УДК *004.056.5*

И.А.Щербаков[1], В.В. Михаэлис[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

АНАЛИЗ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ NVIDIA MORPHEUS ДЛЯ ОБНАРУЖЕНИЯ КИБЕРУГРОЗ

Аннотация. *В рамках данной статьи рассматривается возможность использования технологии Nvidia Morpheus для обнаружения киберугроз в компьютерных сетях, в особенности Spear-Fishing. Описаны основные характеристики и принципы работы этой технологии, включая алгоритмы и методы обнаружения угроз. Проанализированы результаты текущих исследований и практического использования Nvidia Morpheus и его эффективность сравнена с другими методами обнаружения киберугроз. Обсуждено применение технологии в контексте обеспечения безопасности компьютерных сетей и возможность ее дальнейшего развития. Работа выполнена в рамках научно-исследовательской работы студентов [1].*

Ключевые слова: *киберугрозы в вычислительных сетях, применение облачного фреймворка кибербезопасности.*

I.A.Shcherbakov[1], V.V. Mikhaelis[1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

ANALYZING THE APPLICATION OF NVIDIA MORPHEUS TECHNOLOGY FOR CYBER THREAT DETECTION

Abstract. *This article examines the potential of utilizing Nvidia Morpheus technology for detecting cyber threats in computer networks especially on Spear-Fishing. The main characteristics and principles of operation of this technology, including algorithms and threat detection methods, are described. The results of current research and practical applications of Nvidia Morpheus are analyzed, and its effectiveness is compared with other methods of cyber threat detection. The application of the technology in ensuring the security of computer networks is discussed, along with the possibility of its further development. The work was carried out as part of student research work [1].*

Keywords*: cyber threats in computer networks, the use of a cloud-based cybersecurity framework.*

Введение

В современном информационном обществе люди все чаще встречаются с возрастающим количеством киберугроз, которые требуют новые подходы к обеспечению безопасности информационных систем [2]. Поэтому тема, касающаяся такого важного аспекта нашей технологической сферы – роли искусственного интеллекта в обеспечении информационной безопасности в вычислительных сетях, становится крайне актуальной в условиях нарастающего технологического развития и цифровизации, так как именно они предлагают эффективные решения для борьбы с данными проблемами [3].

В данном исследовании мы рассмотрим применение технологии Nvidia Morpheus основывающуюся на искусственном интеллекте (ИИ) и машинном обучения (МО) и анализируем ее функциональность в технике обнаружения аномалий и предотвращения угроз.

Техники, использующие в своей основе искусственный интеллект и машинное обучение для обнаружения аномалий и киберугроз, предлагают мощные инструменты для борьбы с ними (табл.1). Нейронные сети в современном мире являются одной из ключевых техник, позволяющих моделировать сложные угрозы, а также обнаруживать аномалии в данных. Именно нейронные сети позволяют злоумышленникам генерировать спирфишинговые письма и помогать создавать все более по-настоящему выглядящие тексты, которые могут привести к утечке информации. Генетические алгоритмы позволяют удобно оптимизировать процессы и обнаруживать аномалии, выбирая максимально эффективные решения на основе эволюционных принципов. Анализ поведения пользователей это важный

инструмент для нахождения отклонений от нормы и раннего обнаружения, а статистическое моделирование позволяет выявлять паттерны, которые кажутся аномальными на основе статистических методов и моделей, что позволяет более точно обнаруживать киберугрозы.

Все эти техники имеют свои плюсы и минусы, но эффективная техника зависит от конкретной задачи в которое это потребуется. Это позволяет открывать новые горизонты в области применения искусственного интеллекта и машинного обучения в сетевой кибербезопасности

Таблица 1- Техники обнаружения киберугроз и аномалий на основе ИИ и МО

Техника	Описание
Нейронные сети	Алгоритмы, моделирующие работу человеческого мозга и обнаруживающие аномалии на основе обучения с ментором или без него.
Генетические алгоритмы	Алгоритмы используют эволюционные принципы для определения аномалий и выбора оптимальных решений.
Анализ поведения	Техника основана на анализе нормального поведения пользователей и выявлении отклонений от эталонных моделей.
Статистическое моделирование	Использует статистические методы и модели для обнаружения аномалий и данных.

Spear-Fishing

Рассмотрим серьезную угрозу сетевой кибербезопасности такую как Spear-Fishing (целевой фишинг или дословно копье-фишинг) – одну из самых сложных и опасных форм кибератак использующую электронные письма, цель которой заключается в том, чтобы обманом заставить определенного человека или группу людей совершить действие, которое позволит злоумышленникам получить конфиденциальную информацию или совершить злонамеренные действия. По официальной информации, только в 2021 году, эта угроза обошлась в $2.4 миллиарда долларов американским организациям. И до сих пор, все известные субъекты сетевых угроз в 65% случаев атак используют этот метод атаки [4].

В отличии от традиционного фишинга, который обычно направлен на более широкое количество пользователей сети, этот метод направлен на конкретного человека или небольшое количество пользователей в сети объединенных чем-то общим, обычно, местом работы. Метод Spear-фишинга базируется на сборе личной информации о цели, которая может быть получена из общедоступных источников, таких как социальные сети или профессиональные профили в общедоступных базах данных.

