НАУЧНЫЙ ОБЗОР

УДК 004.77
DOI 10.17513/snt.40579

# СПОСОБЫ ЗАЩИТЫ ОТ ПРЕДНАМЕРЕННЫХ ПЕРЕГРУЗОК ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ, СОЗДАННЫХ ПОСРЕДСТВОМ РАСПРЕДЕЛЕННЫХ МНОЖЕСТВЕННЫХ СЕТЕВЫХ ЗАПРОСОВ: ПАТЕНТНЫЙ АНАЛИЗ

**Сарайкин А.И. ORCID ID 0009-0005-3954-8027, Галимов Р.Р., Абрамова Т.В.**

*Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», Оренбург, Российская Федерация, e-mail: saraikin-a@yandex.ru*

Цель исследования – анализ современных патентных решений в области защиты от преднамеренных перегрузок вычислительной системы, созданных посредством распределенных множественных сетевых запросов. На основе изучения 8325 патентных заявок выявлены ключевые технологические направления и их динамика развития с 2000 по 2025 г. Установлено, что рост публикационной активности имеет экспоненциальный характер, подтверждающий высокую актуальность темы. Построена и проанализирована кластерная структура авторов, определяющая научные связи и лидеров в данной области. Основное внимание уделено классификации патентов по категориям: блокчейн-решения (координация защиты через смарт-контракты, квантово-устойчивые алгоритмы), искусственный интеллект (генеративные модели, прогнозирование атак), программно-определяемые сети, аппаратные решения и интеграция с облачными платформами. Выявлена высокая концентрация патентной активности вокруг крупных технологических корпораций, 14 из которых суммарно формируют более половины всех исследуемых решений. Указывается переход к комплексным подходам, сочетающим несколько технологий, однако отмечаются сохраняющиеся вызовы: минимизация ложных срабатываний, защита от атак с применением квантовых вычислений и масштабируемость решений. Практическая значимость исследования заключается в систематизации передовых методов защиты, что может быть использовано для разработки стратегий кибербезопасности организаций.

**Ключевые слова: преднамеренная перегрузка вычислительной системы, блокчейн, программно-определяемые сети**

# METHODS OF PROTECTION AGAINST INTENTIONAL OVERLOADS OF A COMPUTING SYSTEM CREATED VIA DISTRIBUTED MULTIPLE NETWORK REQUESTS: PATENT ANALYSIS

**Saraykin A.I. ORCID ID 0009-0005-3954-8027, Galimov R.R., Abramova T.V.**

*Federal State Budgetary Educational Institution of Higher Education "Orenburg State University", Orenburg, Russian Federation, e-mail: saraikin-a@yandex.ru*

The purpose of the study is to analyze modern patent solutions in the field of protection against intentional computing system overloads created through distributed multiple network requests. Based on the study of 8,325 patent applications, key technological trends and their development dynamics from 2000 to 2025 have been identified. It has been established that the growth in publication activity follows an exponential trend, confirming the high relevance of the topic. A cluster structure of authors has been constructed and analyzed, revealing scientific connections and leaders in this field. The primary focus is on the classification of patents by categories: blockchain solutions (protection coordination via smart contracts, quantum-resistant algorithms), artificial intelligence (generative models, attack prediction), software-defined networks, hardware solutions, and integration with cloud platforms. A high concentration of patent activity around major technology corporations has been identified, with fourteen of them collectively accounting for over half of all studied solutions. A shift towards comprehensive approaches combining multiple technologies is indicated; however, persistent challenges are noted: minimizing false positives, protection against quantum computing-based attacks, and solution scalability. The practical significance of the research lies in the systematization of advanced protection methods, which can be used for developing cybersecurity strategies for organizations.

**Keywords: intentional computing system overload, blockchain, software-defined networks**

## Введение

На сегодняшний день защита от преднамеренных перегрузок вычислительной системы посредством сетевых запросов является неотъемлемой частью стратегии кибербезопасности любой организации. Игнорирование данной угрозы может привести не только к снижению производительности внутренних систем компании, но и к потере данных, когда преднамеренная перегрузка используется в виде отвлекающего маневра для более сложных атак, таких как кража конфиденциальной информации или внедрение вредоносного программного обеспечения. Анализ инцидентов и использование более усовершенствованных инструментов защиты являются ключевыми факторами в эффективной защите от распределенных

атак типа «отказ в обслуживании» (DDoS). С этой целью стратегически важно выявлять наиболее передовые способы защиты от данных типов угроз.

