ГЛУБОКОЕ ОБУЧЕНИЕ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СЕТЕВЫХ СИСТЕМАХ

Бекматов Акмал Курбонмахматович

Ассистент кафедры «Оптические системы связи и сетевая безопасность» Каршинского филиала ТУИТ им. Мухаммада ал-Хоразми

Аннотация. *Статья изучает глубокое обучение в улучшении систем обнаружения сетевых вторжений, рассматриваются подходы в идентификации скрытых угроз и отклике на кибератаки.*

Ключевые слова: *Кибербезопасность, Искусственный интеллект (ИИ), Глубокое обучение (DL), Нейросети, Обнаружение вторжений, IDS.*

DEEP LEARNING FOR ENHANCING THE EFFECTIVENESS OF INTRUSION DETECTION IN NETWORK SYSTEMS

Bekmatov Akmal Kurbonmahmatovich

Assistant of the Department "Optical Communication Systems and Network Security" of the Karshi Branch of TUIT named after Muhammad al-Khwarizmi

Abstract. *The article explores deep learning in improving network intrusion detection systems, considering approaches in identifying hidden threats and responding to cyber-attacks.*

Keywords: *Cybersecurity, Artificial Intelligence (AI), Deep Learning (DL), Neural Networks, Intrusion Detection, IDS.*

Введение. В эпоху усиления цифровизации мира, вопросы кибербезопасности приобретают особую актуальность. От постоянно растущего количества устройств, подключенных к Интернету вещей (IoT), до распределенных сетевых систем больших предприятий, от уязвимости

данных до роста сложности кибератак - все это ставит безопасность сетей на передний край борьбы с киберпреступностью. В таком контексте системы обнаружения вторжений (IDS) выступают как первая линия защиты, предназначенная для идентификации, анализа и противодействия киберугрозам.

Огромные объемы данных, генерируемые современными сетями, требуют нового уровня интеллектуального анализа, который могут предложить методы глубокого обучения. Эти методы позволяют создавать модели, способные обучаться на основе опыта, распознавать сложные паттерны и прогнозировать потенциальные угрозы с быстродействием и точностью, недостижимыми для традиционных подходов.

Однако внедрение глубокого обучения в IDS сопряжено с рядом сложностей, начиная от сбора и предварительной обработки качественных обучающих наборов данных до интерпретации результатов работы сложных нейронных сетей. В этой статье мы рассмотрим, как глубокое обучение трансформирует пейзаж IDS, обеспечивая более высокую точность и надежность в обнаружении вторжений, при этом подчеркивая необходимость комплексного подхода к разработке и поддержке этих систем для поддержания безопасности в динамичной сетевой среде.

Основная часть. Исследования в области IDS показывают, что глубокое обучение значительно улучшает обнаружение несанкционированных вторжений. Разнообразие исследований фокусируется на применении сверточных нейронных сетей (CNN), рекуррентных нейронных сетей (RNN) и автоэнкодеров для выявления атак. Академические работы поднимают вопросы обучения сетей на полноценных и актуальных наборах данных, стратегиях обнаружения ранее неизвестных атак и механизмах минимизации ложных срабатываний.

N. Shone, T.N. Ngoc, V.D. Phai и др. разработали технику глубокого обучения для систем обнаружения вторжений, представив несимметричный

глубокий автоэнкодер для неуправляемого изучения функций, достигая высокой точности обнаружения.

A. Javaid, Q. Niyaz, W. Sun, M. Alam предложили подход на основе глубокого обучения для разработки систем IDS, используя самообученное обучение на наборе данных NSL-KDD, являющемся эталоном для систем обнаружения сетевых вторжений.

L. Ashiku, C. Dagli рассмотрели системы обнаружения сетевых вторжений с использованием последних симулированных сетевых нагрузок и предложили глубокую архитектуру классификации с полудинамической настройкой.

Z. Ahmad, A. Shahid Khan, C. Wai Shiang и др. исследовали, как глубокое обучение и машинное обучение могут комбинироваться для обнаружения сетевых вторжений, обеспечивая улучшенную точность определения аномалий в сети.

Теоретические положения утверждают важность обучения сетей с учетом специфики сетевого трафика и необходимость интерпретируемости моделей, чтобы обеспечить возможность анализа и корректировки принимаемых системой решений.

