Вестник МИРБИС. 2025. № 4 (44)′. С. 109–115.
Vestnik MIRBIS. 2025; 4 (44)′:109–115.

Научная статья
УДК: 004.8:004.056
DOI: 10.25634/MIRBIS.2025.4.13

Искусственный интеллект в кибербезопасности

Никита Евгеньевич Прибытков[1,2], **Филипп Геннадьевич Ванюрихин**[1,3]

Аннотация. Современный рост количества и сложности киберугроз ставит под сомнение эффективность традиционных методов защиты. Инструменты кибербезопасности на основе искусственного интеллекта (ИИ) и машинного обучения позволяют анализировать огромные массивы данных и выявлять атаки на ранних стадиях, включая ранее неизвестные угрозы, что недостижимо статическими сигнатурными системами. В данной статье представлены результаты исследования технологий ИИ в сфере информационной безопасности: рассмотрены современные подходы (машинное обучение, нейросетевые алгоритмы, поведенческий анализ и др.) и их применение для обнаружения вторжений, вредоносного кода и аномалий; проанализированы практические кейсы внедрения ИИ в кибербезопасности в российских и зарубежных организациях (банковский сектор, корпорации, госсектор); описаны методологии и модели, используемые для выявления кибератак (SVM, Decision Tree, K-Means, CNN, Autoencoder и др.), а также приведены примеры инструментов и платформ (IBM Watson, решения «Лаборатории Касперского», OpenAI Codex, разработки Сколтеха и др.). Выполнен сравнительный анализ возможностей ИИ-систем и традиционных методов киберзащиты. Отдельное внимание уделяется ограничениям и рискам, связанным с внедрением ИИ: непрозрачности моделей, уязвимостям алгоритмов, дефициту кадров и др. В заключение определены перспективы развития ИИ в кибербезопасности. Результаты подтверждают, что искусственный интеллект становится ключевым компонентом проактивной защиты от кибератак, однако эффективное его использование требует преодоления текущих вызовов и формирования доверия к интеллектуальным системам.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, обнаружение угроз, нейронные сети, поведенческий анализ, информационная безопасность.

Для цитирования: Прибытков Н. Е. Искусственный интеллект в кибербезопасности / Н. Е. Прибытков, Ф. Г. Ванюрихин. DOI: 10.25634/MIRBIS.2025.4.13 // Вестник МИРБИС. 2025; 4:109–115.

JEL: O31, O32, O33

Original article

Artificial intelligence in cybersecurity

Nikita E. Pribytkov[4,5], **Philipp G. Vanyurikhin**[4,6]

Abstract. The modern increase in the number and complexity of cyber threats challenges the effectiveness of traditional protection methods. Artificial intelligence (AI) and machine learning-based cybersecurity tools enable the analysis of massive volumes of data and the detection of attacks at early stages, including previously unknown threats—something static signature-based systems cannot achieve. This article presents the results of a study on AI technologies in the field of information security. It explores modern approaches (machine learning, neural network algorithms, behavioral analysis, etc.) and their application for intrusion detection, malware identification, and anomaly detection. Practical cases of AI implementation in cybersecurity across Russian and international organizations (banking sector, corporations, public sector) are analyzed. The article describes the methodologies and models used to identify cyberattacks (SVM, Decision Tree, K-Means, CNN, Autoencoder, and others), along with examples of tools and platforms (IBM Watson, Kaspersky Lab solutions, OpenAI Codex, Skoltech developments, etc.).

1 Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия.
2 n.pribytkov_04@mail.ru
3 Vanyurikhin_fg@pfur.ru
4 Peoples' Friendship University of Russia named after Patrice Lumumba, Moscow, Russia.
5 n.pribytkov_04@mail.ru
6 Vanyurikhin_fg@pfur.ru

A comparative analysis of the capabilities of AI systems versus traditional cybersecurity methods is provided. Particular attention is given to the limitations and risks associated with AI implementation: model opacity, algorithmic vulnerabilities, talent shortages, and more. The article concludes by outlining the prospects for AI development in cybersecurity. The review's findings confirm that artificial intelligence is becoming a key component of proactive cyberattack defense, though its effective use requires overcoming current challenges and building trust in intelligent systems.

