УДК 004.056.52

Управление доступом с использованием искусственного интеллекта: возможности и риски

Блюм Владислав Станиславович — канд. техн. наук, доцент кафедры бизнес-информатики и менеджмента. Область научных интересов: иммунокомпьютинг, технологии искусственного интеллекта. E-mail: vladblum7@gmail.com

Григорьева Дарья Алексеевна — студент кафедры бизнес-информатики и менеджмента. Область научных интересов: информационные технологии. E-mail: daria_grig4221@mail.ru

Санкт-Петербургский государственный университет аэрокосмического приборостроения, Россия, 190000, Санкт-Петербург, ул. Большая Морская, 67

Для цитирования: Блюм В. С., Григорьева Д. А. Управление доступом с использованием искусственного интеллекта: возможности и риски // Интеллектуальные технологии на транспорте. 2024. № 4 (40). С. 5–12. DOI: 10.20295/2413-2527-2024-440-5-12

Аннотация. *В современных условиях компаниям необходимо своевременно внедрять новые технологии и следить за выполнением требований по информационной безопасности, чтобы эффективно противостоять современным угрозам. Одним из основных инструментов, обеспечивающих должный уровень информационной безопасности на предприятии и упрощающих контроль за предоставлением доступа к ресурсам организации, являются системы управления доступом.* ***Основная цель:*** *исследовать возможности применения искусственного интеллекта для систем управления доступом, выделяя его значение в контексте повышения уровня информационной безопасности организации и эффективности управления правами доступа.* ***Метод исследования:*** *анализ современных инструментов и технологий, включая искусственный интеллект и большие языковые модели, а также оценка практических кейсов внедрения ИИ в системы управления доступом. Рассматриваются как преимущества, так и риски, связанные с автоматизацией управления доступом с использованием ИИ.* ***Практическая значимость:*** *результаты работы могут быть использованы организациями для повышения безопасности и эффективности управления доступом к информационным ресурсам. Выявленные риски и рекомендации по внедрению технологий ИИ позволят компаниям более осознанно подходить к улучшению процессов информационной безопасности.*

Ключевые слова: *система управления доступом, информационная безопасность, защита информации, идентификация, аутентификация, контроль прав доступа, автоматизация, ролевая модель, IDM, IAM, IGA*

1.2.1 *— искусственный интеллект и машинное обучение (технические науки);* ***2.3.6*** *— методы и системы защиты информации, информационная безопасность (технические науки)*

Введение

В последние годы искусственный интеллект (ИИ) играет все более значимую роль в управлении различными процессами и информационными системами (ИС). Его потенциал для оптимизации, автоматизации и анализа данных меняет традиционные подходы к управлению бизнесом и общественными структурами. ИИ становится ключевым элементом, способным трансформировать экономику и организационные процессы, делая их более гибкими и эффективными.

ИИ влияет на управление в различных отраслях — от производства до логистики, в связи с этим становится актуальной оценка не только текущей ситуации, но и дальнейших перспектив, а также рассмотрение возможных рисков и вызовов.

Особенности и возможности искусственного интеллекта и больших языковых моделей

Основные характеристики ИИ включают в себя способность к обучению, решению проблем, распознаванию образов, пониманию языка и принятию решений [1]. Все это делает его перспективным инструментом в управленческом аппарате для организаций. Поэтому сейчас ИИ активно используется в стратегическом планировании и поддержке принятия управленческих решений, анализируя большие объемы данных и прогнозируя развитие событий. Это позволяет руководителям эффективно управлять рисками, оптимизировать ресурсы и снижать издержки. Автоматизация бизнес-процессов с помощью ИИ помогает компаниям ускорять выполнение задач и сокращать влияние человеческого фактора [2].

Появление больших языковых моделей — Large language models (LLM) значительно укрепило возможность использования ИИ для принятия стратегических решений и ускорило этот процесс. LLM представляют собой алгоритмы прогнозирования текста, созданные на основе анализа обширных объемов текстовых данных. При обучении на достаточно крупных массивах данных сложные модели приобретают умение отвечать на вопросы, обобщать информацию и логически рассуждать.

Возможности LLM обусловливают их значимость для принятия стратегических решений с использованием ИИ по трем ключевым причинам. Во-первых, такие модели способны работать с текстовыми данными, которые часто представляют собой как входные, так и выходные данные в стратегических процессах. Во-вторых, LLM могут сравниться или даже превзойти человека в задачах, требующих аналитического мышления. В-третьих, данные, на которых обучаются LLM, включают ценную информацию, полезную для стратегического анализа: предпочтения потребителей, сведения о конкурентах и другие стратегически значимые знания [3].