Методология, используемая для исследования и анализа данных. Методология исследования базируется на применении техник глубокого обучения для расширения возможностей систем обнаружения вторжений. На первом этапе собираются и агрегируются большие наборы сетевых данных, включая нормальный трафик и разнообразные виды атак, для обучения и тестирования моделей. Эти данные могут быть получены из публично доступных наборов, таких как NSL-KDD, или скомпилированы посредством внедрения в экспериментальные сетевые среды.

Для подготовки данных применяются методы очистки, нормализации и стандартизации. Затем определяются характеристики и параметры входных данных, которые важны для обучения нейросетевых моделей. В качестве

архитектур глубокого обучения для IDS широко используются сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), подкрепленные нейронные сети (Reinforcement Neural Networks) и другие, в зависимости от специфики задачи.

На этапе обучения модель настраивается для распознавания закономерностей атак и нормального трафика. Для увеличения точности применяются методы перекрестной проверки и тонкой настройки гиперпараметров. После тренировки модели проводится их оценка с использованием отложенных тестовых наборов данных для измерения реальной производительности.

Анализ данных включает в себя изучение метрик, таких как точность, полнота, F1-мера и матрица ошибок. Также акцент делается на сравнении обнаруженных атак с известными сценариями и на способности модели адаптироваться к новым и неизвестным угрозам.

Заключительный этап методологии включает интерпретацию и визуализацию результатов, которые помогут специалистам в сфере сетевой безопасности более быстро определить источник и природу угрозы, а также разработать соответствующую стратегию реагирования.

Описание и сравнение моделей глубокого обучения применимых в IDS. В контексте систем обнаружения вторжений (IDS) модели глубокого обучения играют ключевую роль в точном и эффективном распознавании атак. Представим обзор наиболее популярных архитектур нейросетей и сравнение их применимости и эффективности в условиях IDS.

Сверточные нейронные сети (CNN) хорошо подходят для анализа визуальных образов данных и часто используются для обработки изображений. В сфере IDS они применимы для анализа сетевых потоков, преобразуя полученные данные в изображения или использования CNN для автоматического извлечения признаков из сырых сетевых данных.

Рекуррентные нейронные сети (RNN) и их вариации, такие как LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit), эффективно работают с временными рядами и последовательными данными, что делает их идеальными для анализа сетевого трафика, который часто имеет временную природу.

Автоэнкодеры используются в IDS для выявления аномалий, сжимая входные данные и затем восстанавливая их, что позволяет выделить несоответствия между нормальным и аномальным трафиком.

Кроме того, рассматриваются генеративно-состязательные сети (GAN), которые могут генерировать синтетические обучающие примеры, помогающие в увеличении количества данных для тренировки в случаях, когда реальные данные ограничены.

Сравнительный анализ моделей, предоставленная в таблице 1, демонстрирует, что нет одной универсальной модели, и выбор подходящей архитектуры зависит от специфик атак, типовых шаблонов в сетевом трафике и доступности обучающих данных. Так, свойства LSTM могут быть более применимы к детекции сложных сетевых атак, которые происходят на протяжении длительного времени, в то время как CNN может быть более подходящей для быстрого анализа визуализированных данных сетевого трафика.

Важно подчеркнуть, что успех применения моделей глубокого обучения в IDS значительно зависит от качества и разнообразия использованных для обучения данных, а также от тонкой настройки гиперпараметров архитектуры, адаптированные под конкретные цели и условия эксплуатации IDS.

Ключевой проблемой при применении глубокого обучения в IDS является баланс между обнаружением и ложноположительными срабатываниями. Эффективность любой модели IDC обычно оценивается через такие метрики, как точность, отзыв и F1-score.

В заключении раздела изложены результаты сравнения моделей, которые указывают на то, что нет универсального решения для IDS; выбор подходящей модели глубокого обучения зависит от конкретных требований системы и специфики сетевой среды.

Сравнительный анализ моделей глубокого обучения применимых в IDS

Таблица 1.

