БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 1 (120). – 69–83

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2026-1-69-83

ОСОБЕННОСТИ ПРОГНОЗИРОВАНИЯ КИБЕРАТАК НА ОСНОВЕ ИСТОРИЧЕСКИХ ДАННЫХ*

А.С. МАРТЫНОВ[1], Н.А. АЛЕКСЕЕВ[2], В.Г. ЛАПИН[3]

[1] *РФ, 115191, г. Москва, внутренняя территория городского муниципального округа Даниловский, ул. Серпуховский Вал, 17, к. 1, Московский финансово-юридический университет, аспирант. E-mail: doskam@narod.ru*
[2] *РФ, 355017, г. Ставрополь, ул. Пушкина, 1, Северо-Кавказский федеральный университет, лаборант кафедры вычислительной математики и кибернетики. E-mail: helpmetobesad@bk.ru*
[3] *РФ, 355017, г. Ставрополь, ул. Пушкина, 1, Северо-Кавказский федеральный университет, доцент кафедры вычислительной математики и кибернетики. E-mail: vitlx@yandex.ru*

Аналитический обзор современных кибератак на основе анализа открытого статистического датасета Global Cybersecurity Threats за 2015–2024 гг. Рассматриваются основные источники кибератак, целевые отрасли, типы угроз и применяемые меры защиты. Особое внимание уделено выявлению устойчивых закономерностей в распределении атак, а также анализу взаимосвязей между источниками угроз, отраслевой принадлежностью организаций и используемыми средствами информационной безопасности. На основе эмпирических данных показано, что киберугрозы носят многофакторный и устойчивый характер, при этом отсутствие доминирующего типа атак или источника подчеркивает сложность их прогнозирования и атрибуции. Полученные результаты могут быть использованы для повышения эффективности систем информационной безопасности и разработки аналитически обоснованных мер противодействия киберугрозам.

Ключевые слова: кибератаки, кибербезопасность, анализ данных, информационная безопасность, источники атак, целевые отрасли, меры защиты

* Статья получена 14 февраля 2026 г.

ВВЕДЕНИЕ

В условиях активной цифровизации и широкого внедрения информационных технологий кибербезопасность становится одной из ключевых проблем современного общества [1, 2]. Рост объема передаваемых и обрабатываемых данных, развитие облачных сервисов и удаленных форм работы приводит к увеличению числа кибератак и усложнению их методов [3]. Кибератаки наносят значительный финансовый ущерб, нарушают устойчивость информационных систем и представляют угрозу для различных отраслей экономики [2, 3].

Особую актуальность приобретает анализ кибератак на основе реальных статистических данных [4, 5]. Несмотря на наличие большого количества открытых отчетов и аналитических обзоров, значительная часть исследований носит описательный характер и не всегда направлена на выявление устойчивых закономерностей [6], которые могли бы быть использованы для снижения рисков и последствий кибератак. В связи с этим использование данных о киберинцидентах в 2015–2024 гг. представляет собой перспективное направление научных исследований.

За 2015–2024 гг. характер киберугроз претерпел существенные изменения. Если в начале рассматриваемого периода преобладали относительно простые атаки, направленные преимущественно на отдельные компьютеры, сайты или локальные сети, то в последние годы наблюдается устойчивый рост целевых, многоэтапных и хорошо спланированных атак. Современные киберинциденты часто сочетают в себе эксплуатацию технических уязвимостей, ошибки конфигурации систем и методы социальной инженерии. Злоумышленники активно используют фишинговые кампании, вредоносное и вымогательское программное обеспечение, атаки на цепочки поставок, а также автоматизированные инструменты и элементы искусственного интеллекта, что значительно повышает эффективность атак и затрудняет их своевременное обнаружение [19].

В статье рассматриваются кибератаки как комплексное явление, сочетающее в себе источники угроз, типы атак, используемые уязвимости, последствия инцидентов и меры защиты, которые применяются для различных типов киберугроз. Такой подход позволяет систематизировать информацию и сформировать целостное представления о современных киберугрозах [7].