Примеры практического использования искусственного интеллекта путем внедрения в информационные системы

Существуют специализированные системы для принятия решений. В качестве примера можно рассмотреть IBM Planning Analytics. Система способна анализировать большие объемы данных, выявлять тенденции и закономерности, а также предоставлять рекомендации и прогнозы [4, 5] (рис. 1).

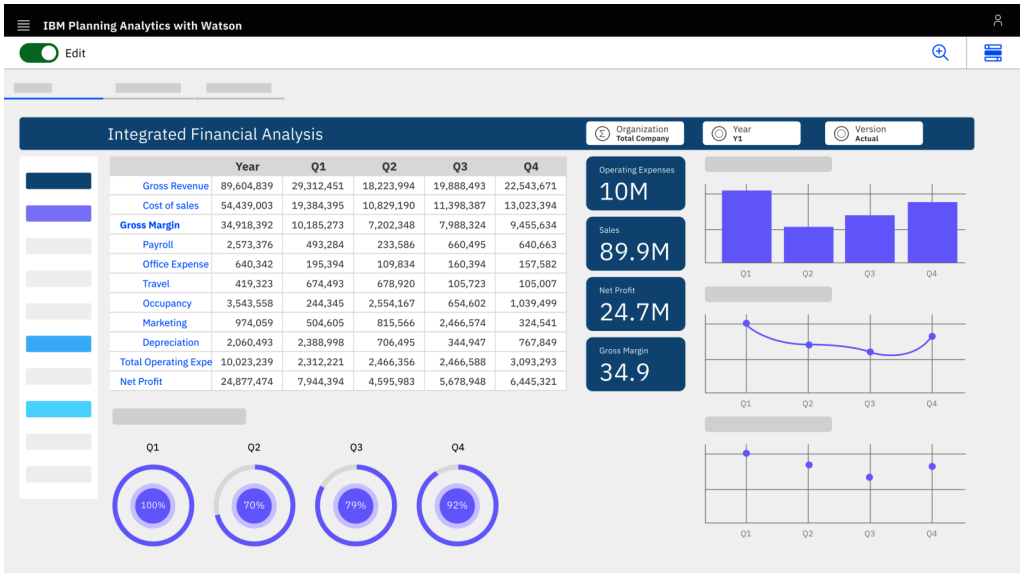

Рис. 1. Интерфейс системы IBM Planning Analytics

Известны реальные кейсы применения IBM Planning Analytics для бизнеса. Например, сегодня Vaasan использует встроенные алгоритмы планирования на основе ИИ в трех важнейших областях бизнеса: прогнозирование энергопотребления и ценообразования, анализ тенденций в центрах затрат и долгосрочное планирование продукции.

Использование аналитики планирования для прогнозирования энергопотребления помогает компании лучше планировать и согласовывать цены на энергоносители с производителями. Алгоритм учитывает внешние факторы, такие как ожидаемая температура на улице, а также производственные показатели [6].

Solar Coca-Cola поставила задачу IBM оптимизировать процессы, с помощью которых она проводила финансовое моделирование, столь важное для планирования и принятия решений в компании. Для руководства было важно сократить объемы ручной обработки массивов данных и получать быстрые решения по текущим вопросам. Сегодня компания использует модель «что, если», встроенную в IBM Planning Analytics, чтобы увидеть, как изменения во внешних факторах, влияющих на стоимость, таких как цены на сырьевые товары, налоги и обменные курсы, влияют не только на ценовую политику, но и на уровень спроса, запасы и производственные планы [7].

Искусственный интеллект в области информационной безопасности

Другой областью применения ИИ в управлении является информационная безопасность. В сфере кибербезопасности ИИ активно используется для обнаружения аномалий, предотвращения мошенничества и мгновенного реагирования на угрозы. Модели машинного обучения, анализирующие большие объемы данных, позволяют улучшить защиту организаций, однако важность прозрачности остается ключевым аспектом доверия и соблюдения норм безопасности. Раньше приблизительные ежемесячные прогнозы составлялись вручную и не приносили особой пользы компании.