Key words: artificial intelligence, cybersecurity, machine learning, threat detection, neural networks, behavioral analysis, information security.

For citation: Pribytkov N. E. Artificial intelligence in cybersecurity. By N. E. Pribytkov, Ph. G. Vanyurikhin. DOI: 10.25634/MIRBIS.2025.4.13. *Vestnik MIRBIS*. 2025; 4:109–115 (in Russ.).

JEL: O31, O32, O33

Введение

Активное развитие цифровой экономики и глобальной сети сопровождается экспоненциальным ростом кибератак и новых видов угроз. По данным аналитиков McKinsey, в период с 2021 по 2022 год общее число киберугроз в мире увеличилось на 200%. Ожидается, что к 2025 году глобальный ущерб от кибератак достигнет астрономической величины в $10,5$ трлн долларов [Овчинников 2024]. Одновременно усложняется и ландшафт угроз. Так, в 2023 году четверть опрошенных пользователей лично столкнулись с мошенничеством, выполненным с помощью подделки голоса через ИИ, причём 77 % из них понесли финансовые потери. Традиционные средства кибербезопасности часто оказываются недостаточно эффективными перед лицом таких сложных и новых атак. Применение искусственного интеллекта в информационной безопасности стало насущной необходимостью, поскольку человек, даже обладая высокой квалификацией, не способен оперативно обработать колоссальные объёмы данных, генерируемых современными информационными системами [там же].

ИИ предоставляет кибербезопасности новые качества: динамичность и адаптивность. Вместо предустановленных правил и сигнатур, интеллектуальные модели обучаются на больших массивах данных и способны самостоятельно обнаруживать аномальные паттерны, соответствующие потенциально вредоносной активности. Это означает переход от реактивной защиты к проактивной — предугадыванию и предотвращению атак на ранних стадиях. Например, поведенческие алгоритмы способны обучиться профилю нормальной активности пользователей и узлов сети и мгновенно сигнализировать о любых отклонениях, характерных для атаки, ещё до причинения ущерба. Кроме того, технологии ИИ позволяют автоматизировать рутинные операции киберзащиты, тем самым значительно ускоряя время обнаружения и реагирования на атаки.

Актуальность темы обусловлена не только ростом угроз, но и доступностью ИИ как для защитников, так и для злоумышленников.

Цель данной работы — выполнить всесторонний обзор технологий искусственного интеллекта.

Методология исследования

1. Методологическую основу исследований составляют:
2. Анализ современных ИИ-методов обеспечения информационной безопасности [Deep Learning-based... 2021; 7-10];
3. Изучение аналитических отчётов и материалов профессиональных организаций [Овчинников 2024; Искусственный интеллект в информационной... 2024; «Т-Банк» создал ИИ-ассистента... 2025; Кибербезопасность и искусственный интеллект 2025];
4. Сравнительный анализ архитектур и алгоритмов (SVM, Random Forest, K-Means, CNN, Autoencoder и др.);
5. Исследование практических кейсов внедрения решений на базе ИИ в финансовом, корпоративном и промышленном секторах [«Т-Банк» создал ИИ-ассистента... 2025; Соловьев 2025; Кибербезопасность и искусственный интеллект 2025].

Использовались методы контент-анализа, систематизации и сравнительного анализа.