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ КИБЕРАТАК

1.1. КЛАССИФИКАЦИЯ КИБЕРАТАК И ИСТОЧНИКОВ УГРОЗ

В качестве источников кибератак выделяют разные категории злоумышленников, которые преследуют различные цели. Это местные жители (nation-state), киберпреступные группировки, внутренние нарушители (insider threats), хактивисты, «скрипт-кидди» и др. По определению IBM, «угрозы представляют собой любые группы или индивиды, причиняющие вред цифровым системам», включая как профессионально мотивированных хакеров, так и инсайдеров и кибертеррористов. Наиболее часто упоминаемые категории: хактивисты (движимые идеологией), государственные хакеры (спонсируемые правительством, занимающиеся промышленным шпионажем и т. д.), киберпреступники (ради финансовой выгоды), а также инсайдеры и скрипт-кидди (хакеры-любители) [8]. Эти категории изображены в таблице ниже.

Таблица 1

Источники киберугроз

Категория источника	Описание и мотивация	Примеры последствий
Государственные хакеры	Поддерживаемые государством группы, цели – шпионаж, саботаж, политическое влияние	Кража секретных данных, атаки на критически важную инфраструктуру
Киберпреступники	Организованные банды или одиночные хакеры, мотив – финансовая выгода (вымогатели, мошенничество)	Финансовые потери (вымогательство, мошенничество)
Хактивисты	Группы с политическими / социальными мотивами, цель – заявить о себе или нарушить деятельность объекта	Утечка данных, порча репутации, дестабилизация процессов
Инсайдеры	Сотрудники или партнеры организации, намеренно / случайно раскрывающие внутренние данные	Утечка конфиденциальных данных, нарушение процессов
Скрипт-кидди	Новички и любители, атакующие из интереса, часто используют готовые инструменты	Разовые инциденты, вторичные последствия (продажа данных)

Различные источники кибератак часто комбинируют свои усилия, что усложняет атрибуцию инцидентов. Так, аналитики Positive Technologies отмечают, что за 2024–2025 гг. хактивисты и APT-группы нанесли 18…22 % всех атак по СНГ (преимущественно на госструктуры и промышленность). В целом многофакторный характер угроз означает, что организации должны оценивать риски от внешних и внутренних источников одновременно [8, 12].

Анализ исходного датасета [19] выявил, что в 2015–2024 гг. наибольшую долю составляли атаки местных граждан, а также атаки из неустановленного источника. На рис. 1 изображены основные источники кибератак и их доля.

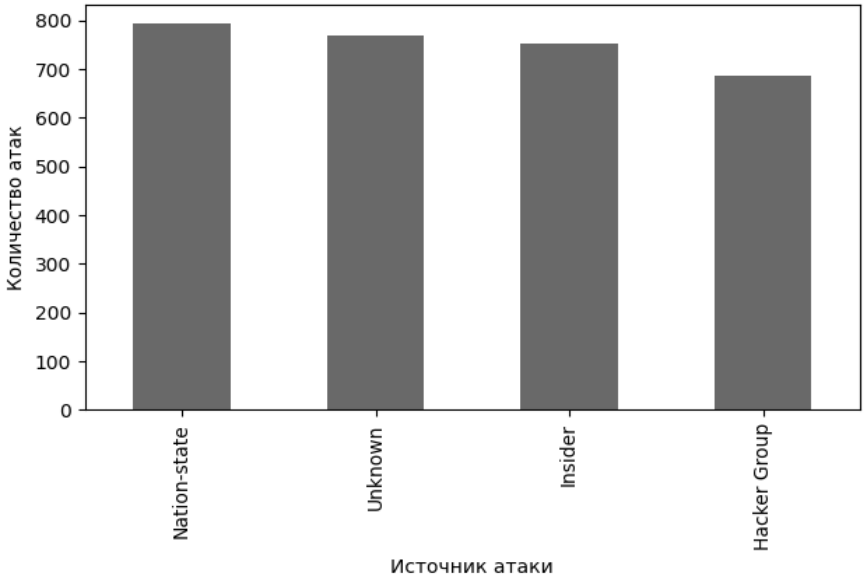

Рис. 1. Основные источники кибератак и их доля

1.2. КЛАССИФИКАЦИЯ КИБЕРАТАК

Кибератаки классифицируются по техническим методам. Наиболее распространенные из них представлены в табл. 2.

