Перевертун Д.Р. Искусственный интеллект и машинное обучение в сфере информационной безопасности: как это работает и какие угрозы они несут // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 9(35) с. 47–49

Международный журнал информационных технологий и энергоэффективности

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

УДК 004

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КАК ЭТО РАБОТАЕТ И КАКИЕ УГРОЗЫ ОНИ НЕСУТ

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

Современные технологии превратили информационную безопасность в одну из наших главных забот. Но с появлением искусственного интеллекта (ИИ) и машинного обучения (МО) появились новые способы борьбы с киберугрозами, но и новые угрозы. Эта статья познакомит вас с тем, как ИИ и МО используются в защите данных и какие риски они представляют.

Ключевые слова: Искусственный интеллект, машинное обучение, информационная безопасность, киберугрозы, обнаружение аномалий, адаптивная защита, угрозы кибербезопасности.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE FIELD OF INFORMATION SECURITY: HOW IT WORKS AND WHAT THREATS THEY CARRY

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

Modern technologies have turned information security into one of our main concerns. But with the advent of artificial intelligence (AI) and machine learning (MO), new ways to combat cyber threats have emerged, but also new threats. This article will introduce you to how AI and MO are used in data protection and what risks they pose.

Keywords: Artificial intelligence, machine learning, information security, cyber threats, anomaly detection, adaptive protection, cybersecurity threats.

В современном мире цифровых технологий безопасность данных стала настолько важной, что не обратить внимание на использование искусственного интеллекта (ИИ) и машинного обучения (МО) в этой области просто невозможно.

Искусственный интеллект - это набор технологий, позволяющих компьютерам "учиться" на основе данных. [1] В сфере информационной безопасности ИИ используется, чтобы обнаруживать аномалии в данных. Он способен быстро анализировать огромные объемы информации и выявлять подозрительные моменты, которые могли бы ускользнуть от человеческого внимания.

Использование ИИ также позволяет предотвращать атаки. Системы, управляемые ИИ, могут обнаруживать киберугрозы на ранних этапах и реагировать на них быстрее и эффективнее.

Машинное обучение - это метод, который позволяет компьютерам учиться на основе опыта и данных. В сфере информационной безопасности МО используется для создания точных моделей для выявления угроз и аномалий. Эти модели могут анализировать трафик сети, действия пользователей и другие факторы для выявления потенциальных угроз.

Использование ИИ и МО в области информационной безопасности открывает перед нами множество новых возможностей [2-3]:

- Автоматизированное обнаружение и реагирование: Системы с ИИ и МО способны автоматически обнаруживать атаки и моментально реагировать на них, что делает защиту данных более эффективной.
- Анализ больших объемов данных: ИИ и МО способны обрабатывать огромные объемы информации, что помогает выявлять скрытые угрозы и аномалии.
- Адаптивная защита: Системы, основанные на ИИ и МО, могут адаптироваться к новым видам угроз и изменять методы защиты, чтобы уменьшить риски.

Однако с новыми возможностями приходят и новые угрозы. Киберпреступники также используют эти технологии, чтобы создавать более сложные и хитрые атаки. Например, они могут применять алгоритмы МО для создания более реалистичных фишинговых писем или ботов, которые способны обойти системы обнаружения.[4-5]

В современном мире информационной безопасности искусственный интеллект и машинное обучение предоставляют нам мощные инструменты в борьбе с киберугрозами. Однако, они не могут заменить человеческое внимание и заботу. Постоянное развитие и совершенствование наших подходов и стратегий необходимо для эффективной защиты наших данных и информационной инфраструктуры.

Искусственный интеллект и машинное обучение в информационной безопасности - это не только технологический шаг вперед, но и культурный вызов, который требует сознательного отношения к безопасности данных и постоянного внимания к угрозам и инновациям в этой области. Вместе мы можем сделать наши данные более защищенными и остаться в безопасности в цифровом мире.[6-7]

Искусственный интеллект и машинное обучение - это мощные инструменты в борьбе за информационную безопасность. Однако они также требуют постоянного обновления и адаптации, чтобы эффективно защищать данные в постоянно меняющемся мире киберугроз. Использование ИИ и МО становится неотъемлемой частью современных стратегий информационной безопасности, но требует осторожности и непрерывного мониторинга.

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.–№. 4.–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.