DOI 10.37882/2223-2966.2025.01.43

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ НА ОСНОВЕ БЛОКЧЕЙН В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

USING BLOCKCHAIN-BASED NEURAL NETWORKS IN INFORMATION SECURITY

S. Shipulin

Summary. This article examines the integration of neural networks and blockchain technologies in the context of information security. Statistics show a growing number of cyberattacks, making the need for data protection more significant than ever. Neural networks play a key role in analyzing large volumes of information and identifying anomalies, while blockchain ensures reliable and transparent data storage, enhancing trust levels.

The article presents successful case studies of the use of these technologies, including examples of blockchain transaction analysis, the creation of decentralized markets, and authentication systems. Lessons learned from these examples are discussed, along with future research prospects in the field of cybersecurity, such as resilience to attacks, model interpretability, and adaptive threat detection systems.

Potential challenges to implementation, legal and ethical aspects, and future development opportunities are also addressed. The article emphasizes that the combination of neural networks and blockchain technologies is a promising area of research capable of shaping a more secure digital world and improving data protection.

Keywords: neural networks, blockchain, information security, cyberattacks, anomalies, data analysis, decentralized systems, authentication, its ethics, development prospects.

Шипулин Святослав Станиславович
Аспирант, Отдел аспирантуры и докторантуры, (ГУАП) «Санкт-Петербургский государственный университет аэрокосмического приборостроения»
profi.social@gmail.com

Аннотация. Данная статья посвящена обзору нейронных сетей и блокчейн-технологий в контексте информационной безопасности. Число киберугроз растет с каждым годом, как и объемы данных, которые нуждаются в защите. Нейронные сети играют ключевую роль в анализе больших объемов информации, в то время как блокчейн обеспечивает надежное и прозрачное хранение данных.

В статье представлены успешные примеры использования этих технологий, включая случаи анализа блокчейн-транзакций, создание децентрализованных рынков и системы аутентификации. Формулируются выводы на основе этих примеров, и выделяются перспективы для будущих исследований в области кибербезопасности, такие как устойчивость к атакам, интерпретируемость моделей и адаптивные системы обнаружения угроз.

Также затрагиваются потенциальные трудности на пути внедрения, правовые и этические аспекты и возможности для будущего развития. Статья подчеркивает, что комбинация нейронных сетей и блокчейн-технологий является перспективной областью исследований, способной сформировать более безопасный цифровой мир и улучшить уровень защиты данных.

Ключевые слова: нейронные сети, блокчейн, информационная безопасность, кибератаки, аномалии, анализ данных, децентрализованные системы, аутентификация, этика в ИТ, перспективы развития.

Введение

В связи с цифровизацией все большего числа процессов, информационная безопасность становится одним из приоритетов для частных организаций, отдельных людей и даже стран. По мере роста объемов данных и киберугроз, традиционные методы информационной безопасности уже не справляются. В связи с вышеупомянутым, существует потребность в разработке более совершенных методов защиты.

Технологии поколения интернета Web3[4], например, блокчейн и нейросети, благодаря децентрализации и машинному обучению, открывают новые горизонты в сфере информационной безопасности. Нейронные сети, благодаря машинному обучению способны обнаруживать новые, ранее не задокументированные угрозы, и обрабатывать огромные массивы данных. Блокчейн, в свою очередь, благодаря своей децентрализованной системе, позволяет минимизировать риски от локальных уязвимостей.

Целью данной статьи является анализ и обзор использования технологий нейросетей, на основе блокчейн, в контексте информационной безопасности. Мы рассмотрим, как сочетание этих двух технологий может повысить защиту информационных систем и эффективность обнаружения киберугроз, а также обсудим возможные трудности, с которыми могут столкнуться специалисты информационной безопасности. В заключение статья предложит перспективы будущих исследований и разработки на стыке нейронных сетей и блокчейн.

Обзор технологий

Обзор нейросетей

Нейронная сеть представляет собой математическую модель, а также её программную или аппаратную реализацию, основанную на принципах работы биологических нейронных сетей — систем нервных клеток живых организмов [1]. Они состоят из взаимосвязанных «нейронов», сгруппированных в слои. Каждый нейрон полу-

чает входные данные, обрабатывает их и передает сигнал следующему уровню сети. Этот процесс позволяет нейросетям выявлять сложные закономерности и принимать решения на основе полученной информации.

Нейросети разделяют по типам: полносвязные, сверточные и рекуррентные [8]. Полносвязные сети хорошо подходят для задач классификации, тогда как сверточные применяются в работе с изображениями, а рекуррентные наиболее результативны в анализе последовательностей данных, например, текстовых массивах.