Таблица 2

Классификация типов кибератак

Тип атаки	Краткое описание	Примеры последствий
Вредоносное ПО (Malware)	Любое ПО, повреждающее систему: вирусы, трояны, руткиты, кейлогеры и др.	Кража, шифрование данных, несанкционированный вход, служебный сбой
Вымогательное ПО (Ransomware)	Особый вид вредоносного ПО, шифрующий файлы жертвы и требующий выкуп за ключ дешифрования	Паралич бизнес-процессов, убытки из-за возмещения, оплата выкупа
Фишинг (Phishing)	Социальная атака, при которой жертве отправляются фальшивые сообщения (обычно e-mail) для сбора данных	Утечка паролей, несанкционированный вход и кража данных, запуск malware
Селективный фишинг (Spear Phishing)	Таргетированная атака на конкретных пользователей или сотрудников организации, поддельные письма от имени доверенного лица	Кража учетных данных, проникновение в системы, целевые проникновения
SQL-инъекция	Внедрение вредоносного SQL-кода в запросы к базе данных (web-приложения) с получением неавторизованного доступа	Эксплуатация хранимых данных (ПДн, финансовые данные), нарушение конфиденциальности
XSS-атака (межсайтовый скриптинг)	Внедрение вредоносного скрипта в web-страницу, который выполняется в браузере пользователя	Кража сессионных cookie, подмена контента сайта, фишинговые перенаправления
DDoS/DoS (отказ в обслуживании)	Перегрузка сервера или сети огромным количеством запросов, что делает сервис недоступным	Простой сервисов, сбой доступности (сайтов, приложений), потеря выручки
MITM («человек посередине»)	Перехват и/или подмена сетевого трафика между участниками обмена данными	Кража данных при передаче (пароли, банковские операции), подмена информации
Атаки на веб-приложения	Включают ввод кода (инъекции), уязвимости авторизации и др. (OWASP Top 10)	Неавторизованный доступ, разрушение целостности данных в web-сервисах
Инсайдерские угрозы	Нежелательные действия (умышленные или ошибочные) сотрудников с доступом к системе	Утечка внутренних данных, установка malware (например, по неосторожности)

Описанные атаки часто комбинируются: злоумышленники могут начать с фишинга для проникновения, затем развернуть вымогательное ПО, использовать DDoS для отвлечения внимания и т. д. Основными целями атак являются

ключевые IT-системы и данные организаций. Как отмечают аналитики, Windows остается главной мишенью большинства кибератак, а количество обнаруживаемых вредоносных файлов растет (в среднем 467 тыс. в день в 2024 г., что на 14 % больше, чем в 2023 г.) [7]. Многие атаки связаны с известными уязвимостями (например, троянами через популярные MFT или VPN).

После анализа исходного датасета выяснилось, что за указанный период (2015–2024 гг.) зафиксированы следующие типы кибератак:

1) DDoS – 531 инцидент;
2) phishing – 529 инцидентов;
3) SQL Injection – 503 инцидента;
4) ransomware – 493 инцидента;
5) malware – 485 инцидентов;
6) man-in-the-middle – 449 инцидентов.

Анализ датасета показывает, что наибольшее количество кибератак связано с DDoS и фишингом, каждая из которых превышает 500 зафиксированных инцидентов. Незначительно меньшую долю составляют SQL-инъекции и вымогательские атаки (ransomware), что указывает на устойчивую популярность как технических, так и социально-инженерных методов атак. Наименьшее количество инцидентов связано с атаками типа MITM, однако их доля остается значимой и сопоставимой с другими категориями. Полученное распределение подтверждает многофакторный характер современных киберугроз и необходимость комплексных мер защиты. Визуализация данных из датасета представлена на рис. 2.