Результаты исследования

Машинное обучение и анализ данных. Классические алгоритмы МО нашли широкое применение в системах кибербезопасности. На этапе

обнаружения атак алгоритмы классификации обучаются различать «злоумышленное» поведение по множеству признаков сетевого трафика, системных вызовов, файловых характеристик и т. д. Например, в решениях «Лаборатории Касперского» для выявления продвинутых угроз используются алгоритмы Random Forest и анализ TF-IDF, обрабатывающие огромные объёмы телеметрии со множества устройств. Это позволяет выделять едва заметные индикаторы компрометации, которые могли бы ускользнуть от традиционных сигнатурных систем, и тем самым повысить общий уровень обнаружения атак на 25 % [Овчинников 2024]. С другой стороны, неподконтрольное обучение позволяет искать аномалии без заранее размеченных данных [Deep Learning-based... 2021]. Методики кластеризации (например, K-Means) группируют схожие события и выявляют выбросы — потенциально подозрительную активность, ранее не встречавшуюся. Такой поведенческий анализ строит профиль нормы для пользователей и систем и сигнализирует о нетипичном отклонении, что особенно эффективно против новых, неизвестных угроз.

Глубокое обучение и нейросети. Современные нейронные сети находят применение в задачах кибербезопасности, требующих выявления сложных нелинейных зависимостей. Рекуррентные нейросети используются для анализа последовательностей событий во времени — системных логов, серий сетевых запросов, команд, вводимых злоумышленником. Они позволяют улавливать временные зависимости и паттерны, предшествующие атаке, что помогает в выявлении целевых атак и APT-кампаний [Deep Learning Approaches... 2025]. Автоэнкодеры — ещё один распространённый тип нейросетевых моделей — применяются для детектирования аномалий: автоэнкодер обучается сжимать и восстанавливать данные, характеризующие нормальную работу системы, а при поступлении отклоняющихся данных ошибка реконструкции резко возрастает, сигнализируя о возможной атаке [Autoencoder Based Network... 2020]. Такой подход показал эффективность в обнаружении сетевых аномалий, скрытого вредоносного трафика и даже в выявлении мошенничества в финансовых транзакциях. Наконец, генеративные модели (например, GAN — генеративно-состязательные сети) находят применение как для атаки, так и для защиты: злоумышленники могут генерировать реалистичные фишинговые письма или изображения (дипфейки) для обмана систем и людей, а специалисты по защите используют GAN для создания искусственных данных, на которых можно обучать детекторы без риска утечки реальной информации, или для тестирования моделей на устойчивость (генерируя адверсарные примеры — особым образом изменённые входные данные, способные ввести ИИ в заблуждение).

Интеллектуальный анализ содержимого (NLP и др.). ИИ активно применяется для понимания и фильтрации текстовой и мультимедийной информации с целью обеспечения безопасности. Алгоритмы обработки естественного языка (NLP) используются в системах фильтрации спама и фишинга: современные модели (например, трансформеры вроде BERT и GPT) способны анализировать содержание писем, сообщений и веб-страниц, выявляя в них социально-инженерные уловки, признаки фишинга или команд управления malware [Ogundairo 2024].

Предиктивная аналитика и Threat Intelligence. ИИ-технологии позволяют повысить эффективность разведки угроз (Threat Intelligence) за счёт автоматического сбора и анализа открытых источников, теневых форумов, данных о новых уязвимостях и атаках. Например, алгоритмы могут проанализировать сообщения хакерских форумов и заранее обнаружить планы кампаний или обсуждение эксплойтов, ещё до того как атака реализована [Искусственный интеллект в информационной... 2024]. Кроме того, на основе статистики прошлых атак ИИ-модели строят прогнозы наиболее вероятных векторов нападения на конкретную организацию с учётом её профиля и уязвимостей, что помогает проактивно усилить защиту на этих направлениях. Такие прогнозирующие модели риска уже внедряются в SOC (центрах мониторинга безопасности), позволяя распределять ресурсы на наиболее критичные угрозы.