В развитии технологий и информационных систем (ИС) все больше процессов в организациях нуждаются в автоматизации. Компании сталкиваются с необходимостью управления огромным количеством пользователей, приложений и ресурсов. В условиях сложных инфраструктур с множеством уровней доступа и разнообразных политик безопасности процесс предоставления и контроля доступа становится трудоемким и подверженным ошибкам.

В крупных организациях и производствах стабильность управленческого аппарата является необходимым условием для эффективного функционирования всех процессов. В условиях цифровизации управлять нужно не только людьми, но и информационными ресурсами, которые становятся наиболее ценным активом нашего времени. Защита данных, предотвращение их утечек и несанкционированного доступа (НСД) — одни из ключевых задач современной безопасности. Именно поэтому организации все чаще внедряют специализированные ИС для обеспечения информационной безопасности (ИБ).

Процесс управления доступом включает предоставление прав пользователям, ограничение их доступа к ресурсам, контроль и мониторинг за выполнением требований безопасности. Использование ручных методов управления становится все менее эффективным из-за увеличения вероятности ошибок, задержек и угроз безопасности. Классические подходы нередко тормозят работу бизнеса и не отвечают современным стандартам кибербезопасности. Среди таких методов можно выделить использование Active Directory (AD). Данная система каталогов предоставляет возможность управлять доступом к различным ресурсам — от офисных документов до критически важных систем и баз данных. Однако изменения в бизнес-процессах и требованиях законодательства выявляют недостатки традиционного подхода к управлению через AD:

1) трудоемкость настройки прав доступа для пользователей;

2) высокий риск ошибок при ручной обработке данных;

3) долгие процедуры согласования прав;

4) ограниченная масштабируемость при росте числа ресурсов и пользователей.

В сложившихся условиях автоматизация управления доступом становится не просто удобством, а необходимостью. Системы управления доступом (СУД) представляют собой многофункциональные программные комплексы, разработанные для надежного и упрощенного контроля прав пользователей на доступ к информационным ресурсам организации. Эти системы позволяют централизованно управлять учетными записями и распределением прав доступа, а также нередко интегрируются с кадровыми системами. Существуют различные виды СУД, например, Identity Management (IDM) и Identity and Access Management (IAM), они выполняют ряд важных функций: создание и администрирование учетных записей, предоставление и аннулирование прав доступа, соблюдение требований политики безопасности и предотвращение несанкционированного использования ресурсов [8].

ИИ трансформирует подход к управлению доступом, предоставляя возможность предотвращать НСД и другие нарушения за счет автоматизированного принятия решений. В совокупности с технологиями машинного обучения он представляет собой мощный инструмент для повышения уровня автоматизации и самостоятельности в принятии решений. Внедрение ИИ особенно актуально для новейших типов СУД, таких как Identity Governance and Administration (IGA), которые обрабатывают большие объемы данных и оценивают риски.

Машинное обучение играет важную роль в управлении доступом, создавая модели стандартного поведения пользователей и ресурсов. При обнаружении отклонений, таких как вход с непривычного устройства или в нестандартное время, система может оперативно реагировать, блокируя доступ или запрашивая дополнительную аутентификацию.

Кроме того, искусственный интеллект активно используется для оптимизации управления правами доступа и ролями. Анализируя текущие настройки, ИИ выявляет возможности для улучшений, предлагает оптимальные конфигурации и создает новые роли. Это позволяет минимизировать риски, связанные с избыточными привилегиями и конфликтами прав, что одновременно повышает безопасность и упрощает процесс администрирования.

Примеры внедрения искусственного интеллекта в системы управления доступом

Современные лидеры мирового рынка СУД активно интегрируют ИИ в свои продукты. Ярким примером такого подхода является микросервис Identity Role Intelligence от компании Oracle, представляющий решения класса IGA. Этот инструмент применяет ИИ для анализа данных и совершенствования управления правами доступа. Благодаря машинному обучению система автоматически формирует роли, которые соответствуют текущим потребностям бизнеса. Пользователи, ответственные за создание новых ролей, могут принимать решения на основе рекомендаций и аналитики от Role Intelligence, которая также сравнивает новые роли с существующими, исключая дублирование [9].

Компания Okta также разработала обширный набор функций на основе ИИ, объединенных под брендом Okta AI. Этот инструмент используется для предотвращения кибератак в таких продуктах, как Workforce Identity Cloud и Customer Identity Cloud. Okta AI включает технологии машинного обучения, которые позволяют анализировать пользовательское поведение, выявлять аномалии и автоматизировать управление доступом. В режиме реального времени система оценивает риски при входе, обнаруживает потенциальные угрозы и помогает улучшить соответствие требованиям безопасности. Кроме того, Okta AI предоставляет рекомендации по оптимизации управления учетными записями и ролями, что упрощает администрирование и повышает безопасность [10].