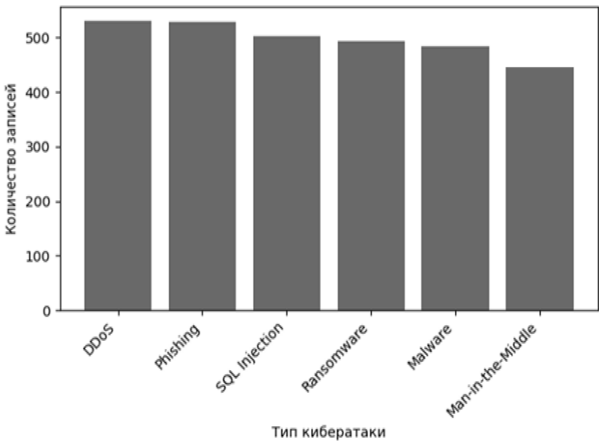

Рис. 2. Классификация типов кибератак

2. ИНТЕРПРЕТАЦИЯ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

2.1. АНАЛИЗ ИСТОЧНИКОВ АТАК

Анализ данных показывает, что в рассматриваемом периоде источники атак распределены весьма равномерно. Наибольшая доля инцидентов приходится на действия местных жителей (nation-state) – около 26 % случаев, при этом значительную часть занимают также атаки с неустановленным источником (около 25 %), инсайдерские атаки (25 %) и атаки организованных хакерских групп (22 %) (рис. 3).

Ни одна из категорий не доминирует явно, что указывает на многофакторный характер угроз и трудности в атрибуции нападений. Аналогичные выводы содержатся и в международных отчетах: например, Verizon DBIR 2024 отмечает, что внешние угрозы остаются ведущими (65 % нарушений против 35 % внутренних), однако большинство внутренних инцидентов связано с непреднамеренными ошибками персонала (73 % среди внутренних случаев) [15].

Mandiant также сообщает, что 54 % обнаруженных компрометаций выявляются извне – чаще всего через уведомления извне (например, требование выкупа при ransomware) [9].

При этом ENISA подчеркивает, что современные атакующие используют методы, затрудняющие атрибуцию: они стремятся скрыть свою причину, усложняя анализ источника атаки [15]. В целом анализ совпадает с данными датасета: источник атаки не всегда можно установить, а доля внутренних ошибок высокая, что подтверждает вывод об отсутствии «типичного» инициатора инцидентов. На рис. 3 представлено наглядное распределение источников кибератак.

2.2. АНАЛИЗ ЦЕЛЕВЫХ ОТРАСЛЕЙ

Мероприятия по кибератакам затрагивают широкий спектр отраслей. В датасете Global Cybersecurity Threats наиболее часто фигурируют отрасли «ИТ» (15,9 % случаев), «Банковское дело» (14,8 %) и «Здравоохранение» (14,3 %), далее с небольшим отставанием идут «Розничная торговля», «Образование», «Телекоммуникации» и «Государственный сектор» (по 13–14 % каждая). Такая близкая по значению доля указывает на то, что угрозы довольно равномерно распределены по перечисленным отраслям.

Сторонние отчеты поддерживают идею о широком охвате целей. Так, IBM X-Force выявила, что промышленность (manufacturing) четвертый год подряд является самой подвергаемой атакам сферой, испытывая наибольшее число случаев вымогательства и кражи данных [18]. ENISA

в отчете ETL 2024 отмечает, что в глобальном масштабе за отчетный год большинство инцидентов пришлось на государственный сектор (~19 %) и транспорт (~11 %) [15], а в отчете ETL-2023 на первом месте инциденты в области общественного управления (19 %). Аналитики Forescout указывают на то, что наиболее атакуемыми являются государственные и финансовые организации [13].