**Цель исследования** – анализ современных патентных решений в области защиты от преднамеренных перегрузок вычислительной системы, созданных посредством распределенных множественных сетевых запросов. Для достижения поставленной цели сформулированы следующие задачи: выявить ключевые технологические направления в области защиты от DDoS атак; классифицировать патентные решения по основным категориям; проследить динамику развития этих технологий с 2000 по 2025 г.; построить и проанализировать кластерную структуру авторов для определения научных связей и лидеров в области; обобщить вызовы и перспективы развития методов защиты.

## Материалы и методы исследования

Данные о патентах были собраны из агрегированной базы данных «Lens» [1] за период с 2000 по 2025 г. Первоначальный поиск по ключевому слову «DDoS» выявил 19 594 патентных заявки, опубликованных в указанный период. После применения фильтрации по техническому содержанию и ранжирования по релевантности итоговая выборка для детального анализа составила 8325 патентов. В списке литературы данного исследования представлены 32 наиболее релевантных патентных документа, послуживших основой для классификации технологий и выводов. В ходе исследования использованы следующие методы: терминологический анализ, синтез, обобщение, классификация.

## Результаты исследования и их обсуждение

На рис. 1 представлена диаграмма, отображающая динамику публикации патентов по тематике с 2000 по 2025 г.

На момент сбора данных (март 2025 г.) за январь – февраль 2025 г. в базе данных была найдена 341 публикация. Линия тренда на диаграмме имеет экспоненциальный характер, описывается уравнением

$$y = 55{,}25e^{0{,}1495x},$$

что свидетельствует об актуальности исследования. На рис. 2 изображена диаграмма, отображающая распределение заявок на патенты по юрисдикциям.

Всемирная организация интеллектуальной собственности (ВОИС), США и Китай являются лидерами по количеству опубликованных заявок. Мировая индустрия сетевых технологий остается динамичной и высококонкурентной, однако США, Китай, страны ЕС и Восточной Азии являются ключевыми в разработке сетевых решений, облачных технологий и телекоммуникационного оборудования.

Данная геополитическая расстановка сил находит свое отражение и на корпоративном уровне. Анализ выявил высокую концентрацию патентной активности, где 14 ведущих организаций-патентообладателей суммарно формируют 56,8 % от всего исследованного массива. Это наглядно демонстрирует доминирование ограниченного числа крупных международных корпораций, включая технологических гигантов вроде Cisco Technology Inc. (1117 патентов), Amazon (338 патентов), Huawei (330 патентов), IBM (312 патентов) и даже финансовые структуры, такие как Capital One (612 патентов), которые определяют основные направления развития в данной критически важной области кибербезопасности.

На рис. 3 представлена визуализация кластерной структуры авторов анализируемых патентов и общая сила связи.

В таблице представлены авторы с наибольшей публикационной активностью среди анализируемых патентов.

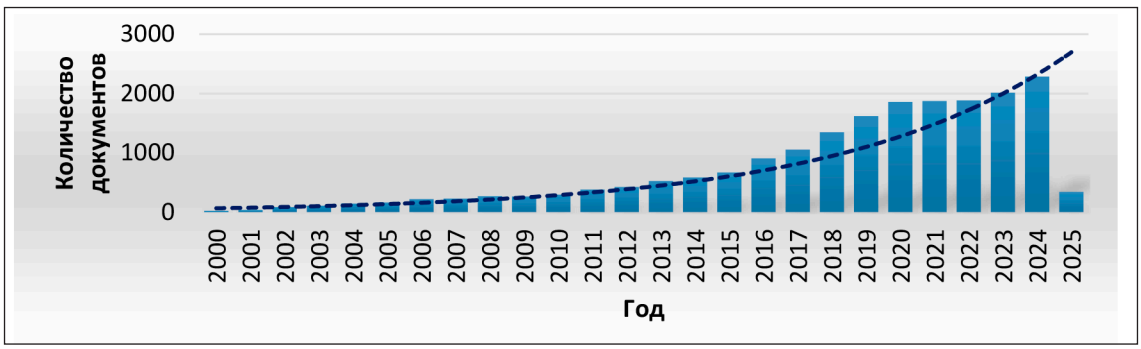


*Рис. 1. Динамика публикации патентов по тематике с 2000 по 2025 г.*
*Примечание: составлен авторами по результатам данного исследования*