Российские разработчики системы управления доступом Solar inRights также наметили курс на активное внедрение ИИ в свои технологии. Планируется, что искусственный интеллект и машинное обучение будут анализировать поведение пользователей, выявлять аномалии и предотвращать конфликты обязанностей. На основании накопленных данных система сможет оптимизировать процесс

назначения ролей и прав, обрабатывать неструктурированные запросы, снижать нагрузку на администраторов и усиливать защиту системы управления доступом [11].

Таким образом, можно заключить, что внедрение ИИ в СУД открывает возможности для автоматизации, повышения безопасности и оптимизации процессов. ИИ упрощает управление правами доступа, анализирует поведение пользователей и помогает выявлять отклонения, предотвращая потенциальные угрозы. Это обеспечивает динамическую настройку доступа в зависимости от контекста и улучшает соответствие требованиям безопасности. Кроме того, использование ИИ снижает нагрузку на администраторов, ускоряет выполнение задач и повышает эффективность работы всей системы.

Риски использования искусственного интеллекта в контексте управления и контроля доступа

Внедрение ИИ в СУД, несмотря на свои преимущества, связано с рядом рисков. Один из основных — возможность ошибок в принятии решений, так как ИИ сильно зависит от качества и точности входящих данных. Неправильная информация может привести к ошибочному предоставлению прав доступа или блокировке пользователей, что нарушит рабочие процессы.

Еще одной проблемой является отсутствие прозрачности в работе алгоритмов. Многие ИИ-системы функционируют как «черные ящики», и в случае ошибок или споров трудно понять, на каких данных и принципах было основано решение. Также, если алгоритмы неправильно обучены или недостаточно адаптированы, они могут не справиться с новыми или нестандартными ситуациями, что приведет к их неправильной интерпретации и принятию неверных решений.

Помимо прочего, использование ИИ в СУД может повысить их уязвимость к кибератакам. Злоумышленники могут манипулировать данными, поступающими в систему, что может привести к ошибочным решениям и возникновению ситуаций с НСД.

Не менее важным риском является соблюдение нормативных и юридических требований. ИИ-системы могут столкнуться с проблемами, связанными с конфиденциальностью данных и правами пользователей, что создает дополнительные сложности в правовом поле. Кроме того, полная автоматизация с использованием ИИ делает организацию зависимой от технологий, и в случае сбоя системы или неадекватной работы алгоритмов могут возникнуть проблемы с доступом, что повлияет на бизнес-процессы. И наконец, ИИ может усиливать предвзятость, если алгоритмы обучаются на ошибочных или предвзятых данных, что приведет к несправедливому распределению прав доступа [12].

Контроль за использованием искусственного интеллекта на международном уровне

Сейчас многие страны находятся в активной фазе формирования правил и норм использования ИИ. Оценить, насколько эти страны эффективно используют и регулируют ИИ с точки зрения этики, защиты прав человека и других социальных факторов можно при помощи глобального индекса ответственного искусственного интеллекта — The Global Index on Responsible AI (GIRAI). Это комплексное исследование, которое оценивает, насколько страны по всему миру внедряют принципы ответственного использования ИИ.

В цели GIRAI входит установка единых глобальных стандартов для ответственного ИИ, повышение осведомленности о влиянии ИИ и измерение прогресса стран.

В первом издании 2024 года индекс охватывает 138 стран, в том числе 41 страну Африки. Оценка проводится по трем направлениям: права человека и ИИ, управление ответственным ИИ и возможности для внедрения ответственного ИИ. Эти направления оцениваются по трем аспектам: государственные документы, инициативы правительства и действия негосударственных организаций.

Данные собирались региональными исследовательскими центрами в период с 2021 по 2023 год. Для оценки использовались как первичные, так и вторичные источники данных, включая

правительственные документы, законы, отчеты и программы. Эксперты оценивали актуальные инициативы, рассматривали механизмы защиты прав человека в контексте ИИ, присутствие стратегий по управлению рисками и наличие механизмов возмещения ущерба при использовании ИИ [13].

В табл. 1 приведен список из десяти стран с самым высоким значением индекса.