Модель	Характеристики	Преимущества	Недостатки	Применимость в IDS
Свёрточные нейронные сети (CNN)	Эффективное распознавание структурированных данных.	Высокая точность, автоматическое выявление признаков.	Требуют большого количества данных и вычислительных ресурсов.	Подходят для анализа визуальных данных и временных рядов трафика.
Рекуррентные нейронные сети (RNN)	Обработка последовательных данных с временем.	Хорошо подходят для временных зависимостей в данных.	Могут страдать от проблем с переобучением и затянутыми циклами обучения.	Эффективны в обнаружении аномалий в трафике и поведении пользователей.
Глубокие нейронные сети (DNN)	Глубокое и многослойное обучение для выявления сложных признаков.	Могут выявлять неочевидные шаблоны атак.	Требуют значительных объемов обучающих данных, риск переобучения.	Используются для решения различных комплексных задач в области безопасности.
Автоэнкодеры	Не требуют маркированных данных, обучаются на нормальных шаблонах поведения.	Низкий уровень ложноположи-тельных срабатываний.	Могут не обнаруживать новые, неизвестные типы атак.	Хороши для обнаружения сетевых аномалий.
Генеративно-состязательные сети (GAN)	Могут генерировать новые данные для улучшения обучения моделей.	Создают существенное улучшение модели за счет новых данных.	Сложны в настройке, высокий риск нестабильного обучения.	Применяются для генерации дополнительного обучающего материала.

Анализ эффективности подходов на основе глубокого обучения. Анализ результатов применения моделей глубокого обучения в системах IDS

выявил позитивные тенденции и одновременно определенные сложности. Эффективность изученных подходов оценивалась на основе нескольких ключевых показателей, включая точность (accuracy), полноту (recall), точность (precision) и F1-меру, которые совместно обеспечивают комплексную оценку способности моделей корректно классифицировать трафик и выявлять вторжения.

Модели глубокого обучения, особенно с использованием ансамблевых методов, могут демонстрировать более высокие уровни точности по сравнению с традиционными методами машинного обучения. Особенно это касается комплексных задач обнаружения, где необходимо распознавать новые и неизвестные типы вторжений или атак с малым количеством признаков.

Тем не менее, некоторые модели страдают от переобучения из-за сложности и многомерности сетевого трафика. Кроме того, нейронные сети, обученные на недостаточно разнообразных данных, могут не обнаруживать новые типы вторжений, что требует регулярного обновления и уточнения наборов обучающих данных.

Также следует отметить, что для более низких показателей ложнопозитивных срабатываний нужно обеспечить более тонкую настройку пороговых значений и балансировку классов данных. Проблемы вычислительной эффективности, связанные с обработкой большого количества данных в реальном времени, предстоит решить путем оптимизации моделей и инфраструктуры.

В целом, применение глубокого обучения в IDS обещает более эффективное и динамичное обнаружение вторжений с возможностью адаптации к быстро развивающимся киберугрозам, но требует дальнейшего исследования оптимальных конфигураций и подходов к обучению для достижения наилучших результатов.

Заключение. Глубокое обучение трансформирует IDS, предлагая усовершенствованные способы для борьбы с угрозами. Однако возникающие вызовы связанные с ресурсоемкостью и требуемыми данными, требуют дополнительных решений для оптимизации процессов обучения и повышения общей эффективности обнаружения вторжений.

Источники литературы.

1. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection (https://ieeexplore.ieee.org/abstract/document/8264962/). IEEE Transactions on Emerging Topics in Computational Intelligence.

2. Ashiku, L., & Dagli, C. (2021). Network intrusion detection system using deep learning (https://www.sciencedirect.com/science/article/pii/S1877050921011078). Procedia Computer Science.

3. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system (https://dl.acm.org/doi/abs/10.4108/eai.3-12-2015.2262516). EAI Endorsed Transactions on Security and Safety.

4. Ahmad, Z., Khan, A. S., Che, W. S., & Cheema, M. A. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches (https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4150). Transactions on Emerging Telecommunications Technologies.

5. Sohi, S. M., Seifert, J. P., & Ganji, F. (2021). RNNIDS: Enhancing network intrusion detection systems through deep learning (https://www.sciencedirect.com/science/article/pii/S0167404820304247). Computers & Security.

6. Thapa, N., Liu, Z., Kc, D. B., Gokaraju, B., & Roy, K. (2020). Comparison of machine learning and deep learning models for network intrusion detection systems (https://www.mdpi.com/1999-5903/12/10/167). Future Internet.

7. Бекматов А.К., Кутдусова Э.Р., Мукимов Ш.И., & Давлатова Н.Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Экономика и социум, (6-1 (109)), 1264-1270.

8. Бекматов, А. К., Кутдусова, Э. Р., & Муқимов, Ш. И. (2023). ПРЕИМУЩЕСТВА И ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ. O'ZBEKISTONDA FANLARARO INNOVATSIYALAR VA ILMIY TADQIQOTLAR JURNALI, 2(20), 280-286.