Одна из распространенных тактик таких атак – отправка поддельных электронных писем которые могут выглядеть как официальные сообщения от руководства компании, банка, сервисных провайдеров или других доверенных источников. Эти письма обычно содержат персональную информацию, такую как имя пользователя сети, должность, компания где он работает или учебное заведение где он учится, что делает такие письма убедительнее. Часто в таких письмах просят предоставлять конфиденциальные данные, номера кредитных карт или банковские реквизиты, либо просят перейти по ссылке или скачать вложение, которое может содержать вредоносные программы.

Такие атаки могут привести к серьезным утечкам конфиденциальных данных, финансовым потерям и нарушению безопасности компьютерных сетей и систем в компании, что может привести к компрометации всей сети организации. Для защиты от спирфишинга необходимо проводить обучение для персонала организации умениям распознавать подозрительные электронные письма, использовать многофакторную аутентификацию и не посещать небезопасные сайты с рабочих устройств в сети компании.

Nvidia Morpheus

Злоумышленники уже используют генеративные языковые модели ИИ для создания персонализированных писем в целях атаки. Основанные на ИИ детекторы теоретически, могут легко определять такие атаки, но для эффективного обучения такой модели для защиты потребуются сотни тысяч уникальных тренировочных писем, поэтому сочетание Nvidia Morpheus работающего на основе генеративного ИИ создает революционный рабочий процесс [5]. В основе их технологии используется генеративный ИИ который сгенерировал более 1 миллиона высокореалистичных симулированных фишинговых писем, которые включают в себя подлинно выглядящие изображения и вложения, в итоговом счете имеющие больший шанс на успех атаки. Именно здесь используется техника нейронных сетей, позволяющая моделям обучаться на основе работы человеческого мозга и обучаться на основе этого.

Эти синтетически сгенерированные письма затем использовались для обучения ИИ детектора, созданного в Nvidia Morpheus, для защиты от сложных реальных спирфишиговых атак. С помощью Morpheus и генеративного ИИ, модель продолжает учиться и совершенствоваться в реальном времени, с возможностью пользователей давать обратную связь по отмеченным письмам, непрерывно снижая уровень ложных срабатываний, на протяжении всего использования [5].

Используя генеративный ИИ, Nvidia Morpheus улучшила автоматическое обнаружение спирфишинговых электронных писем с 70% до 90%. Этот результат был достигнут всего за 24 часа с старта обучения (рис.1).

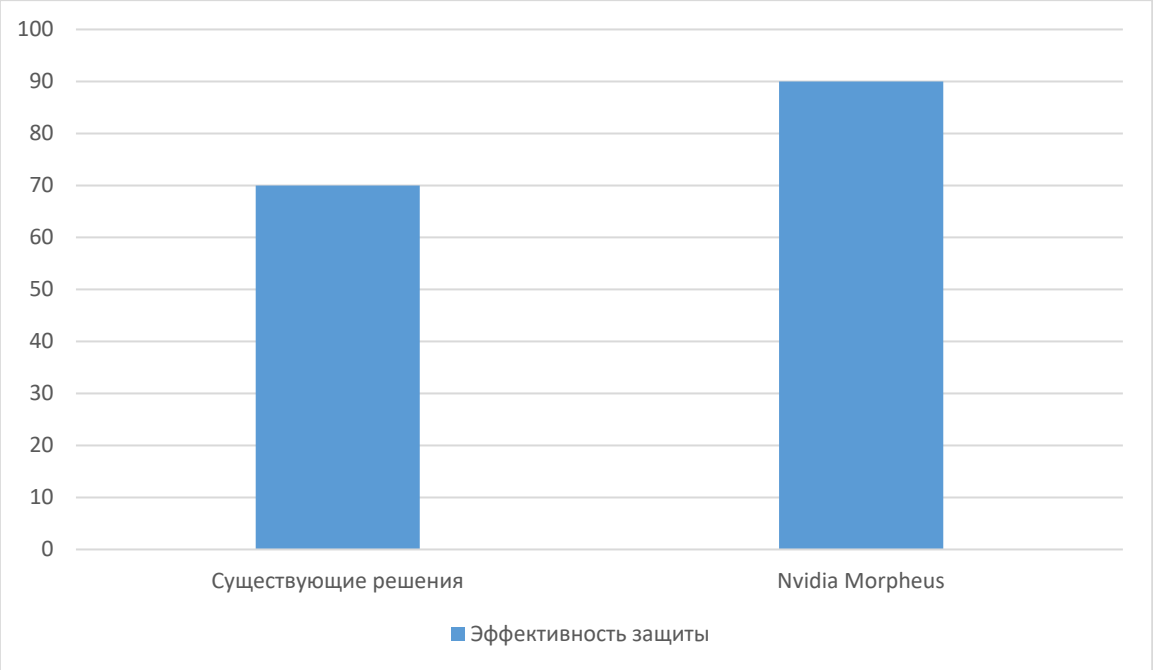

Рис. 1. Эффективность защиты Nvidia Morpheus

Применение

Как пример, можно привести компанию РЖД, где использование этой технологии не позволило бы допустить большую утечку данных. В 2022 году, РЖД была атакована с помощью спирфишингово письма, что в итоге привело к утечке данных о более чем 1,3 млн участников программы «РЖД Бонус» [6]. Файл с базой данных сотрудники компании оставили прямо в корневом каталоге сервера этой программы из-за чего доступ к нему не был сложной задачей для злоумышленника и файл получил широкое распространение в сети интернет. Вместе с самой базой данных были доступны для скачивания приватный ключ RSA и скрипт с прописанным путем, доступ в который ограничивался только логином и паролем сотрудника.