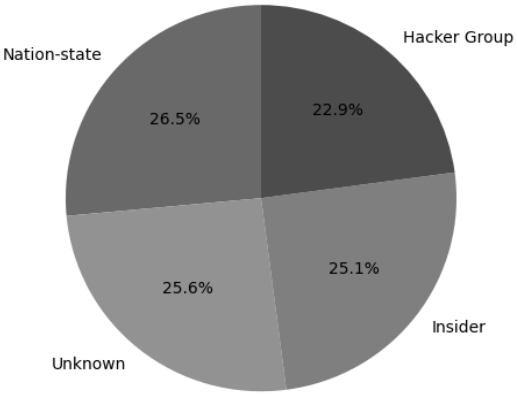

Рис. 3. Распределение источников кибератак

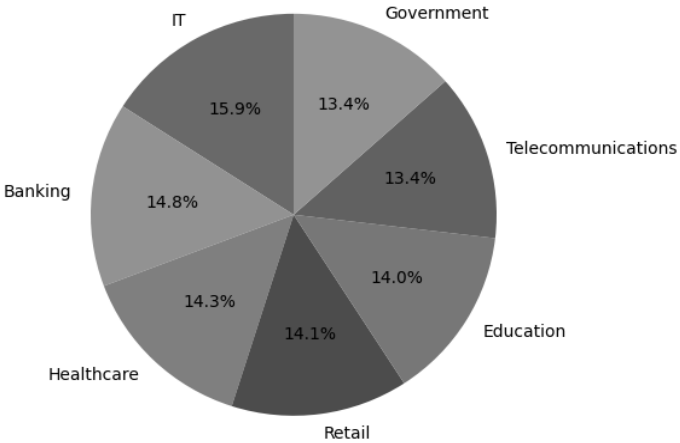

Рис. 4. Распределение целевых отраслей

Таким образом, несмотря на фокус исходного датасета на несколько категорий (который объясняет доминирование ИТ- и финансового направлений), общемировая практика показывает атаки по всем ключевым секторам экономики – от госсектора до промышленных и сервисных отраслей. Высокая представленность банков и информационных технологий в исходном датасете коррелирует с сообщениями о сильном давлении на финансовый сектор и на организации с большим ИТ-процессом, а также свидетельствует об общей «неизбирательности» киберугроз, на что указывают и ENISA, и IBM [4, 8]. Распределение целевых отраслей представлено на рис. 4.

2.3. АНАЛИЗ ПРИМЕНЯЕМЫХ МЕР ЗАЩИТЫ

Датасет фиксирует использование различных технологий защиты, причем распределение по типам средств выглядит сравнительно равномерно: около 20–21 % инцидентов сопровождалось наличием антивируса, ~20 % – VPN, шифрование ~19,7 %, межсетевой экран ~19,5 %, а системы на базе ИИ (AI-based detection) ~19,4 % случаев. Наглядное представление аналитических данных представлено на рис. 5.

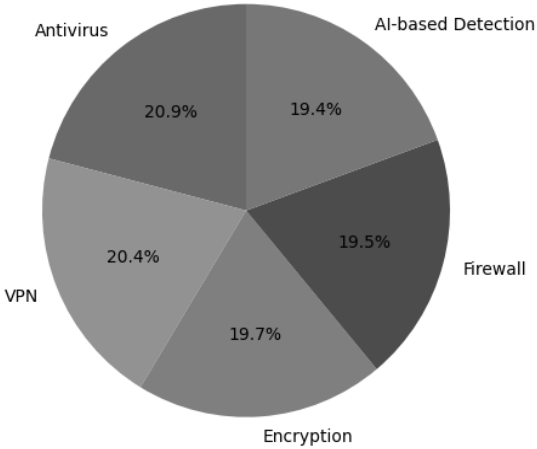

Рис. 5. Распределение применяемых мер защиты

Это отражает широкое использование традиционных мер безопасности (антивирус, брандмауэр, шифрование, VPN) наряду с современными решениями на базе машинного обучения.

Тем не менее аналитики предостерегают: наличие таких технологий далеко не гарантирует полную защиту. Например, Deloitte отмечает, что ИИ открывает новые возможности для защиты: он помогает выявлять сложные закономерности и автоматизировать реакцию на угрозы. Однако одновременно подчеркивается, что атаки становятся тоже более изощренными [17].