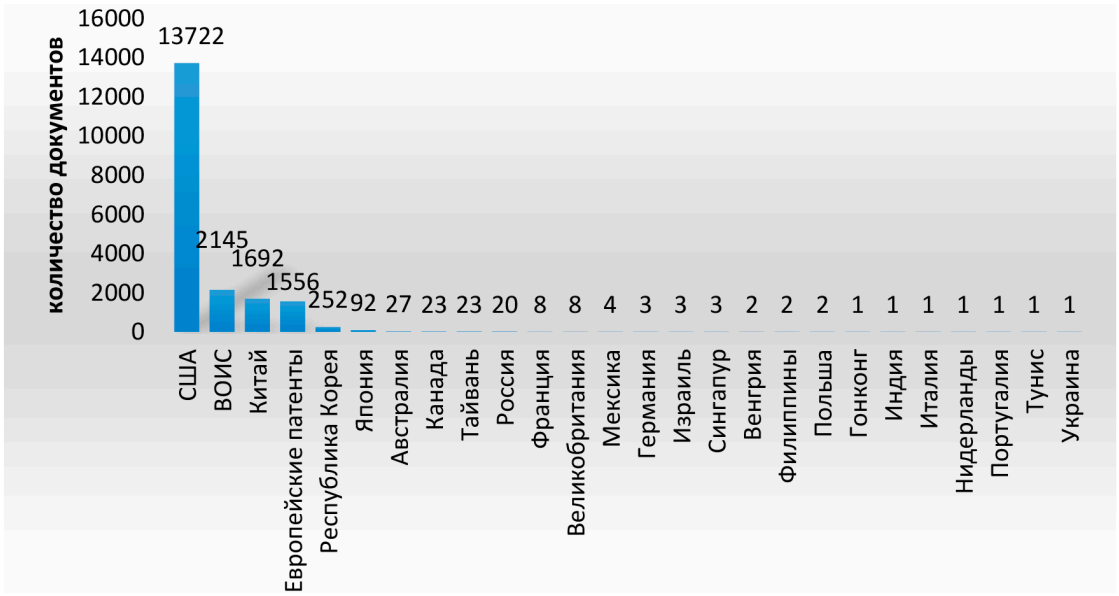


*Рис. 2. Диаграмма распределения заявок на патенты по юрисдикциям*
*Примечание: составлен авторами по результатам данного исследования*

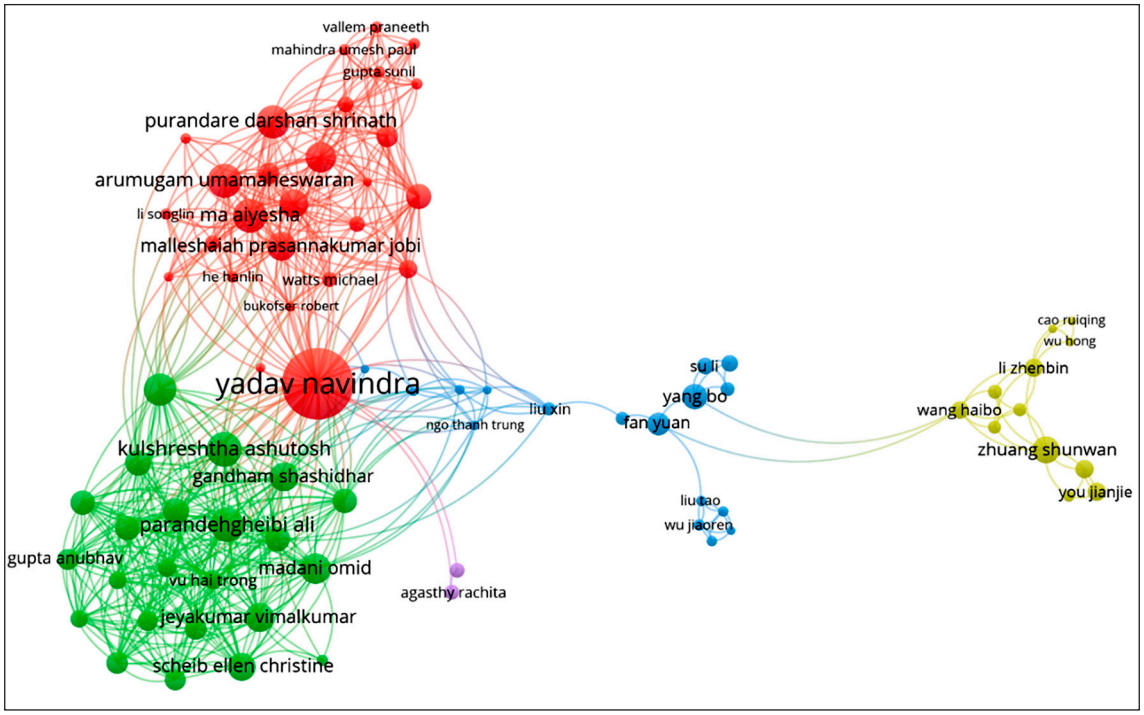


*Рис. 3. Визуализация кластерной структуры авторов анализируемых патентов*
*Примечание: составлен авторами по результатам данного исследования*

