Перевертун Д.Р. Роль искусственного интеллекта в информационной безопасности // Международный журнал информационных технологий и энергоэффективности. - 2024. – Т. 9 № 5(43) с. 92–97

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

В статье рассматривается роль искусственного интеллекта (ИИ) в сфере информационной безопасности, охватывая его использование для обнаружения и предотвращения кибератак, анализа и классификации вредоносного программного обеспечения, а также прогнозирования будущих угроз. Освещаются преимущества, возможности и перспективы применения ИИ, включая повышение эффективности защиты информационных систем и адаптацию к эволюционирующему ландшафту угроз. Однако статья также подчеркивает существующие риски и проблемы, связанные с приватностью, этическими вопросами и потенциалом злоупотреблений.

Ключевые слова: Искусственный интеллект, информационная безопасность, кибератаки, вредоносное ПО, прогнозирование угроз, машинное обучение, управление рисками, этические вопросы, приватность данных, обучение специалистов, международное сотрудничество.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article examines the role of artificial intelligence (AI) in the field of information security, covering its use to detect and prevent cyber attacks, analyze and classify malicious software, as well as predict future threats. The advantages, opportunities and prospects of AI application are highlighted, including increasing the effectiveness of information system protection and adaptation to the evolving threat landscape. However, the article also highlights the existing risks and challenges related to privacy, ethical issues and the potential for abuse.

Keywords: Artificial intelligence, information security, cyber attacks, malware, threat forecasting, machine learning, risk management, ethical issues, data privacy, training of specialists, international cooperation.

Искусственный интеллект может быть использован в информационной безопасности для решения различных задач, включая обнаружение угроз, анализ и классификацию вредоносного ПО, а также прогнозирование и предотвращение кибератак. Системы на основе ИИ способны анализировать большие объемы данных в реальном времени, выявляя сложные и скрытые угрозы, что значительно повышает эффективность защиты информационных систем.

Одним из основных направлений применения ИИ в информационной безопасности является обнаружение угроз. Алгоритмы машинного обучения могут обучаться на исторических данных о кибератаках, что позволяет им эффективно распознавать потенциально опасные действия в сети. Такие системы способны не только обнаруживать известные виды атак, но и предсказывать новые, еще неизвестные угрозы, адаптируясь к постоянно меняющемуся ландшафту кибербезопасности.

Одним из наиболее перспективных направлений использования искусственного интеллекта в области информационной безопасности является обнаружение и предотвращение угроз. Искусственный интеллект вносит значительный вклад в повышение эффективности и актуальности мер по обеспечению кибербезопасности, адаптируясь к постоянно меняющемуся ландшафту угроз.

Системы на основе ИИ способны анализировать огромные объемы данных в реальном времени, что включает в себя трафик сети, журналы операций, а также разнообразные внешние источники информации. Этот анализ позволяет выявлять аномалии и нестандартное поведение, которые могут указывать на попытку несанкционированного доступа, распространение вредоносного ПО или другие виды кибератак.[5] Основываясь на обнаруженных данных, ИИ может с высокой степенью точности определить потенциальную угрозу, даже если она маскируется под легитимные процессы или использует ранее неизвестные методы атаки.

Благодаря способности к обучению, системы ИИ с течением времени становятся только эффективнее в определении угроз, учитывая новые вирусные сигнатуры, тактики, техники и процедуры, используемые киберпреступниками. Это позволяет не только реагировать на текущие угрозы, но и прогнозировать потенциальные атаки, адаптируя защитные механизмы в соответствии с изменениями в поведении атакующих.

Таким образом, внедрение искусственного интеллекта в системы обнаружения и предотвращения угроз позволяет значительно повысить уровень защищенности информационных систем, сократить время на обнаружение и нейтрализацию атак, а также оптимизировать процессы принятия решений в области кибербезопасности.[3] Это становится особенно важным в условиях постоянно растущего количества угроз и их сложности, где традиционные методы защиты уже не способны обеспечить должный уровень безопасности.

Системы ИИ также находят применение в анализе и классификации вредоносного программного обеспечения. Используя методы глубокого обучения, они могут анализировать поведение ПО, выявлять скрытые вредоносные функции и даже предсказывать потенциальное поведение нового ПО на основе сходства с уже известными вирусами и троянами.