Более того, как указывает Verizon DBIR, большинство инцидентов связано даже не с техническими средствами, а с человеческим фактором: сотрудники сами по себе вызвали 51…68 % нарушений (ошибки и фишинг) [15, 16]. По этим данным можно сделать вывод, что традиционные инструменты (антивирус, фаерволы, шифрование и т. д.) и даже новые ИИ-системы больше снижают ущерб и облегчают обнаружение, чем полностью предотвращают атаки.

Данные в датасете подтверждают это: несмотря на то что во всех случаях использовалось, по крайней мере, одно из упомянутых средств защиты, атаки продолжались, что согласуется с выводом экспертов о необходимости комплексного подхода, включающего не только технологии, но и организационные меры (обучение персонала, аудит конфигураций и др.) [15, 17].

2.4. ВЫЯВЛЕННЫЕ ЗАКОНОМЕРНОСТИ

Анализ данных позволяет отметить устойчивые тенденции во времени и по типам атак. Временные ряды датасета показывают устойчивое сохранение активности на высоком уровне, что подтверждает выводы международных исследований о стабильно высокой интенсивности угроз [2]. Важной закономерностью стало бурное развитие новых векторов.

Так, почти 180-процентный рост использования эксплуатации уязвимостей в качестве пути в систему зафиксирован и в отчете Verizon (в том числе за счет уязвимости MOVEit и Log4Shell) [2–4]. В результате уязвимости типа zero-day и непатченных систем вышли на первый план как путь атаки. Одновременно выросли фишинговые атаки: по данным опроса Всемирного экономического форума, 42 % организаций сообщали о значительном росте фишинга в 2024 г. Практически во всех крупных отчетах по-прежнему лидирует ransomware: Verizon DBIR указывает, что в 2023 году вымогательство было одним из главных источников инцидентов (входит в 92 % отраслей), а IBM отмечает рост pure extortion и перестройку тактики преступников.

Разнообразие индустрий-мишеней остается высоким: киберпреступники совершают атаки практически на все секторы экономики (что также подтверждает ENISA: «угрозы неизбирательны, охватывают все отрасли») [15]. Таким образом, основные закономерности – это синхронный рост цифросложных

методов (эксплуатация уязвимостей, фишинг, вымогательство) и сохранение распространенности атак по всем направлениям бизнеса.

ЗАКЛЮЧЕНИЕ

Анализ инцидентов в датасете показал, что с 2015 по 2024 г. сохранялся устойчивый высокий уровень киберугроз с выявляемыми закономерностями. Ведущими источниками атак выступают как внешние группировки, так и инсайдеры, при этом значительная часть случаев связана с человеческой ошибкой. Целевые отрасли разнообразны: финансовый и государственный секторы демонстрируют высокую подверженность, в то время как наше эмпирическое распределение фиксирует максимумы в ИТ и банковском сегменте.

Инструменты защиты (антивирусы, шифрование, VPN, ИИ) широко применяются, но сами по себе не избавляют от рисков. Основные выявленные тенденции – рост атак через эксплуатацию уязвимостей, продолжение роста фишинга и ransomware – соответствуют консолидированным итогам ведущих индустриальных исследований.

Полученные результаты дают аналитическую основу для выстраивания эффективных мер безопасности, подчеркивая необходимость комплексного подхода: сочетания технологических (включая ИИ) и организационных средств, направленных на снижение последствий и предупреждение атак.

СПИСОК ЛИТЕРАТУРЫ

1. ENISA Threat Landscape 2024 / European Union Agency for Cybersecurity. – ENISA, 2024. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed: 26.02.2026).

2. 2024 Data Breach Investigations Report. – Verizon Business, 2024.

3. Mandiant. M-Trends 2024. – Google Cloud Security, 2024.

4. *Dass S., Datta P., Namin A.S.* Attack prediction using hidden Markov model // arXiv. – 2021. – URL: https://arxiv.org/pdf/2106.02012 (accessed: 26.02.2026).

5. *Engelen G., Joosen W.* Troubleshooting an intrusion detection dataset: the CICIDS2017 dataset // IEEE Security & Privacy Workshops. – IEEE, 2021. – P. 207–213. – DOI: 10.1109/SPW53761.2021.00034.