Автоматизация и ответные действия. Ещё одно преимущество ИИ в кибербезопасности — способность ускорять реагирование на инциденты и даже выполнять часть операций автоматически в режиме реального времени. Современные решения класса SOAR (Security Orchestration, Automation and Response), интегрированные с ИИ, могут самостоятельно проводить расследование

типовых инцидентов по заданным параметрам и даже предпринимать защитные меры без участия человека. Например, компания IBM сообщает, что её система IBM Security QRadar с ИИ-помощником может автоматически обрабатывать до 85 % оповещений о безопасности, самостоятельно повышая или понижая их критичность, и тем самым снимать с аналитиков рутинную нагрузку [Овчинников 2024]. А включение генеративного ИИ в контур SOC позволило сократить время расследования оставшихся сложных инцидентов почти наполовину за счёт автоматического суммирования данных, корреляции событий и рекомендаций по реагированию. Похожий подход реализован и в новом сервисе Microsoft Security Copilot, где модель GPT-4 обрабатывает сигналы и логирует инциденты, отвечая на запросы аналитиков в диалоговом режиме и предлагая шаги по устранению угроз. Таким образом, ИИ не только обнаруживает атаки, но и значительно повышает эффективность этапа реагирования, уменьшая «время жизни» угрозы в системе.

Подводя итог, современные технологии ИИ охватывают весь цикл кибербезопасности: от мониторинга и обнаружения аномалий до анализа инцидентов, предиктивной аналитики и автоматизации защитных мер. Благодаря машинному обучению и нейросетям системы киберзащиты стали более адаптивными, проактивными и масштабируемыми. В следующем разделе рассмотрим примеры реального внедрения этих технологий в организациях различных секторов.

Обзор практики применения ИИ

Подводя итог: современные технологии ИИ охватывают весь цикл кибербезопасности: от мониторинга и обнаружения аномалий до анализа инцидентов, предиктивной аналитики и автоматизации защитных мер. Благодаря машинному обучению и нейросетям системы киберзащиты стали более адаптивными, проактивными и масштабируемыми. В следующем разделе рассмотрим примеры реального внедрения этих технологий в организациях различных секторов.

Практический опыт показывает, что использование искусственного интеллекта уже приносит ощутимые результаты в защите информации. Рассмотрим несколько конкретных кейсов внедрения ИИ-решений в кибербезопасности, как в российских компаниях, так и за рубежом, включая банковский сектор и корпоративные системы.

Финансовые организации традиционно находятся в авангарде внедрения инноваций в ИБ, поскольку сталкиваются с постоянными кибератаками и мошенничеством. Яркий пример — группа «Тинькофф» («Т Банк»), которая в 2024 году разработала первого в России ИИ-ассистента по информационной безопасности под названием Safeliner. Его задача — помочь защищать программные продукты банка на этапе разработки и эксплуатации. Safeliner интегрирован в среду разработки (GitLab) и использует большую языковую модель (LLM) для анализа исходного кода на наличие уязвимостей и выдачи разработчикам рекомендаций по исправлению [«Т-Банк» создал ИИ-ассистента... 2025]. Если статический анализ кода обнаруживает потенциально опасное место, ИИ-ассистент фильтрует ложные срабатывания, доступным языком поясняет суть проблемы и тут же предлагает исправленный фрагмент кода, который разработчику остаётся лишь утвердить. Все вычисления происходят внутри контура компании, без обращения к внешним API, что важно для сохранения конфиденциальности кода. В результате внедрения Safeliner процессы поиска и устранения уязвимостей у «Тинькофф» ускорились до 5 раз, а количество ошибок безопасности в выпуске продуктов значительно снизилось. Оценочный экономический эффект — экономия свыше 1 млрд руб. в год за счёт предотвращённых инцидентов и оптимизации трудозатрат. Кроме того, банк планирует предоставить Safeliner как сервис и другим компаниям, что говорит о высокой уверенности в решении. Этот кейс демонстрирует возможности сдвига влево (shift-left) в безопасности с помощью ИИ — устранения уязвимостей ещё на этапе их появления, до того как они смогут быть эксплуатированы злоумышленниками.