Таблица 1

Ведущие страны по GIRAI

Рейтинг	Страна	Индекс
1	Нидерланды	86,16
2	Германия	82,77
3	Ирландия	74,98
4	Великобритания	73,12
5	Соединенные Штаты Америки	72,81
6	Эстония	67,61
7	Италия	61,8
8	Франция	57,62
9	Канада	57,39
10	Австралия	56,22

По данным на июнь 2024 года, первое место в международном рейтинге по ответственному ИИ занимают Нидерланды. В связи с геополитической ситуацией в мире России нет в данном списке. Однако в нашей стране формируются подобные исследования для улучшения нормативной базы по использованию ИИ [14].

Заключение

В итоге отметим, что ИИ открывает новые возможности для решения задач по управлению доступом. Его применение позволяет ускорить процессы, снизить количество ошибок и обеспечить более гибкое управление правами пользователей. Однако, несмотря на очевидные преимущества, внедрение ИИ в СУД не лишено рисков: ошибки алгоритмов, сложности настройки и уязвимости самих систем могут стать причиной новых угроз. Чтобы реализовать все преимущества и минимизировать риски, организациям необходимо тщательно планировать внедрение ИИ в процессы управления доступом, обеспечивая адекватный контроль и прозрачность работы этих систем.

Сейчас крупные компании активно развиваются в данном направлении и в будущем использование ИИ в СУД станет неотъемлемой частью защиты данных, что делает необходимым дальнейшее изучение этой темы и разработку механизмов по устранению рисков.

В заключение можно также отметить, что ИИ продолжает изменять управление в различных отраслях, улучшая производительность и сокращая издержки. Однако его внедрение сопровождается вызовами, которые требуют продуманного подхода и ответственности. Перспективы развития ИИ в управлении остаются колоссальными, и успех будущих инициатив будет зависеть от осознания вызовов и активного поиска решений, ориентированных на долгосрочные выгоды.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Носова В. И. Искусственный интеллект в образовании // Молодой ученый. 2023. № 49 (496). С. 190–192.

2. AI-Driven Decision Support Systems in Management: Enhancing Strategic Planning and Execution / S. Dodda [et al.] // International Journal on Recent and Innovation Trends in Computing and Communication. 2024. Vol. 12 (1). P. 1.

3. Csaszar F. A., Ketkar H., Kim H. Artificial Intelligence and Strategic Decision-Making: Evidence from Entrepreneurs and Investors. 2024.

4. IBM Planning Analytics. URL: https://www.ibm.com/products/planning-analytics?lnk=STW_UK_PHP_SP4_BLK&psrc=NONE&pexp=DEF&lnk2=trial_PlanningAnalytics

5. IBM Planning Analytics 2.0 URL: //https://www.ibm.com/docs/en/planning-analytics/2.0.0

6. Baking in AI and Analytics to Meet Rising Demand. URL: https://www.ibm.com/case-studies/vaasan

7. A “Revolution” in Financial Reporting Brings Faster and Deeper Insights. URL: https://www.ibm.com/case-studies/solar-coca-cola

8. Блюм В. С., Григорьева Д. А. Система управления доступом как современный способ обеспечения информационной безопасности в организации // Актуальные проблемы экономики и управления. 2024. № 2 (42). С. 27–33.

9. Administering Oracle Identity Role Intelligence. URL: https://docs.oracle.com/en/middleware/idm/identity-role-intelligence/amiri/overview-oracle-identity-role-intelligence.html#GUID-3D761974-3533-4051-B939-1B45E4ACC3CD

10. Introducing Okta AI. URL: https://www.okta.com/products/okta-ai/

11. Севастьянова Л. Управление доступом: развитие технологий, процессов, машинного обучения // Solar: 2024. URL: https://rt-solar.ru/events/blog/4080/

12. AI Hype as a Cyber Security Risk: the Moral Responsibility of Implementing Generative AI in Business / D. Humphreys [et al.] // AI Ethics. 2024. No. 4. P. 791–804.