Введение в блокчейн

Блокчейн представляет собой децентрализованную технологию хранения и передачи данных, основанную на принципе распределенного реестра [7]. Каждая транзакция записывается в блок, который затем добавляется к цепочке блоков, что делает данные неизменяемыми и защищенными от фальсификаций. Блокчейн обеспечивает прозрачность, безопасность и невозможность несанкционированного изменения записей [9].

Основные компоненты технологии блокчейн включают сетевые узлы, которые обрабатывают и хранят данные, а также механизмы консенсуса, которые обеспечивают единство данных среди всех участников сети. Наиболее известными примерами блокчейн-технологий являются: биткойн и эфир, однако их применение распространяется далеко за пределы криптовалют, включая финансовые услуги, управления цепочками поставок и, что особенно актуально, информационную безопасность.

Связь между технологиями блокчейн и нейросетей

Сочетание нейронных сетей и блокчейн-технологий открывает новые возможности для повышения уровня безопасности информационных систем. Нейросети способны обрабатывать большие массивы информации, хранящихся в блокчейне, и выявлять новые, ранее неизвестные угрозы. Одновременно, блокчейн может служить надежным хранилищем для основы нейросетей, гарантируя их целостность и доступность.

Нейросети в сфере информационной безопасности

Обнаружение угроз

Нейросети способны обрабатывать большие массивы информации за короткие временные промежутки, что делает их ценным инструментом в сфере информационной безопасности. Используя алгоритмы машинного обучения, эти сети могут выявлять паттерны, характерные для атак, такие как DDoS-атаки, фишинг или вирусные инфекции. Применяя обученные модели на исторических данных о киберугрозах, нейросети могут идентифицировать новые и неизвестные атаки с высокой степенью точности.

Успешные примеры технологий на основе нейросетей

В современных реалиях, в сфере информационной безопасности, разработано большое количество успешных решений, использующих нейросети. Одним из ярких примеров можно считать системы обнаружения вторжений (IDS), которые могут анализировать сетевой трафик, основывая свои принципы работы на эксплуатации сверточных нейросетей.

Другим примером является использование рекуррентных нейронных сетей (RNN) для анализа логов систем, где модель обучается выявлять аномалии, указывающие на возможные атаки или внутренние угрозы. Такие подходы помогают не только повышать уровень защиты, но и ускорить время принятия санкций на инциденты.

Трудности при использовании нейросетей

Учитывая все преимущества нейросетей, существует и ряд проблем.

Во-первых, модели требуют больших объемов обучающих данных, которые не всегда доступны и могут включать в себя чувствительную информацию. Во-вторых, нейронные сети подвержены проблеме «черного ящика», когда сложно интерпретировать, как они принимают решения. Это может затруднять анализ и проверку моделей на предмет их надежности. Наконец, атаки на саму модель, такие как атаки с использованием подмены данных, могут приводить к сбоям в работе систем безопасности.

Таким образом, идентификация угроз с помощью нейросетей, предоставляет многообещающие результаты, но вместе с этим требует тщательного подхода к обучению и тестированию моделей, а также разработки методов их защиты.

Интеграция блокчейн-технологий

Как блокчейн может улучшить безопасность нейросетей

Интеграция блокчейна с нейросетями открывает новые горизонты в области информационной безопасности благодаря повышению надежности и прозрачности обработки данных. Один из ключевых аспектов блокчейна — его децентрализованная архитектура. Это позволяет повышать уровень защитной информации

от несанкционированных манипуляций. Каталоги данных, используемых нейросетями для обучения, могут храниться в блокчейне, что гарантирует их целостность и защищенность от изменений [4].

Кроме того, благодаря прозрачности блокчейна можно отслеживать процесс обучения нейросетей и формирование их модели. Это облегчает проверку и аудирование, что крайне необходимо в условиях регуляторных требований и стандартов безопасности.

Примеры реализации проектов с использованием комбинации технологий

Существуют уже множество проектов, которые успешно комбинируют нейронные сети и блокчейн. Например, в системах управления идентификацией и доступа можно использовать блокчейн для устойчивого хранения идентификационных данных пользователей, когда нейросетям можно поручить обнаружение аномалий в поведении пользователей для раннего выявления возможных уязвимостей.

Другой пример — системы обнаружения угроз, где блокчейн применяется в аутентификации и подтверждения источников данных, поступающих для обработки в нейросети. Это помогает избежать манипуляций с переменными и гарантирует высокую степень доверия к результатам анализа.

Плюсы и минусы применения блокчейн для нейронных сетей

Преимущества применения блокчейн-технологий в нейросетях очевидны: значительное повышение уровня безопасности, прозрачность и возможность децентрализации данных. Однако существуют и определенные недостатки. Например, блокчейн может быть медленнее по сравнению с традиционными централизованными базами данных, что может негативно сказаться на темпах обучения нейросетей. Кроме того, сложность интеграции различных технологий и высокий уровень энергопотребления блокчейн-сетей могут послужить значительными препятствиями для их широкого использования.