Российские банки применяют ИИ не только для защиты приложений, но и для противодействия мошенничеству и кибератакам. Так, в СМИ отмечалось, что один из банков с помощью собственной платформы на базе ИИ предотвратил хищения более чем на 500 млн рублей всего за короткий период. Системы fraud detection на базе машинного обучения анализируют поведение клиентов и транзакции в режиме реального времени, мгновенно блокируя подозрительные переводы [Овчинников 2024]. Например, ИИ способен учитывать десятки факторов (геолокацию,

время операции, тип получателя, историю активности клиента) и присваивать динамический риск-балл каждой транзакции. Если совокупный риск превышает порог — операция помечается как потенциально мошенническая и требует дополнительного подтверждения. Благодаря обучению на исторических данных о мошенничествах такие модели выявляют сложные схемы (череда мелких переводов, «разогрев» счёта, подмена SIM-карт и т. п.), недоступные для жёстко прописанных правил. По данным компании Тинькофф, её сервис «Ловушка для мошенников» с ИИ-определением звонков уже не первый год помогает блокировать телефонное мошенничество, автоматически фильтруя подозрительные вызовы и предотвращая социальную инженерию клиентов.

Корпорации и промышленные компании. Крупные бизнес-структуры активно внедряют решения на базе ИИ для защиты своих информационных систем и интеллектуальной собственности. Применение варьируется от продуктов сторонних вендоров до разработок in-house. Один из мировых лидеров кибербезопасности — Darktrace (Великобритания) — предлагает корпоративным клиентам платформу Enterprise Immune System, которая использует передовые алгоритмы машинного и глубокого обучения для мониторинга сетевого трафика организации. Система в автономном режиме строит «иммунитет» — профиль нормальной активности — и способна мгновенно обнаруживать отклонения, свидетельствующие о проникновении или внутренней угрозе [Кибербезопасность и искусственный интеллект 2025]. Дополнительный модуль Darktrace Antigena выполняет автоматическое реагирование: при выявлении атаки он без участия человека изолирует заражённые устройства или блокирует подозрительные соединения, предотвращая развитие инцидента. Подобные системы уже используются тысячами компаний по всему миру для защиты корпоративных сетей, включая банки, телекоммуникационные и промышленные предприятия.

Другой пример — американская фирма CrowdStrike, специализирующаяся на защите конечных точек. Её флагманский продукт CrowdStrike Falcon оснащён ИИ-модулем, анализирующим поведение процессов на рабочих станциях и серверах. Falcon отслеживает сотни параметров активности в системе и при помощи алгоритмов машинного обучения отличает нормальную работу приложений от вредоносной (например, шифрование файлов ransomware, попытки эскалации привилегий и пр.). Важной частью является аналитика поведенческих индикаторов (UBA): Falcon накапливает профили пользователей и устройств и обнаруживает аномалии, например, если учетная запись администратора вдруг выполняет действия, ей не свойственные (массовое создание аккаунтов, остановка служб безопасности), то срабатывает мгновенное оповещение. По данным CrowdStrike, их ИИ-система позволяет автоматизировать до 88 % рутинных расследований инцидентов на рабочих станциях и существенно сокращает время от выявления атаки до ее локализации [там же]. Решения CrowdStrike применяются в организациях здравоохранения, розничной торговли, финансового сектора по всему миру.

Корпорации также используют AI для защиты веб-приложений и облачных систем. Например, компания Fortinet интегрировала ИИ в свои межсетевые экраны: брандмауэр FortiGate с поддержкой AI анализирует сетевые сессии, выявляя угрозы на основе паттернов трафика, и может автоматически применять фильтры и правила в ответ на обнаруженную атаку [там же]. Веб-экран FortiWeb с элементами МО отслеживает поведение пользователей на сайтах и посредством машинного обучения вычисляет вероятности того, что определённая последовательность запросов является атакой (SQL-инъекцией, XSS и пр.). Этот подход позволяет блокировать даже те атаки, сигнатуры которых ещё не внесены в базы, — за счёт поведенческих аномалий и вероятностного анализа. Подобные решения от Palo Alto Networks (например, платформа Cortex XDR) совмещают анализ телеметрии с рабочих станций, сетей и облака, применяя ML/DL-алгоритмы для выявления угроз и координации защиты на разных узлах инфраструктуры. Palo Alto заявляет, что их ИИ-системы помогают таким клиентам, как Salesforce, в режиме реального времени отсекать сложные атаки и вредоносные активности, которые раньше могли оставаться незамеченными.