13. Comprehensive, Comparable, Country-Level Data. URL: https://www.global-index.ai/Countries

14. Росстат проводит мониторинг создания и результатов применения технологий искусственного интеллекта // Союз «Одинцовская ТПП»: официальный сайт. URL: https://odintsovo.tpprf.ru/ru/mobile/news/538587/

Дата поступления: 24.11.2024
Решение о публикации: 24.11.2024

Access Control Using Artificial Intelligence: Opportunities and Risks

Vladislav S. Blyum — PhD in Engineering, Associate Professor of Business Informatics and Management Department. Research interests: immunocomputing, artificial intelligence technologies. E-mail: vladblum7@gmail.com

Darya A. Grigoryeva — Student of Business Informatics and Management Department. Research interests: information technology. E-mail: daria_grig4221@mail.ru

Saint Petersburg State University of Aerospace Instrumentation, 67, Bolshaya Morskaya str., 190000, St. Petersburg, Russia

For citation: Blyum V. S., Grigoryeva D. A. Access Control Using Artificial Intelligence: Opportunities and Risks // Intellectual Technologies on Transport. 2024. № 4 (40). Pp. 5–12. DOI: 10.20295/2413-2527-2024-440-5-12. (In Russian)

Abstract. *In modern conditions, companies need to introduce new technologies in a timely manner and monitor compliance with information security requirements in order to effectively counter modern threats. Access control systems are one of the main tools that ensure an adequate level of information security at the enterprise and simplify control over the provision of access to the organization's resources.* ***The main goal:*** *to explore the possibilities of using artificial intelligence for access control systems, highlighting its importance in the context of increasing the level of information security of the organization and the effectiveness of access rights management.* ***Research method:*** *analysis of modern tools and technologies, including artificial intelligence and large language models, as well as assessment of practical cases of AI implementation in access control systems. Both the advantages and risks associated with automated access control using AI are considered.* ***Practical significance:*** *the results of the work can be used by organizations to improve the security and efficiency of access management to information resources. The identified risks and recommendations for the introduction of AI technologies will allow companies to take a more conscious approach to improving information security processes.*

Keywords: *access control system, information security, information protection, identification, authentication, access rights control, automation, role model, IDM, IAM, IGA*

REFERENCES

1. Nosova V. I. Iskusstvennyj intellekt v obrazovanii // Molodoj uchenyj. 2023. № 49(496). S. 190–192. (In Russian)
2. AI-Driven Decision Support Systems in Management: Enhancing Strategic Planning and Execution / S. Dodda [et al.] // International Journal on Recent and Innovation Trends in Computing and Communication. 2024. Vol. 12(1). P. 1.
3. Csaszar F. A., Ketkar H., Kim H. Artificial Intelligence and Strategic Decision-Making: Evidence from Entrepreneurs and Investors. 2024.
4. IBM Planning Analytics. URL: https://www.ibm.com/products/planning-analytics?lnk=STW_UK_PHP_SP4_BLK&psrc=NONE&pexp=DEF&lnk2=trial_PlanningAnalytics
5. IBM Planning Analytics 2.0 URL: //https://www.ibm.com/docs/en/planning-analytics/2.0.0
6. Baking in AI and Analytics to Meet Rising Demand. URL: https://www.ibm.com/case-studies/vaasan
7. A “Revolution” in Financial Reporting Brings Faster and Deeper Insights. URL: https://www.ibm.com/case-studies/solar-coca-cola
8. Blyum V. S., Grigor’eva D. A. Sistema upravleniya dostupom kak sovremennyj sposob obespecheniya informacionnoj bezopasnosti v organizacii // Aktual’nye problemy ekonomiki i upravleniya. 2024. No. 2(42). S. 27–33. (In Russian)
9. Administering Oracle Identity Role Intelligence. URL: https://docs.oracle.com/en/middleware/idm/identity-role-intelligence/amiri/overview-oracle-identity-role-intelligence.html#GUID-3D761974-3533-4051-B939-1B45E4ACC3CD
10. Introducing Okta AI. URL: https://www.okta.com/products/okta-ai/
11. Sevast’yanova L. Upravlenie dostupom: razvitie tekhnologij, processov, mashinnogo obucheniya // Solar: 2024. URL: https://rt-solar.ru/events/blog/4080/ (In Russian)
12. AI Hype as a Cyber Security Risk: the Moral Responsibility of Implementing Generative AI in Business / D. Humphreys [et al.] // AI Ethics. 2024. № 4. S. 791–804.
13. Comprehensive, Comparable, Country-Level Data. URL: https://www.global-index.ai/Countries
14. Rosstat provodit monitoring sozdaniya i rezul’tatov primeneniya tekhnologij iskusstvennogo intellekta // Soyuz “Odincovskaya TPP”: oficial’nyj sajt. URL: https://odintsovo.tpprf.ru/ru/mobile/news/538587/ (In Russian)

Received: 24.11.2024
Accepted: 24.11.2024