Стоит отметить публикационную активность авторов в исследуемой области – Yadav Navindra, Rao Supreeth Hosur Nagesh и Madani Omid, имеющих аффилиацию с компанией Cisco Technology Inc. Количество публикаций с их авторством составляет 2,38% от всего массива анализируемых документов с общей силой связи 27,28%. Общая сила связи указывает не только на общее количество документов, написанных в соавторстве, но и общее число авторов в каждом из документов, созданных в соавторстве.

Авторы с наибольшей публикационной активностью среди анализируемых патентов

| Авторы (страна, город, организация) | Количество документов | Общая сила связи |
|---|---|---|
| Yadav Navindra, Cisco Technology Inc., Сан-Франциско, Калифорния, США | 126 | 1017 |
| Kulshreshtha Ashutosh, Google, Менло-Парк, Калифорния, США | 42 | 443 |
| Parandehgheibi Ali, Массачусетский технологический институт, Кембридж, Массачусетс, США | 41 | 452 |
| Arumugam Umamaheswaran, Университет штата Мичиган, Ист-Лансинг, Мичиган, США | 40 | 331 |
| Purandare Darshan Shrinath, Университет центральной Флориды, Орландо, Флорида, США | 39 | 316 |
| Rao Supreeth Hosur Nagesh, Cisco Technology Inc., Сан-Франциско, Калифорния, США | 38 | 479 |
| Madani Omid, Cisco, Сан-Франциско, Калифорния, США | 34 | 424 |
| Gandham Shashidhar, The University of Texas at Dallas Richardson, США | 27 | 416 |

Примечание: составлена авторами по результатам данного исследования.

Проанализировав исследуемые публикации, было определено, что значительная часть патентов связана с использованием блокчейна, искусственного интеллекта (ИИ), программно-определяемых сетей и аппаратных решений для борьбы с DDoS атаками. Существенная часть работ посвящена прогнозированию уязвимостей, интеграции с облачными платформами и квантово-устойчивым технологиям.

В патентах [2–4] используются системы на основе блокчейна для координации и обмена информацией об атаках между участниками сети (провайдерами, правоохранительными органами). Если целевая сеть и провайдеры защиты от DDoS не являются частью блокчейна, для валидации блоков могут использоваться смарт-контракты и алгоритмы консенсуса [5–7].

В патентах [8–10] представлены квантово-устойчивые блокчейны с заменой алгоритма с открытым ключом «ECDSA» на алгоритмы «Rainbow» и «Winternitz One-Time Signature Plus». Данные решения защищают от атак с применением квантовых компьютеров. Динамическое ограничение транзакций в блокчейн-сетях через алгоритм «Least Mean Square», представленных в патентах [11, 12], обеспечивают предотвращение атак от переполнения буфера памяти.

Компания Salesforce предлагает систему генеративных моделей ИИ для создания конфигураций межсетевых экранов и прогнозирования атак [13]. Компания Mazebolt Technologies использует тестирование на уязвимость к DDoS атакам без нарушения работы системы и модели машинного обучения, способные предсказывать уровень уязвимости производственного элемента к DDoS атакам на основе входных данных о среде, таких как защитные слои, используемые сервисы, IP-адреса, порты и т.д. [14]. В патенте [15] используется трехуровневая аналитика на основе ИИ для выявления паттернов атак, угроз, окружения. Применяется объединение и обработка для формирования расширенных наборов данных (например, добавление информации об источниках, целях, географии). Возможна блокировка трафика, перенаправление и прогнозирование будущих атак. Методы машинного обучения также применяются в патентах с использованием протокола динамической маршрутизации «BGP» [16–18]. Компания AT&T применяет методы ИИ для выявления и блокировки DDoS атак, исходящих от скомпрометированных IoT-устройств в домашних сетях [19].