Выводы

Проведённый анализ демонстрирует, что:

- ИИ значительно повышает эффективность обнаружения угроз, обеспечивая проак-

тивную защиту;
- модели МО и глубокого обучения успешно выявляют сложные аномалии и новые типы атак;
- ИИ снижает нагрузку на специалистов, автоматизирует этапы реагирования и расследования;
- в реальных кейсах внедрение ИИ приводит к существенному снижению рисков и экономии ресурсов;
- ключевыми проблемами остаются непрозрачность моделей, уязвимости ИИ, дефицит квалифицированных кадров.

Искусственный интеллект становится критически важным компонентом современной кибербезопасности, однако для его эффективного применения требуется развитие методологии, нормативной базы и повышение доверия к интеллектуальным системам.

Список источников

1. Искусственный интеллект в информационной... 2024 — Искусственный интеллект в информационной безопасности: добро или зло. Текст : электронный // B-152 : сайт. 25/06/24. URL: https://b-152.ru/iskusstvennyj-intellekt-v-ib# (дата обращения: 30.11.2024).
2. Кибербезопасность и искусственный интеллект 2025 — Кибербезопасность и искусственный интеллект. // Falcongaze : официальный сайт компании 21.10.2025. URL: https://falcongaze.com/ru/pressroom/publications/kiberbezopasnost/kiberbezopasnost-i-iskusstvennyj-intellekt.html (дата обращения: 03.09.2025).
3. Овчинников 2024 — Овчинников А. Как ИИ помогает кибермошенникам и противостоит им. Текст : электронный// РБК : сайт Группы компаний, объединяющая медиа, IT-сервисы и инфраструктуру для бизнеса. Как ИИ помогает кибермошенникам и противостоит им. 09/12/2024. URL: https://trends.rbc.ru/trends/industry/6756bcfb9a7947690bdc259a (дата обращения: 03.09.2025).
4. Соловьев 2025 — Соловьев Д. Лучшие AI-компании в области кибербезопасности. Текст : электронный // RecoverIT : станица сайта компании Wondershare. 06/01/2025. URL: https://recoverit.wondershare.com.ru/windows-computer-tips/ai-cybersecurity-companies.html (дата обращения: 03.09.2025).
5. «Т-Банк» создал ИИ-ассистента... 2025 — «Т-Банк» создал ИИ-ассистента в сфере кибербезопасности. Текст : электронный // CNews : сетевое издание. URL: https://safe.cnews.ru/news/line/2025-05-21_t-bank_sozdal_ii-assistenta (дата обращения: 03.09.2025).
6. Autoencoder Based Network... 2020 — Autoencoder Based Network Anomaly Detection. By Mukkesh Ganesh and Akshay Kumar. DOI:10.1109/TEMSMET51618.2020.9557464 // 2020 IEEE International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET), 2020. URL: URL:https://www.researchgate.net/publication/355327124_Autoencoder_Based_Network_Anomaly_Detection (дата обращения: 03.09.2025).
7. Deep Learning Approaches... 2025 — Deep Learning Approaches Deep Learning Approaches for Malware Detection: A Comprehensive Review of Techniques, Challenges, and Future Directions. By Mohammad Alshoulie and Abid Mehmood. DOI: 10.1109/ACCESS.2025.3582875 // IEEE Access, 2025. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11048875 (дата обращения: 30.09.2025).
8. Deep Learning-based... 2021 — Deep Learning-based Intrusion Detection Systems: A Survey. By Zhiwei Xu [et al.] URL: https://arxiv.org/html/2504.07839v3 (дата обращения: 30.11.2024).

