защиты и предотвращения кибератак.

ИИ в сфере кибербезопасности привносит инновационные методы анализа, обнаружения и реагирования на угрозы, ранее недоступные. От машинного обучения до анализа поведения, эти технологии становятся неотъемлемой частью стратегий киберзащиты, способствуя повышению эффективности и точности выявления потенциальных рисков[1].

В настоящей статье мы рассмотрим, как искусственный интеллект трансформирует ландшафт кибербезопасности, предоставляя новые инструменты и перспективы для борьбы с современными киберугрозами. Разберем, какие методы применяются для предотвращения атак, какие

преимущества приносит использование ИИ в этой сфере, а также рассмотрим вызовы и перспективы будущего развития этой захватывающей области.

Кибербезопасность: Текущая обстановка и растущие угрозы

Современная информационная безопасность сталкивается с постоянно эволюционирующими и сложными угрозами, требующими инновационных подходов к обеспечению защиты. Актуальность применения искусственного интеллекта (ИИ) в информационной безопасности нельзя переоценить, поскольку технологии ИИ предоставляют уникальные возможности для более эффективного выявления, предотвращения и реагирования на кибератаки[2].

Проблематика защиты от киберугроз заключена в множестве факторов:

1. **Сложность и масштаб угроз:** Современные киберугрозы становятся все более сложными, используют новые методы атак и охватывают широкий спектр уязвимостей. ИИ предоставляет возможность более глубокого анализа и обработки данных для выявления скрытых угроз и аномалий.
2. **Скорость атак и требования к реакции:** Кибератаки происходят в реальном времени, требуя моментальной реакции. ИИ способен обеспечить автоматизированную и быструю реакцию на угрозы, ускоряя процесс предотвращения и минимизации ущерба.
3. **Обработка больших объемов данных:** С ростом объемов данных, собираемых в рамках кибербезопасности, становится необходимым использовать технологии, способные обрабатывать и анализировать большие объемы информации. ИИ позволяет эффективно анализировать, классифицировать и извлекать полезную информацию из больших данных.
4. **Изменчивость угроз:** Технологии ИИ способны адаптироваться к постоянно меняющимся методам атак, что делает их более эффективными в выявлении новых и неизвестных угроз.
5. **Минимизация человеческого фактора:** Ошибка человека может стать слабым звеном в системе безопасности. Использование ИИ позволяет

автоматизировать процессы мониторинга и реагирования, снижая вероятность человеческих ошибок.

6. **Прогнозирование и проактивное реагирование:** ИИ способен анализировать данные, выявлять тенденции и предсказывать потенциальные угрозы, что позволяет принимать меры по их предотвращению до активации.

В совокупности эти факторы подчеркивают актуальность использования искусственного интеллекта в обеспечении информационной безопасности, предоставляя новые возможности для более эффективной защиты от современных угроз[4].

Внедрение искусственного интеллекта в сферу информационной безопасности представляет собой значительный шаг вперед в обеспечении кибербезопасности. Научная новизна данного направления проявляется в нескольких ключевых аспектах:

1. **Алгоритмы машинного обучения и глубокого обучения:** Новейшие методы машинного обучения, включая глубокое обучение, позволяют анализировать и понимать сложные паттерны и зависимости в данных. Это особенно полезно для выявления неявных угроз, которые трудно обнаружить с использованием традиционных методов[3].

2. **Автоматическое обучение и адаптация к новым угрозам:** Искусственный интеллект в области безопасности обладает способностью автоматического обучения на основе новых данных о киберугрозах. Это позволяет системам быстро адаптироваться к изменяющейся угрозовой среде и выявлять ранее неизвестные атаки.

3. **Комбинирование данных из различных источников:** Использование ИИ позволяет эффективно интегрировать и анализировать данные из различных источников, таких как системы журналирования, сетевой трафик, антивирусные программы и многое другое. Это дает возможность создания комплексной картины безопасности и выявления тонких связей между различными событиями[7].

4. **Прогнозирование и предупреждение:** Системы ИИ могут не только выявлять текущие угрозы, но и предсказывать потенциальные атаки на основе анализа тенденций и истории. Это позволяет предпринимать проактивные меры по предотвращению угроз до их активации.

5. **Интеллектуальные системы реагирования:** Новаторские технологии позволяют создавать интеллектуальные системы реагирования на инциденты, которые способны автоматически принимать решения и предпринимать меры для сдерживания атак в реальном времени.

6. **Анализ поведения и контекста:** ИИ обеспечивает возможность анализа поведения пользователей и сетевого трафика в контексте конкретных сценариев. Это позволяет выявлять подозрительные активности, не ограничиваясь заранее определенными сигнатурами угроз.

Новые горизонты защиты

Искусственный интеллект преобразовывает подходы к кибербезопасности, предоставляя множество методов, способных эффективно бороться с современными киберугрозами. В этом разделе мы рассмотрим ключевые методы использования ИИ, которые революционизируют обнаружение и предотвращение кибератак.