Положительные примеры

Обзор удачных решений

В последние годы наблюдается рост интереса к интеграции нейросетей и блокчейн-технологий в различных отраслях. Рассмотрим несколько успешных кейсов, где такие решения были реализованы для повышения уровня информационной безопасности.

- Кейс 1: Анализ блокчейн-транзакций с помощью технологий нейросетей

Платформы Chainalysis [11] или Elliptic [12] в области финансовых технологий применяли нейросети для выявления мошеннических транзакций на базе данных блокчейна. Модель, прошедшая обучение на реальных примерах о транзакциях, способна выявлять аномалии, указывающие на потенциальные мошеннические схемы с высокой точностью. Это позволяет значительно снизить уровень фродовых операций, обеспечив безопасность как для своих клиентов, так и для платформы.

- Кейс 2: Децентрализованный рынок продажи и эксплуатации нейросетевых моделей

— OpenSea [13]: Крупнейшая платформа для торговли не взаимозаменяемыми токенами (NFT) определяет цены на NFT, с помощью применения нейросетевых алгоритмов. Эти алгоритмы анализируют данные с рынка и помогают пользователям оценить стоимость токенов, учитывая спрос и предложения.
— Augur [14]: это децентрализованная платформа для прогнозирования, которая использует блокчейн для подтверждения итогов ставок. Нейросети могут применяться для анализа тенденций и предсказания результатов событий, делая платформу более эффективной и полезной для пользователей.
— Origin Protocol [15]: Платформа, которая позволяет пользователям создавать децентрализованные приложения для торговли. Нейросети анализируют пользовательские данные и предпочтения, помогая находить наиболее подходящие предложения или партнеров для сделок.

Эти примеры показывают, как технологии нейронных сетей и блокчейна могут работать вместе для создания более прозрачных и эффективных рынков.

- Кейс 3: Системы аутентификации и управления доступом

Еще один интересный пример связан с применением нейросетей и блокчейна в системах аутентификации. Команда разработчиков создала решение, которое использует блокчейн для хранения учетных данных пользователей, а нейронные сети анализируют поведение пользователей для выявления подозрительных действий. Это позволяет не только повысить защищенность, но и улучшить пользовательский опыт, минимизируя количество ложных срабатываний.

— Civic [16]: Эта платформа предоставляет решения для управления идентификацией на основе блок-

чейна. Civic использует биометрическую аутентификацию, позволяя пользователям подтверждать свою личность с помощью отпечатков пальцев или распознавания лиц. Нейронные сети применяются для улучшения точности распознавания, а блокчейн обеспечивает безопасное хранение и управление данными пользователя.

— Selfkey [17]: Платформа Selfkey позволяет пользователям управлять своей идентификацией и личными данными, используя технологии блокчейн и биометрическую аутентификацию. Нейросети применяются в анализе и последующей обработке биометрических данных, что повышает уровень безопасности и упрощает процесс верификации идентичности.

— Zug: Город Zug в Швейцарии, известный как «Криптодолина», экспериментирует с системами цифровой идентификации, которые включают биометрические технологии. Как уже упоминалось ранее, биометрическая аутентификация с применением нейросетевых технологий повышает уровень безопасности, а данные, в свою очередь, безопасно хранятся и управляются через блокчейн.

Выводы, извлеченные из кейсов

Эти примеры демонстрируют, как интеграция нейронных сетей и блокчейн-технологий может значительно повысить уровень информационной безопасности в различных сферах. Основные выводы, полученные из анализа этих кейсов, включают необходимость в комплексном подходе к разработке решений, сочетая технологии для достижения максимальной эффективности, а также важность обеспечения прозрачности и надежности данных для повышения доверия пользователей.

Перспективы исследований и будущие направления

Области будущих исследований

С учетом стремительного развития технологий, интеграция нейронных сетей и блокчейн-технологий открывает множество возможностей для дальнейших исследований. Ниже перечислены некоторые ключевые направления, которые могут быть интересными для исследователей и профессионалов в области кибербезопасности.

1. Устойчивость к атакам

Одним из важных направлений является изучение методов повышения устойчивости нейронных сетей к атакам, таким как атаки на подсчет градиентов или отравление данных. Исследования могут сосредоточиться на разработке алгоритмов, которые способствуют улучшению защитных механизмов нейронных сетей и блокчейна, определяя уязвимости и методы их минимизации.

2. Улучшение интерпретируемости моделей

Как упоминалось ранее, нейронные сети часто рассматриваются как «черные ящики». Исследования в области объяснимого ИИ могут помочь разработать методы, которые позволят понять, каким образом модели принимают решения, а также обеспечивать максимальную прозрачность в процессе анализа данных. Это особенно важно в контексте блокчейн-технологий, где доверие и прозрачность являются основополагающими.