References

1. Iskusstvennyy intellekt v informatsionnoy bezopasnosti: dobro ili zlo [Artificial Intelligence in Information Security: Good or Evil]. Text : online. *B-152* : website. 06/25/24. Available at: https://b-152.ru/iskusstvennyj-intellekt-v-ib# (accessed: 11/30/2024) (in Russ.).
2. Kiberbezopasnost' i iskusstvennyy intellekt [Cybersecurity and Artificial Intelligence]. Text : online. *Falcongaze* : official company website, 10/10/2025. Available at: https://falcongaze.com/ru/pressroom/publications/kiberbezopasnost/kiberbezopasnost-i-iskusstvennyj-intellekt.html (accessed: 09/03/2025) (in Russ.).
3. Ovchinnikov A. How AI Helps and Counters Cybercriminals. Text : online. *RBC* : website of the Group of Companies, uniting media, IT services, and business infrastructure. 12/09/2024. Available at: https://trends.rbc.ru/trends/industry/6756bcfb9a7947690bdc259a (accessed: 09/03/2025) (in Russ.).
4. Soloviev D. Luchshiye AI-kompanii v oblasti kiberbezopasnost [The Best AI Companies in Cybersecurity]. Text : online. *RecoverIT* : Wondershare website. 06/01/2025. Available at: https://recoverit.wondershare.com.ru/windows-computer-tips/ai-cybersecurity-companies.html (accessed: 09/03/2025) (in Russ.).

5. "T-Bank" sozdal II-assistenta v sfere kiberbezopasnosti [T-Bank Creates an AI Assistant in Cybersecurity]. Text : online. *CNews* : online publication. Available at: https://safe.cnews.ru/news/line/2025-05-21_t-bank_sozdal_ii-assistenta (accessed: 09/03/2025) (in Russ.).
6. Autoencoder Based Network Anomaly Detection. By Mukkesh Ganesh and Akshay Kumar. DOI:10.1109/TEMSMET51618.2020.9557464. *2020 IEEE International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET)*, 2020. Available at: URL:https://www.researchgate.net/publication/355327124_Autoencoder_Based_Network_Anomaly_Detection (accessed: 09/03/2025).
7. Deep Learning Approaches Deep Learning Approaches for Malware Detection: A Comprehensive Review of Techniques, Challenges, and Future Directions. By Mohammad Alshoulie and Abid Mehmood. DOI: 10.1109/ACCESS.2025.3582875. *IEEE Access*, 2025. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11048875 (accessed: 09/03/2025).
8. *Deep Learning-based Intrusion Detection Systems: A Survey*. By Zhiwei Xu [et al.] Available at: https://arxiv.org/html/2504.07839v3 (accessed: 11/30/2024).

Информация об авторах:

Прибытков Никита Евгеньевич — студент, Высшая школа управления; **Ванюрихин Филипп Геннадьевич** — доцент Высшей школы управления, SPIN-код: 4419-7769, AuthorID: 546770.

Место работы авторов: федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы», ул. Миклухо-Маклая, 6, Москва, 117198, Россия.

Information about the authors:

Pribytkov Nikita E. — student, Higher School of Management; **Vanyurikhin Philipp G.** — associate professor, Higher School of Management, SPIN-code: 4419-7769, AuthorID: 546770.

Place of work of the authors: Peoples' Friendship University of Russia named after Patrice Lumumba, 6 Miklukho-Maklaya St., Moscow, 117198, Russia.

Статья поступила в редакцию 30.09.2025; одобрена после рецензирования 17.10.2025; принята к публикации 28.11.2025.
The article was submitted 09/30/2025; approved after reviewing 10/17/2025; accepted for publication 11/28/2025.