1. Машинное обучение для обнаружения вредоносного ПО:

Алгоритмы машинного обучения анализируют характеристики вредоносных программ и выявляют их на основе уникальных паттернов. Это обеспечивает более точное и быстрое обнаружение новых видов вредоносных атак, даже в случае, когда они ранее не были известны[6].

2. Анализ аномалий и поведенческое моделирование:

Системы ИИ анализируют обычное поведение пользователей и сетевого трафика, строят модели и выявляют аномалии, которые могут свидетельствовать о потенциальных атаках. Поведенческое моделирование позволяет создавать детальные профили активности и эффективно выявлять отклонения от нормы.

3. Применение ИИ в системах детекции и предотвращения вторжений:

Искусственный интеллект активно применяется в системах детекции и предотвращения вторжений (IDS/IPS). Это включает в себя использование алгоритмов машинного обучения для выявления подозрительной активности и блокировки потенциальных угроз перед тем, как они смогут причинить вред.

4. Автоматизированная реакция на инциденты:

Системы автоматизированной реакции на инциденты, поддерживаемые ИИ, могут быстро реагировать на обнаруженные угрозы, принимая меры для предотвращения их распространения и минимизации ущерба. Это снижает зависимость от человеческого вмешательства и сокращает время реакции на минимум.

5. Прогнозирование и анализ угроз:

ИИ предоставляет способности прогнозирования возможных угроз на основе анализа больших данных. Это позволяет организациям принимать меры по предотвращению потенциальных атак и укреплению своей кибербезопасности.

6. Использование ИИ в анализе событий безопасности:

Системы ИИ способны обрабатывать огромные объемы данных, связанных с безопасностью, и проводить глубокий анализ событий. Это помогает выявлять неявные связи между различными инцидентами, повышая общую эффективность мер безопасности[9].

Эффективное использование этих методов позволяет создавать более устойчивые и адаптивные системы кибербезопасности, готовые отвечать на вызовы современных цифровых угроз. В следующих разделах мы рассмотрим конкретные примеры и успехи применения этих методов в практике.

Методы обеспечения кибербезопасности

Для достижения поставленных целей и решения задач в области кибербезопасности с использованием искусственного интеллекта применяются разнообразные методы исследования. Важными компонентами этих методов являются технологии машинного обучения, глубокого обучения, анализа данных

и разработка интеллектуальных систем. Ниже перечислены основные методы, которые используются в данной области:

1. **Машинное обучение (МО):** является ключевым методом, используемым для обучения систем ИИ распознавать угрозы, выявлять аномалии и прогнозировать потенциальные атаки. Такие модели могут обучаться на основе исторических данных о безопасности для создания алгоритмов обнаружения аномалий[10].

2. **Глубокое обучение:** представляет собой разновидность машинного обучения, использующую искусственные нейронные сети для анализа сложных данных и выявления неявных закономерностей. Позволяет создавать модели, способные распознавать вредоносные программы на основе их поведения.

3. **Анализ больших данных:** обработка и анализ больших объемов данных о безопасности с использованием технологий и методов, способствующих выявлению паттернов и трендов. Так, например, возможно анализировать сетевой трафик и журналы событий для выявления аномалий и индикации кибератак.

4. **Системы обнаружения и предотвращения вторжений (IDS/IPS):** применение систем обнаружения и предотвращения вторжений для автоматического обнаружения и блокировки атак. Так ИИ может использоваться в системах IDS/IPS для обучения моделей на основе поведения злоумышленников.

5. **Обработка естественного языка (NLP):** применение методов обработки естественного языка для анализа и понимания текстовой информации, такой как отчеты о безопасности и угрозы для создания систем NLP для автоматического анализа текстовых данных о атаках и уязвимостях.

6. **Симуляция кибератак:** использование симуляторов атак для тестирования систем безопасности и обучения персонала, создание сценариев атак с использованием ИИ для оценки уровня готовности систем безопасности.

Эти методы исследования представляют собой многогранный подход к применению искусственного интеллекта в обеспечении информационной безопасности.

Вызовы и ограничения

Несмотря на значительные преимущества, с которыми обладает искусственный интеллект в сфере кибербезопасности, существуют вызовы и ограничения, которые требуют внимания и постоянного улучшения технологий[8]. Рассмотрим некоторые из основных проблем, с которыми сталкиваются специалисты в данной области.

1. Недостатки в обучающих данных:

Эффективность систем ИИ напрямую зависит от качества обучающих данных. Недостатки или предвзятость в данных могут привести к неправильному обучению алгоритмов и, как следствие, к ошибкам в обнаружении угроз.

2. Угрозы атак на системы искусственного интеллекта:

Преступники могут использовать те же технологии искусственного интеллекта, чтобы создавать более изощренные и сложные атаки. Это включает в себя возможность обхода алгоритмов обнаружения и внедрения вредоносного программного обеспечения, спроектированного для обмана систем ИИ.