3. Адаптивные системы обнаружения угроз

Адаптивные системы, применяемые в нейросетях, в комбинации с блокчейном, способны к постоянному обучению и адаптации к новейшим уязвимостям. Исследования в этой области могут помочь выявить эффективные методики для разработки систем, которые автоматически обновляют свои модели на основе новых данных об атаках в реальном времени.

4. Интеграция с IoT и мобильными устройствами

С учетом растущего числа устройств интернета вещей (IoT) и мобильных приложений исследование взаимодействия нейросетей и блокчейн-технологий с целью повышения уровня защищенности этих устройств станет важной областью исследований. Здесь имеются огромные возможности для разработки устойчивых архитектур, которые могут минимизировать риски и повысить уровень безопасности.

Перспективы внедрения технологий

Со временем, когда технологии будут становиться все более интегрированными, можно ожидать появления новых стандартов и протоколов, обеспечивающих взаимодействие между нейронными сетями и блокчейном. Это может привести к созданию готовых решений, проверенных временем и зарекомендовавших себя безопасных систем, которые могут быть легко внедрены в различные сферы бизнеса.

Заключение

В заключение, интеграция нейронных сетей и блокчейн-технологий предлагает многообещающие возможности для улучшения информационной безопасности. Эти технологии можно комбинировать для создания более защищенных и эффективных систем, способных противостоять киберугрозам. Будущее исследований в этой области выглядит ярким, и в нем есть большое количество возможностей для внедрения инновационных решений, которые помогут защищать данные и системы от разнообразных атак.

ЛИТЕРАТУРА

1. Нейронные сети : [арх. 25 октября 2022] / Галушкин А.И. // Большая российская энциклопедия : [в 35 т.] / гл. ред. Ю.С. Осипов. — М.: Большая российская энциклопедия, 2004–2017.
2. Ричард Саттон, Эндрю Барто — Обучение с подкреплением, 2017 г.
3. Александр Табернакулов, Ян Койфманн — Блокчейн на практике, 2019 г.
4. "Как связаны блокчейн и искусственный интеллект — две главные технологии Web3?" (Электронный ресурс. URL: https://rb.ru/story/ai-blockchain-bond/) (дата обращения: 07.12.2023)
5. И. Белоусов, Владимир Попов, Э. Крон, А. Пискунов, С. Симановский — WEB 3.0.Часть I. Настоящее вчерашнего завтра, 2020 г.
6. Гудфеллоу Я., Бенджио И., Курвилль А. — Глубокое обучение, 2017 г.
7. Sherman Alan T., Javani Farid, Zhang Haibin, Golaszewski Enis (January 2019). «On the Origins and Variations of Blockchain Technologies». IEEE Security Privacy. 17 (1): 72–77. arXiv:1810.06130. doi:10.1109/MSEC.2019.2893730. ISSN 1558-4046.
8. Как работают нейросети простое объяснение в картинках URL: https://digitalocean.ru/n/shkola-mysli электронный ресурс. (Дата обращения: 12.01.2024)
9. Nida Khan. FAST: A MapReduce Consensus for High Performance Blockchains // Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. — New York, NY, USA: Association for Computing Machinery, 2018-11-04. — С. 1–6. — ISBN 978-1-4503-6050-0.
10. Michał Pawlak, Jakub Guziur, Aneta Poniszewska-Marańda. Voting Process with Blockchain Technology: Auditable Blockchain Voting System (англ.) // Advances in Intelligent Networking and Collaborative Systems. — Cham: Springer International Publishing, 2018-08-26. — P. 233–244.
11. Как финансовые учреждения могут уверенно предлагать крипто валютные продукты. Электронный ресурс, URL: https://www.chainalysis.com/ (Дата обращения: 19.06.2024)
12. Точно знайте, что происходит в любом блокчейне. Электронный ресурс, URL: https://www.elliptic.co/ (Дата обращения: 19.06.2024)
13. Площадка NFT Электронный ресурс, URL: https://opensea.io/ (Дата обращения: 17.08.2024)
14. «Augur Bets on Blockchain-Powered Prediction Markets». CoinDesk (англ.). 2015-03-01. Архивировано 8 сентября 2018. (Дата обращения: 9 сентября 2018)
15. Origin Protocol (OGN) Электронный ресурс, URL: https://www.binance.com/en/research/projects/origin (Дата обращения: 19.06.2024)
16. Seamless user management Электронный ресурс, URL: https://www.civic.com/ (Дата обращения: 12.07.2024)
17. Self-Key, Singularity DAO and Cogito Finance Announce Strategic Merger to Form Singularity Finance (SFI) Электронный ресурс, URL: https://selfkey.org/ (Дата обращения: 15.06.2024)

Журнал «Современная наука: актуальные проблемы теории и практики»