6. A systematic review of cyber threat intelligence: the effectiveness of technologies, strategies, and collaborations in combating modern threats / P. Santos, R. Abreu, M.J.C.S. Reis, C. Serôdio, F. Branco // Sensors. – 2025. – Vol. 25 (14). – P. 4272. – DOI: 10.3390/s25144272.

7. Kaspersky: The cyber surge: 467k malicious files daily in 2024. – URL: https://www.kaspersky.com/about/press-releases/the-cyber-surge-kaspersky-detected-467000-malicious-files-daily-in-2024 (accessed: 26.02.2026).

8. IBM Security. X-Force Threat Intelligence Index 2024. – IBM Corporation, 2024. – URL: https://www.ibm.com/reports/threat-intelligence (accessed: 26.02.2026).

9. Mandiant. M-Trends 2025. – Google Cloud Security, 2025. – URL: https://www.mandiant.com/resources/m-trends (accessed: 26.02.2026).

10. World Economic Forum. Global Cybersecurity Outlook 2024. – Geneva, 2024. – URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2024 (accessed: 26.02.2026).

11. Kaspersky. The cyber surge: detected malicious files in 2024. – URL: https://www.kaspersky.com/about/press-releases/the-cyber-surge-kaspersky-detected-467000-malicious-files-daily-in-2024 (accessed: 26.02.2026).

12. Positive Technologies. CIS Cyberthreat Landscape H2 2024 – Q3 2025. – 2025. – URL: https://www.ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025/ (accessed: 26.02.2026).

13. Sophos. The State of Ransomware 2024. – Sophos Group, 2024.

14. CrowdStrike. Global Threat Report 2024. – CrowdStrike, 2024.

15. ENISA Threat Landscape 2023 / European Union Agency for Cybersecurity. – ENISA, 2023. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed: 26.02.2026).

16. OWASP Foundation. OWASP Top 10 – 2023. – Open Web Application Security Project. – URL: https://owasp.org/www-project-top-ten/ (accessed: 26.02.2026).

17. Fortinet. Global Threat Landscape Report 2024. – Fortinet, 2024.

18. ISO/IEC 27001:2022. Information Security Management Systems / International Organization for Standardization. – URL: https://www.iso.org/standard/27001 (accessed: 26.02.2026).

19. *Soundankar A.* Global Cybersecurity Threats (2015–2024). – URL: https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024 (accessed: 26.02.2026).

Мартынов Андрей Сергеевич, аспирант Московского финансово-юридического университета. E-mail: doskam@narod.ru

Алексеев Никита Александрович, лаборант кафедры вычислительной математики и кибернетики факультета математики и компьютерных наук имени профессора Н.А. Червякова Северо-Кавказского федерального университета. E-mail: helpmetobesad@bk.ru

Лапин Виталий Геннадьевич, доцент кафедры вычислительной математики и кибернетики факультета математики и компьютерных наук имени профессора Н.А. Червякова Северо-Кавказского федерального университета. E-mail: vitlx@yandex.ru

DOI: 10.17212/2782-2230-2026-1-69-83

Features of cyberattack forecasting based on data analysis*

A.S. Martynov[1], N.A. Alekseev[2], V.G. Lapin[3]

[1] *Moscow University of Finance and Law, 17 Serpukhovsky Val Street, apt. 1, internal territory of the municipal district of Danilovsky, Moscow, 115191, Russian Federation, postgraduate student, doskam@narod.ru*
[2] *North Caucasus Federal University, 1 Pushkin Street, Stavropol, 355017, Russian Federation, laboratory assistant of the Department of Computational Mathematics and Cybernetics. E-mail: helpmetobesad@bk.ru*
[3] *North Caucasus Federal University, 1 Pushkin Street, Stavropol, 355017, Russian Federation, Associate Professor of the Department of Computational Mathematics and Cybernetics. E-mail: vitlx@yandex.ru*

An analytical review of modern cyberattacks based on an analysis of the Global Cybersecurity Threats open statistical dataset for the period 2015–2024. The main sources of cyberattacks, target industries, types of threats, and protective measures used are considered. Particular attention is paid to identifying consistent patterns in the distribution of attacks, as well as analyzing the relationships between threat sources, industry affiliation of organizations, and information security measures used. Empirical data shows that cyber threats are multifactorial and persistent in nature, while the absence of a dominant type of attack or source underscores the complexity of predicting and attributing them. The results obtained can be used to improve the effectiveness of information security systems and develop analytically sound measures to counter cyber threats.