Применение программно-определяемых сетей и ИИ с обратным распространением ошибки позволяет анализировать информацию о потоках и при обнаружении DDoS атак блокировать вредоносный поток [20, 21]. Также данный вид сетей дает возможность перенаправлять вредоносный трафик с помощью скрабинг-комплекса, в то время как нормальный трафик продолжает свой путь к цели [22–24].

Встречаются также аппаратные решения. Устройство для кибербезопасности от компании Teknodc Bilisim, работающее на CentOS, использует модули отбора пакетов, которые осуществляют их дублирова-

ние, не мешая обычной работе маршрутизатора, а также применяет искусственный интеллект для анализа сетевого трафика. Данное решение блокирует 99,1% атак за 0,1–0,5 мс [25]. Коммутаторы компании Barefoot Networks используют специализированную аппаратную логику с возможностью детектирования атак и перенаправлением/блокировкой трафика на скорости линии [26]. Схожий аппаратный комплекс представлен в патентах [27–29].

В рамках интеграции с облачными платформами компания Oracle предлагает перенаправлять вредоносный трафик через «теневые» виртуальные интерфейсы (SD-VNIC) в систему очистки DDoS [30]. Триггером DDoS при этом служит превышение пороговых значений загрузки канала. После снижения угрозы система возвращается к исходным настройкам, удаляя SD-VNIC и обновляя маршруты. Патент [31] предлагает адаптивную систему защиты от DDoS атак для облачных сред. Адаптация достигается за счет перестройки правил фильтрации на основе изменений в сетевой топологии и шаблонах трафика.

Немаловажной остается задача прогнозирования уязвимостей. Базовым остается использование исторических шаблонов трафика для предсказания атак [30, 32] и построение моделей машинного обучения для оценки рисков на основе данных тестирования и журналов [14].

Также нельзя не отметить уже обыденное дифференцирование легитимных пользователей и скриптовых агентов в процессе DDoS атак с использованием тестов на интеллект [33].

## Заключение

Современные патентные решения в области защиты от DDoS атак демонстрируют переход к комплексным подходам, сочетающим блокчейн и распределенные системы для координации и обмена информацией об атаках между участниками сети, генеративные модели ИИ и самообучающиеся алгоритмы, использование аппаратной логики для обработки трафика в реальном времени, интеграцию с облачными платформами и поддержку многопротокольных сред. Несмотря на разнообразие методов, сохраняются общие вызовы: минимизация ложных срабатываний, защита от атак с применением квантовых вычислений и масштабируемость решений для крупных сетей. Перспективы дальнейших разработок видятся в углубленной интеграции технологий ИИ и машинного обучения для предиктивной аналитики, а также в создании единых стандартов и протоколов для обеспечения интероперабельности разнородных систем защиты в глобальном масштабе. Таким образом, эффективная защита от DDoS атак будущего будет основываться на симбиозе технологической мощи, предиктивных возможностей и межсетевого сотрудничества.

## Список литературы

1. Официальный сайт реферативной базы данных «Lens». [Электронный ресурс]. URL: https://www.lens.org/ (дата обращения: 15.03.2025).

2. Konda T.R., Joshi H.R., Joshi P.P., Wuehler E.D. Using a blockchain for distributed denial of service attack mitigation. Patent 2020. WO № 2020131994.

3. Park S.Y., Jung W.W., Lee S.R. Method for Preventing DDoS Attack that Occurs on Blockchain, and Blockchain System that is Capable of Preventing DDoS Attack. Patent 2019. WO № 2019124669A1.

4 Reddy K.T., Patil P., Pignataro C.M., Lokapalli P.R., Priest J.Y. End-to-end policy management for a chain of administrative domains. Patent 2019. US № 10419446.

5. Haber A.B., Maini S., Choo H. Systems and methods for facilitating a double-layer restriction subnet architecture using subnet specific restrictions within data streamed using hierarchical subnet restrictions. Patent US 2023. № 12081532B1.

6. Yu J., Wang Y., Yan B., Wang, G. DDoS attack joint defense system and method based on blockchain. Patent CN 2021. № 112491823A.

7. Yu J., Wang Y., Yan B., Wang G. Blockchain-Based DDoS Attack Joint Defense System and Method. Patent WO 2022. № 2022099966.

8. Ding J., Ding Y. Quantumproof Blockchain. Patent US 2025. № US12047510B2 [Электронный ресурс]. URL: https://patents.google.com/patent/US12047510B2/en?oq=US12047510B2 (дата обращения: 17.10.2025).