Используя технологию обнаружения спирфишинговых писем Nvidia Morpheus, сотрудник мог просто не получить это письмо и утечки бы не произошло.

Заключение

В ходе исследования мы анализировали применение технологии Nvidia Morpheus основанной на генеративной модели ИИ, которая обучается в реальном времени, мы выяснили что это отличный инструмент для обнаружения киберугроз, который стоит использовать в каждой компании, имеющей сетевую инфраструктуру, и сотрудники которой имеют доступ к ней.

Таким образом это исследование показало важность и потенциал нейронных сетей в области сетевой информационной безопасности и рассмотрело доступное на сегодняшний день решение. Дальнейшие исследования и разработки в этой области будут способствовать повышению уровня безопасности информационных систем и сетей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Методическое и организационное обеспечение научно-исследовательской работы студентов кафедры «Информатика» ИРГУПС / С. И. Белинская, А. В. Козыревская, Н. А. Климова [и др.] // Информационные технологии и проблемы математического моделирования сложных систем. 2009. No7. С. 154-163.
2. Михаэлис, В. В. Защита беспроводных сетей / В. В. Михаэлис, С. И. Михаэлис // Информационные технологии и проблемы математического моделирования сложных систем. – 2015. – № 14. – С. 4-10.
3. Михаэлис, В. В. Исследование применимости искусственного интеллекта при решении математических задач / В. В. Михаэлис, С. И. Михаэлис // Информационные технологии и математическое моделирование в управлении сложными системами. – 2024. – № 1(21). – С. 21-26.
4. Чернов А. А., Горбунов В. В. Анализ и предотвращение угроз в компьютерных сетях с использованием алгоритмов машинного обучения. Журнал "Компьютерные исследования и моделирование", 2021, том 13, № 1, с. 63-72.
5. Nvidia Morpheus. Ways to Get Started With NVIDIA Morpheus. Текст: электронный [Электронныйресурс] // URL: https://developer.nvidia.com/morpheus-cybersecurity (дата обращения 21.05.24)
6. РЖД рассказали детали расследования случаев с доступом к камерам и данным «РЖД Бонус» Текст: электронный [Электронный ресурс] // URL: https://company.rzd.ru/ru/9401/page/78314?id=193735 (дата обращения 15.05.24)

REFERENCES

1. Methodological and organizational support for scientific research work of students of the Department of Informatics of IRGUPS / S. I. Belinskaya, A. V. Kozyrevskaya, N. A. Klimova [etc.] // Information technologies and problems of mathematical modeling of complex systems 2009. No7. pp. 154-163.
2. Michaelis, V.V. Protection of wireless networks / V.V. Michaelis, S.I. Michaelis // Information technologies and problems of mathematical modeling of complex systems. – 2015. – No. 14. – P. 4-10.
3. Michaelis, V.V. Study of the applicability of artificial intelligence in solving mathematical problems / V.V. Michaelis, S.I. Michaelis // Information technologies and mathematical modeling in the management of complex systems. – 2024. – No. 1 (21). – pp. 21-26.
4. Chernov A. A., Gorbunov V. V. Analysis and prevention of threats in computer networks using machine learning algorithms. Journal of Computer Research and Modeling, 2021, Vol. 13, No. 1, p. 63-72.

5. Nvidia Morpheus. Ways to Get Started With NVIDIA Morpheus. Text: electronic [Electronic resource] // URL: https://developer.nvidia.com/morpheus-cybersecurity (date of reference 21.05.24)

6. Russian Railways told the details of the investigation of cases with access to cameras and data “RZD Bonus” Text: electronic [Electronic resource] // URL: https://company.rzd.ru/ru/9401/page/78314?id=193735 (date of reference 05.05.24)

Информация об авторах

Щербаков Арсений Иванович – студент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск. e–mail: 1202098985@irgups.ru.

Михаэлис Владимир Вячеславович–к.п.н., доцент, доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e–mail: mihaelis_vv@irgups.ru.

Information about the authors

Arseniy Ivanovich Shcherbakov– student of the Department «In-formation systems and information protection», Irkutsk State Transport University, Irkutsk, e–mail: 1202098985@irgups.ru.

Vladimir Vyacheslavovich Mikhaelis –Ph.D., associate Professor of the Department «In-formation systems and information protection», Irkutsk State Transport University, Irkutsk, e–mail: mihaelis_vv@irgups.ru.