Применение искусственного интеллекта в анализе и классификации вредоносного программного обеспечения является одним из наиболее важных направлений в области кибербезопасности. Развитие технологий ИИ позволило создать системы, способные самостоятельно обучаться на основе анализа больших объемов данных, что значительно увеличивает их эффективность в распознавании и классификации вредоносного ПО.

Данные системы используют различные методы машинного обучения, включая обучение с учителем, без учителя и обучение с подкреплением, для анализа поведенческих паттернов, сигнатур и других характеристик вредоносных программ. Это позволяет не только определять уже известное вредоносное ПО на основе существующих баз данных сигнатур, но и выявлять новые, ранее неизвестные угрозы.[1] Анализ происходит путем сравнения с

обширным набором признаков, характерных для вредоносного кода, что включает в себя анализ поведения, изменения в системных файлах и регистрах, сетевую активность и другие факторы.

Благодаря возможности анализировать и обрабатывать огромные объемы данных в кратчайшие сроки, ИИ значительно ускоряет процесс идентификации вредоносного ПО. Это особенно важно в условиях современного киберпространства, где каждую минуту создаются новые варианты вредоносных программ.[7] Кроме того, ИИ способен обучаться на основе анализа поведения вредоносного ПО в динамике, что позволяет ему предсказывать потенциальные угрозы на основе обнаруженных поведенческих моделей и принимать меры по их нейтрализации еще до того, как они успеют нанести ущерб.

Внедрение ИИ в процессы анализа и классификации вредоносного ПО также способствует повышению точности определения угроз, снижая количество ложноположительных и ложноотрицательных срабатываний, которые могут привести к ненужной тревоге или, наоборот, пропуску реальной угрозы. Это достигается за счет того, что ИИ способен адаптироваться к изменениям в методах атак и поведении вредоносного ПО, постоянно обновляя свои алгоритмы на основе получаемой информации.

Применение ИИ не ограничивается обнаружением и анализом угроз; оно также включает в себя прогнозирование кибератак. Системы могут анализировать тенденции и модели поведения в сети, выявляя потенциальные уязвимости и прогнозируя вероятные направления атак. Это позволяет предпринимать профилактические меры до того, как угроза реализуется.

Прогнозирование кибератак с использованием искусственного интеллекта является одной из наиболее инновационных и перспективных областей в сфере информационной безопасности. Эта технология предоставляет возможность не только реагировать на уже произошедшие или текущие атаки, но и предвидеть потенциальные угрозы до того, как они могут быть реализованы.[2] Основываясь на сложных алгоритмах машинного обучения и анализе больших данных, системы на основе искусственного интеллекта способны выявлять закономерности и взаимосвязи в данных о кибербезопасности, которые могут указывать на предвестники будущих атак.

Эти системы анализируют широкий спектр данных, включая, но не ограничиваясь, журналами событий безопасности, сетевым трафиком, тенденциями в интернете, обсуждениями на форумах хакеров, утечками данных и другими источниками информации, которые могут предоставить индикаторы потенциальной угрозы. Путем обработки и анализа этих данных, ИИ может выявить неочевидные связи и закономерности, которые могут не быть очевидны для человека или традиционных систем безопасности.

Прогнозирование кибератак с помощью ИИ позволяет не только предсказывать специфические атаки, но и определять вероятные цели атак и методы, которые могут быть использованы злоумышленниками. Это дает организациям возможность заблаговременно укрепить защиту наиболее уязвимых точек, разработать и внедрить профилактические меры и стратегии реагирования на инциденты, а также провести обучение персонала для повышения уровня осведомленности о потенциальных угрозах.

Однако, несмотря на значительный потенциал, прогнозирование кибератак с использованием искусственного интеллекта сталкивается с рядом вызовов. Среди них – сложность обработки и интерпретации огромного количества данных, необходимость в постоянном обновлении информационной базы для адаптации к постоянно меняющемуся

ландшафту угроз, а также потенциальные риски, связанные с ложноположительными срабатываниями, которые могут привести к неоправданным затратам ресурсов на неверные угрозы.