9. Smith R.S., Rubin N.C., Otterbach J.S. Quantum State Blockchain. Patent US 2022. № 11477015B1.

10. Yuan Z., Tan Y. Method and Device for Processing Blockchain Account, and Storage Medium. Patent WO 2020. № 2020019341 A1.

11. Barraza Enciso M.C., Kvochko E. Blockchain system for hardening quantum computing security. Patent US 2021. № 20210126779A1.

12. Johnson W.C., Ispiryan K., Khachatryan G. Cyphergenics-Based Ecosystem Security Platforms. Patent WO 2022. № 2022169969A1.

13. Lefin P.J., Singh P., Talla R.Y., Das P. Distributed denial of service protection management. Patent US 2025. № US20250016194A1.

14. Andriani M., Weiner R. Predictive Distributed Denial of Service Vulnerability Identification for Production Environments. Patent WO 2024. № 2024256931.

15. Doron E., Ezra Y.B., Aviv D. System and method for providing insights on distributed denial of service attacks. Patent US 2022. № 11381593.

16. Yadav N., Singh A.R., Gandham S., Scheib E.C., Madani O., Parandehgheibi A., Pang J.N.K., Jeyakumar V., Watts M.S., Nguyen H.V., Deen K., Prasad R.C., Gupta S.K., Rao S.H.N. System for monitoring and managing datacenters. Patent US 2019. № 20190081959A1.

17. Rao S., Yadav N., Arumugam U., Watts M., Gandham S. Systems and methods for detecting hidden vulnerabilities in enterprise networks: Patent US 2022. № 11503063B2.

18. Yadav N., Rao S.H.N., Kulshreshtha A., Madani O., Pang J.N.K., Deen K., Scheib E.C. Determining a reputation of a network entity. Patent US 2020. № 10623284B2.

19. Koral Y., Jana S., Joshi K. Correlating Compromised Home Internet of Things Devices with Distributed Denial of Service Attacks. Patent US 2024. № 12160445.

20. Yoo M.S., Nguyen T.H., Choi J.S. Software defined network capable of detecting DDoS attacks using artificial intelligence and controller included in the same. Patent US 2018. № 20180109557.

21. Jain H.K. System and method for software defined behavioral DDoS attack mitigation. Patent US 2017. № 9602535 B2.

22. Spatscheck O., Van der Merwe J.E. Method for defending a network against DDoS attacks. Patent EP 2006. № EP1691529A1.

23. George W., Sliteris R. Apparatus and methods for mitigation of network attacks via dynamic re-routing. Patent US 2017. № 20170237767A1.

24. Nainar N.K., Pignataro C.M., Barton R.E., Henry J., Sivabalan M. Distributed denial of service remediation and prevention. Patent US 2022. № 11438371.

25. Poyraz Y. A cyber security device manufactured by using artificial intelligence technology. Patent WO 2023. № 2023244190.

26. Kim C., Lee J., Javadi M.M. Forwarding element with a data plane DDoS attack detector. Patent US 2023. № 11750622.

27. Rubenstein J.E., Ore C.E. and other. Systems and methods for providing a global virtual network (GVN). Patent US 2025. № US20250112802A1. [Электронный ресурс]. URL: https://patents.google.com/patent/US20250112802A1/en?oq=US20250112802A1 (дата обращения: 17.10.2025).

28. Santos D.R., Costante E. and other. Framework for investigating events. Patent US 2025. №. US20250112940A1. [Электронный ресурс]. URL: https://patents.google.com/patent/US20250112940A1/en?oq=US20250112940A1 (дата обращения: 17.10.2025).

29. Chen H. DDoS attack defense method, system, and related device. Patent US 2020. № 10771501.

30. Thomas T.L., Kreger-Stickles L.M. Virtual network distributed denial-of-service scrubber. Patent US № US20240214416A1. [Электронный ресурс]. URL: https://patents.google.com/patent/US20240214416A1/en?oq=20240214416 (дата обращения: 17.10.2025).

31. Yadav N., Singh A.R., Gupta A., Gandham S., Pang J.N.K., Shih-Chun C., Vu H.T. Technologies for annotating process and user information for network flows. Patent US 2023. № 11700190B2.

32. Compton R.A. Distributed denial-of-service attack mitigation with reduced latency. Patent US 2023. № 11729209.

33. Tyree D.S. Scripted distributed denial-of-service (DDoS) attack discrimination using turing tests. Patent US 2002. № 20020120853.

**Конфликт интересов:** Авторы заявляют об отсутствии конфликта интересов.

**Conflict of interest:** The authors declare that there is no conflict of interest.