Keywords: cyberattacks; cybersecurity; data analysis; information security; sources of attacks; target industries; protective measures

REFERENCES

1. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2024*. ENISA, 2024. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed 26.02.2026).

2. *2024 Data Breach Investigations Report*. Verizon Business, 2024.

* *Received 14 February 2026.*

3. Mandiant. *M-Trends 2024*. Google Cloud Security, 2024.

4. Dass S., Datta P., Namin A.S. Attack prediction using hidden Markov model. *arXiv*, 2021. Available at: https://arxiv.org/pdf/2106.02012 (accessed 26.02.2026).

5. Engelen G., Joosen W. Troubleshooting an intrusion detection dataset: the CICIDS2017 dataset. *IEEE Security & Privacy Workshops*, 2021, pp. 207–213. DOI: 10.1109/SPW53761.2021.00034.

6. Santos P., Abreu R., Reis M.J.C.S., Serôdio C., Branco F. A systematic review of cyber threat intelligence: the effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*, 2025, vol. 25 (14), p. 4272. DOI: 10.3390/s25144272.

7. Kaspersky. *The cyber surge: 467k malicious files daily in 2024*. Available at: https://www.kaspersky.com/about/press-releases/the-cyber-surge-kaspersky-detected-467000-malicious-files-daily-in-2024 (accessed 26.02.2026).

8. IBM Security. *X-Force Threat Intelligence Index 2024*. IBM Corporation, 2024. Available at: https://www.ibm.com/reports/threat-intelligence (accessed 26.02.2026).

9. Mandiant. *M-Trends 2025*. Google Cloud Security, 2025. Available at: https://www.mandiant.com/resources/m-trends (accessed 26.02.2026).

10. World Economic Forum. *Global Cybersecurity Outlook 2024*. Geneva, 2024. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2024 (accessed 26.02.2026).

11. Kaspersky. *The cyber surge: detected malicious files in 2024*. Available at: https://www.kaspersky.com/about/press-releases/the-cyber-surge-kaspersky-detected-467000-malicious-files-daily-in-2024 (accessed 26.02.2026).

12. Positive Technologies. *CIS Cyberthreat Landscape H2 2024 – Q3 2025*. 2025. Available at: https://www.ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025/ (accessed 26.02.2026).

13. Sophos. *The State of Ransomware 2024*. Sophos Group, 2024.

14. CrowdStrike. *Global Threat Report 2024*. CrowdStrike, 2024.

15. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2023*. ENISA, 2023. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed 26.02.2026).

16. OWASP Foundation. *OWASP Top 10 – 2023*. Open Web Applica-tion Security Project. Available at: https://owasp.org/www-project-top-ten/ (accessed 26.02.2026).

17. Fortinet. *Global Threat Landscape Report 2024*. Fortinet, 2024.

18. ISO/IEC 27001:2022. *Information Security Management Systems*. International Organization for Standardization. Available at: https://www.iso.org/standard/27001 (accessed 26.02.2026).

19. Soundankar A. *Global Cybersecurity Threats (2015–2024)*. Available at: https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024 (accessed 26.02.2026).

Для цитирования:

Мартынов А.С., *Алексеев Н.А, Лапин В.Г.* Особенности прогнозирования кибератак на основе анализа данных // Безопасность цифровых технологий. – 2026. – № 1 (120). – С. 69–83. – DOI: 10.17212/2782-2230-2026-1-69-83.

For citation:

Martynov A.S., Alekseev N.A., Lapin V.G. Osobennosti prognozirovaniya kiberatak na osnove analiza dannykh [Features of cyberattack forecasting based on data analysis]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 1 (120), pp. 69–83. DOI: 10.17212/2782-2230-2026-1-69-83.