3. Проблемы конфиденциальности и этические вопросы:

Сбор и обработка больших объемов данных в кибербезопасности могут поднимать вопросы о конфиденциальности. Правильное использование и защита персональных данных становятся ключевыми аспектами, требующими баланса между безопасностью и правами человека[5].

4. Сложность объяснения решений ИИ:

Некоторые алгоритмы машинного обучения могут быть сложными для понимания и объяснения. Это создает проблемы, особенно в области кибербезопасности, где требуется ясность в принятых решениях для эффективного реагирования на инциденты.

5. Необходимость постоянного обучения:

Преступники постоянно совершают инновационные атаки, и системы ИИ должны быть постоянно обучаемыми, чтобы оставаться актуальными и эффективными. Это требует значительных усилий по поддержке и обновлению систем.

6. Вызовы в интеграции с существующими системами:

Интеграция технологий ИИ с уже существующими системами безопасности может быть сложной задачей, особенно в случаях, когда необходимо обеспечить совместимость и бесперебойную работу.

7. Высокие требования к вычислительным ресурсам:

Многие алгоритмы машинного обучения требуют значительных вычислительных ресурсов. Это может создавать проблемы, особенно для малых организаций или тех, кто сталкивается с ограничениями бюджета.

Решение этих вызовов и ограничений требует комплексного подхода, включая совершенствование алгоритмов, усовершенствование инфраструктуры, ужесточение правил конфиденциальности и улучшение процессов обучения и обновления систем ИИ.

Заключение:

Использование искусственного интеллекта в сфере кибербезопасности приводит к существенному улучшению эффективности систем защиты от современных киберугроз.

Методы машинного обучения и глубокого обучения позволяют системам ИИ адаптироваться к появляющимся новым угрозам, что особенно важно в условиях постоянно меняющегося киберландшафта. Системы, основанные на искусственном интеллекте, не только реагируют на текущие угрозы, но и способны прогнозировать потенциальные атаки, что дает возможность предпринимать меры по их предотвращению.

Внедрение ИИ в кибербезопасность сокращает роль человеческого фактора, что уменьшает вероятность ошибок и повышает общий уровень безопасности. Системы ИИ способны к обучению на новых данных и адаптации к изменяющимся условиям, что делает их более гибкими и эффективными.

Формирование новых горизонтов в обеспечении информационной безопасности при помощи искусственного интеллекта подчеркивает необходимость дальнейших исследований и инноваций в данной области для обеспечения надежной защиты в условиях постоянно меняющейся среды информационных технологий.

Список используемой литературы

1. Rosenzweig, P. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. *Penguin.*
2. Dunn Cavelty, M., & Mauer, V. (2019). The Routledge Handbook of Security Studies. *Routledge.*
3. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521(7553), 436-444*
4. Dhillon, G., & Backhouse, J. (2001). Information system security management in the new millennium. *Communications of the ACM, 44(7), 125-128.*
5. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.*
6. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *National Institute of Standards and Technology (NIST) Special Publication 800-94.*
7. Swamy, M. N. S., Thangavel, K., & Tan, K. (2018). Artificial intelligence in cybersecurity: A comprehensive survey. *Journal of King Saud University-Computer and Information Sciences.*
8. Clarke, R., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. *HarperCollins.*
9. Schroeder, H., & Lotfizadeh, N. (2019). Cybersecurity: The Beginner's Guide. *Packt Publishing.*
10. Liao, Q., Yang, F., & Wang, H. (2019). A survey of deep learning techniques in cyber security. *Computers, Materials & Continua, 60(3), 1019-1042.*

References

1. Rosenzweig, P. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. *Penguin.*
2. Dunn Cavelty, M., & Mauer, V. (2019). The Routledge Handbook of Security Studies. *Routledge.*
3. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521(7553), 436-444*
4. Dhillon, G., & Backhouse, J. (2001). Information system security management in the new millennium. *Communications of the ACM, 44(7), 125-128.*
5. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.*
6. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *National Institute of Standards and Technology (NIST) Special Publication 800-94.*
7. Swamy, M. N. S., Thangavel, K., & Tan, K. (2018). Artificial intelligence in cybersecurity: A comprehensive survey. *Journal of King Saud University-Computer and Information Sciences.*
8. Clarke, R., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. *HarperCollins.*
9. Schroeder, H., & Lotfizadeh, N. (2019). Cybersecurity: The Beginner's Guide. *Packt Publishing.*
10. Liao, Q., Yang, F., & Wang, H. (2019). A survey of deep learning techniques in cyber security. *Computers, Materials & Continua, 60(3), 1019-1042.*

Для цитирования: Дударев К.С., Ерофеев О.Н. Иванов Н.А. Искусственный интеллект в сфере кибербезопасности// Научный сетевой журнал «Столыпинский вестник» №1/2024.