Курманбакеев В.А. Применение нейросетей в сфере защиты информации // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2 с. 99–102

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Курманбакеев В.А.
ФГБОУ ВО "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: slavan787@gmail.com

В последние годы интернет и цифровые технологии стали неотъемлемой частью жизни людей, а также бизнеса и государства. С этим связаны как преимущества, так и недостатки, в частности - риск потери и утечки конфиденциальной информации. В такой ситуации защита информации становится критически важной задачей, и здесь важную роль играют нейронные сети.

Ключевые слова: Нейросети, нейронные сети, кибербезопасность, информационная безопасность.

APPLICATION OF NEURAL NETWORKS IN THE FIELD OF INFORMATION SECURITY

Kurmanbakeev V.A.
Bonch-Bruevich St. Petersburg State University of Telecommunications, St. Petersburg, *Russia (193232, St. Petersburg, 22 Bolshevikov Ave., bldg. 1), e-mail: slavan787@gmail.com*

In recent years, the Internet and digital technologies have become an integral part of people's lives, as well as business and the state. This has both advantages and disadvantages, in particular, the risk of loss and leakage of confidential information. In such a situation, information protection becomes a critical task, and neural networks play an important role here.

Keywords: Neural networks, neural networks, cybersecurity, information security.

Нейронные сети - это компьютерные алгоритмы, которые могут обрабатывать большие объемы данных и выявлять скрытые зависимости между ними. Эти свойства делают их прекрасным инструментом для работы с защитой информации. Рассмотрим несколько способов применения нейронных сетей в этой области.

Первым способом является обнаружение аномалий в сети. Этот метод используется для выявления подозрительного трафика, который может указывать на попытки взлома или кражи данных. Нейронные сети могут обучаться на основе нормального трафика и затем выявлять аномальные пакеты данных, которые не соответствуют норме. Это может помочь обнаружить атаки и предотвратить утечки информации.

Вторым способом является анализ поведения пользователей. Нейронные сети могут использоваться для создания профилей пользователей, которые определяют, какие действия являются типичными для этого пользователя, а какие - нет. Это может помочь выявить

необычное поведение пользователей, что может свидетельствовать о попытке несанкционированного доступа к данным.

Третьим способом является шифрование информации. Нейронные сети могут использоваться для создания шифрованных сообщений, которые трудно поддаются взлому. Это может помочь защитить данные от несанкционированного доступа и утечек.

Наконец, четвертым способом является распознавание образов. Нейронные сети могут использоваться для распознавания образов на изображениях, что может помочь в обнаружении попыток использования фальшивых документов или идентификаторов.

Несмотря на все преимущества, применение нейронных сетей в сфере защиты информации также имеет свои недостатки и ограничения. Один из основных недостатков - это высокая стоимость разработки и обучения нейронных сетей, особенно если требуется обработка большого объема данных. Кроме того, нейронные сети могут быть взломаны, если хакеры найдут способ обмануть систему и ввести ложные данные.

Другой ограничением является ограниченность точности нейронных сетей в условиях непредсказуемых и нестандартных ситуациях, что может привести к ошибкам при обработке информации и выявлении угрозы.

Несмотря на эти ограничения, применение нейронных сетей в сфере защиты информации все еще является многообещающим. При правильной настройке и использовании, нейронные сети могут помочь значительно улучшить защиту конфиденциальной информации и снизить риск утечек.

Таким образом, использование нейронных сетей в сфере защиты информации представляет собой эффективный способ обнаружения и предотвращения угроз. Несмотря на ограничения и недостатки, применение этой технологии является актуальной и многообещающей темой для исследований и разработок в области кибербезопасности.

Нейронные сети могут быть применены в различных аспектах защиты информации, таких как обнаружение атак, предотвращение утечек данных, распознавание аномалий, аутентификация пользователей и многое другое.

Одной из самых распространенных областей применения нейронных сетей в сфере защиты информации является обнаружение вредоносного программного обеспечения (малварь). Нейронные сети могут быть обучены распознавать особенности и поведение вредоносных программ, чтобы предотвратить их воздействие на компьютерную систему.

Еще одним примером использования нейронных сетей является распознавание скомпрометированных пользователей. Эта технология может использоваться для обнаружения незаконного доступа к системам или аккаунтам с помощью анализа поведения пользователя. Например, нейронные сети могут обучаться распознавать, когда пользователь выполняет действия, которые не соответствуют его типичному поведению, такие как попытки доступа в неправильное время или из неправильного места.

Также нейронные сети могут быть использованы для защиты данных на уровне приложений, например, при распознавании спама в электронной почте или при защите от фишинговых атак. Нейронные сети могут помочь автоматически распознавать и блокировать нежелательные сообщения, таким образом снижая риск утечки информации.

Наконец, нейронные сети могут быть использованы для анализа больших объемов данных и выявления тенденций и паттернов, которые могут указывать на возможные угрозы.

Это может помочь организациям разработать эффективные стратегии защиты информации, основанные на реальных данных и анализе рисков.

В целом, применение нейронных сетей в сфере защиты информации позволяет существенно улучшить кибербезопасность и снизить риск утечек конфиденциальной информации. Однако, для того чтобы использовать эту технологию эффективно, необходимы профессиональные знания и навыки в области машинного обучения и кибербезопасности, а также доступ к достаточным вычислительным ресурсам для обучения и развертывания нейронных сетей.

Кроме того, нейронные сети могут быть подвержены атакам со стороны злоумышленников, которые могут попытаться обойти или обмануть систему защиты, использующую нейронные сети. Поэтому важно постоянно обновлять и адаптировать системы защиты, чтобы они оставались эффективными в изменяющихся условиях.

В заключение, использование нейронных сетей в сфере защиты информации представляет собой мощный инструмент, который может помочь организациям более эффективно защищать свои данные и предотвращать кибератаки. Однако, необходимо учитывать, что эта технология является лишь одним из инструментов в борьбе за кибербезопасность, и успешность ее применения зависит от профессионализма и компетентности специалистов, которые ее используют.

Также следует отметить, что использование нейронных сетей в сфере защиты информации имеет свои ограничения и ограничения. Например, некоторые атаки могут быть слишком сложными для обнаружения с помощью нейронных сетей, и может потребоваться дополнительная технология для их обнаружения. Кроме того, нейронные сети могут ошибаться при распознавании определенных типов данных или при наличии шума в данных, что может привести к ложным срабатываниям.

Таким образом, использование нейронных сетей в сфере защиты информации является перспективным направлением развития, которое может помочь организациям более эффективно защищать свои данные и предотвращать кибератаки. Однако, чтобы успешно применять эту технологию, необходимо учитывать ее ограничения, а также обеспечить высокий уровень профессионализма и компетентности специалистов, которые ее используют.

Список литературы

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
2. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. IEEE Symposium on Security and Privacy.
3. Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. IEEE Symposium on Security and Privacy.
4. Xu, W., Evans, D., & Qi, Y. (2019). Feature squeezing: Detecting adversarial examples in deep neural networks. IEEE Symposium on Security and Privacy.
5. 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.

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

References

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
2. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. IEEE Symposium on Security and Privacy.
3. Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. IEEE Symposium on Security and Privacy.
4. Xu, W., Evans, D., & Qi, Y. (2019). Feature squeezing: Detecting adversarial examples in deep neural networks. IEEE Symposium on Security and Privacy.
5. 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.
6. 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.
7. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for automation of software testing // Naukosphere. – 2020. – №. 6. – pp. 152-156.
8. Shterenberg S. I. Methodology for constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology // OPHTHALMIC surgery. – 2022. – No. 4s. – pp. 51-57.