Несмотря на эти трудности, прогнозирование кибератак с использованием искусственного интеллекта продолжает развиваться, предлагая новые возможности для повышения эффективности систем кибербезопасности.[6] Совершенствование технологий ИИ и улучшение методик анализа данных обещают значительное увеличение точности и оперативности прогнозирования угроз, что позволит еще более эффективно противостоя

Внедрение искусственного интеллекта (ИИ) в область информационной безопасности, несмотря на свои очевидные преимущества, также сопровождается рядом возможных рисков и проблем. Эти вызовы охватывают технические, этические и операционные аспекты, требующие тщательного анализа и управления.

Одной из ключевых проблем является зависимость систем безопасности на основе ИИ от качества и объема обучающих данных. Для эффективного обучения модели ИИ требуют доступ к большим и разнообразным наборам данных, которые должны быть актуальными и репрезентативными. Однако, сбор таких данных может столкнуться с проблемами конфиденциальности и защиты персональных данных, а также с риском включения в обучающий набор предвзятых или некорректных данных, что может привести к ошибочным выводам и действиям со стороны ИИ.

Другой серьезной проблемой является угроза создания и использования вредоносного ИИ. Такие системы могут быть разработаны для проведения кибератак, например, для автоматизации фишинговых атак, обхода систем обнаружения вторжений или даже для разработки новых видов вредоносного ПО, способного эффективнее скрываться от традиционных средств защиты.

Кроме того, использование ИИ в информационной безопасности порождает ряд этических вопросов, связанных с прозрачностью и объяснимостью принимаемых системой решений. Важность этих вопросов возрастает в тех случаях, когда неправильные решения могут привести к серьезным последствиям, таким как неверное блокирование законных операций или нарушение конфиденциальности пользовательских данных.

Техническая сложность систем на основе ИИ также поднимает вопросы об их уязвимости для кибератак. Модели ИИ могут стать целью атак, направленных на искажение их работы путем подачи специально подготовленных данных (атаки с использованием "ядовитых" данных), что может привести к непредсказуемым и нежелательным последствиям.[4]

Наконец, необходимо учитывать и проблему недостаточной квалификации персонала. Эффективное использование ИИ в информационной безопасности требует специалистов, обладающих не только знаниями в области кибербезопасности, но и пониманием принципов работы и возможностей искусственного интеллекта. Недостаток таких специалистов может ограничить способность организаций полноценно использовать потенциал ИИ для укрепления своих систем безопасности.

Таким образом, несмотря на значительный потенциал искусственного интеллекта в усилении информационной безопасности, необходимо тщательно управлять связанными с его использованием рисками и проблемами, разрабатывая стратегии и меры, направленные на минимизацию возможных негативных последствий. Важными аспектами такого управления

являются разработка стандартов и процедур для обеспечения качества и безопасности данных, используемых для обучения ИИ, установление этических принципов использования искусственного интеллекта в целях информационной безопасности, а также внедрение процедур регулярной оценки и корректировки алгоритмов ИИ для предотвращения их злоупотребления или ошибочного функционирования.

В заключение, роль искусственного интеллекта (ИИ) в информационной безопасности продолжает набирать обороты, предлагая передовые решения для обнаружения угроз, предотвращения атак, анализа и классификации вредоносного ПО, а также прогнозирования кибератак. Эти технологии обещают значительное улучшение способности организаций защищать свои информационные активы в условиях постоянно развивающегося и усложняющегося ландшафта киберугроз.

Однако внедрение ИИ в системы кибербезопасности также сопряжено с рядом вызовов и рисков, включая вопросы этики, приватности, зависимости от качества данных и угрозы использования вредоносного ИИ. Эффективное управление этими рисками требует комплексного подхода, который включает в себя разработку нормативных стандартов, обеспечение прозрачности и объяснимости решений ИИ, а также постоянное обучение и повышение квалификации специалистов.

По мере развития технологий искусственного интеллекта и углубления понимания их потенциала и ограничений, можно ожидать, что их роль в области кибербезопасности будет только усиливаться. Инвестиции в исследования и разработку, а также в создание международных рамок сотрудничества будут ключевыми факторами в реализации полного потенциала ИИ для защиты информационного пространства от киберугроз.

Таким образом, будущее информационной безопасности неразрывно связано с прогрессом в области искусственного интеллекта. Успех в этой области потребует не только технологических инноваций, но и продуманного подхода к решению этических, правовых и образовательных вопросов, обеспечивающих безопасное, ответственное и эффективное использование ИИ.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. 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.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. 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.
5. 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.

6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. 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.
5. 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.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.