УДК 330.34:004.61

5.2.2. Математические, статистические и инструментальные методы экономики (физико-математические науки, экономические науки)

**ЗАЩИТА ЭКОНОМИЧЕСКИХ ДАННЫХ: КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ СОВРЕМЕННЫХ УГРОЗ**

Савинская Дина Николаевна
к.э.н., доцент кафедры информационных систем
Savi_dinki@mail.ru
*Кубанский государственный аграрный университет им. И. Т. Трубилина, г. Краснодар, Россия*

Абян Виолетта Матевосовна
обучающаяся экономического факультета
Abyan1984@mail.ru
*Кубанский государственный аграрный университет им. И. Т. Трубилина, г. Краснодар, Россия*

Зурнаджиди Серафима
обучающаяся экономического факультета
zurnadzidis@gmail.com
*Кубанский государственный аграрный университет им. И. Т. Трубилина, г. Краснодар, Россия*

Логинова Виктория Олеговна
обучающаяся экономического факультета
vikaloginova2504@gmail.com
*Кубанский государственный аграрный университет им. И. Т. Трубилина, г. Краснодар, Россия*

Кибербезопасность и защита экономических данных приобретают все большее значение в свете современных рисков, связанных с цифровизацией экономики. В результате утечки информации или компрометации могут возникнуть угрозы национальной безопасности, значительные финансовые потери и репутационные риски. Особое внимание уделяется основным категориям киберугроз, включая вредоносное ПО, хакерские атаки и промышленный шпионаж, а также стратегиям предотвращения. Растущее значение защиты данных и инфраструктуры подтверждается анализом динамики расходов России на киберзащиту и технологические достижения в период с 2019 по 2023 гг. Для предотвращения угроз кибербезопасности банковского сектора предлагается алгоритм, который определяет критические регионы и методы обеспечения безопасности. Было подчеркнуто, что необходим комплексный подход к защите данных, включающий использование передовых технологий, создание нормативно-правовой базы и

UDC 330.34:004.61

5.2.2. Mathematical, statistical and instrumental methods of economics (physical and mathematical sciences, economic sciences)

**PROTECTION OF ECONOMIC DATA: CYBERSECURITY IN THE FACE OF MODERN THREATS**

Savinskaya Dina Nikolaevna
Candidate of Economics, Associate Professor of the Department of Information Systems
Savi_dinki@mail.ru
*Kuban State Agrarian University, Krasnodar, Russia*

Abyan Violetta Matevosovna
student at the Faculty of Economics
Abyan1984@mail.ru
*Kuban State Agrarian University, Krasnodar, Russia*

Zurnajidi Serafima
student at the Faculty of Economics
zurnadzidis@gmail.com
*Kuban State Agrarian University, Krasnodar, Russia*

Loginova Victoria Olegovna
student at the Faculty of Economics
vikaloginova2504@gmail.com
*Kuban State Agrarian University, Krasnodar, Russia*

Cybersecurity and economic data protection are becoming increasingly important in the light of modern risks associated with the digitalization of the economy. Information leakage or compromise may result in threats to national security, significant financial losses, and reputational risks. Special attention is paid to the main categories of cyber threats, including malware, hacker attacks and industrial espionage, as well as prevention strategies. The growing importance of data and infrastructure protection is confirmed by an analysis of the dynamics of Russian spending on cyber defense and technological advances in the period from 2019 to 2023. To prevent threats to the cybersecurity of the banking sector, an algorithm is proposed that identifies critical regions and methods of ensuring security. It was emphasized that a comprehensive approach to data protection is needed, including the use of advanced technologies, the creation of a regulatory framework and the strengthening of international cooperation in the field of cybersecurity. This is an important step in ensuring the sustainability of the country's financial

укрепление международного сотрудничества в области кибербезопасности. Это важный шаг в обеспечении устойчивости финансовой системы страны и жизненно важных данных

system and vital data

Ключевые слова: ЗАЩИТА ЭКОНОМИЧЕСКИХ ДАННЫХ, КИБЕРБЕЗОПАСНОСТЬ, ЦИФРОВИЗАЦИЯ, КИБЕРУГРОЗЫ, ВРЕДОНОСНЫЕ ПРОГРАММЫ, ФИНАНСОВЫЙ СЕКТОР, ЗАЩИТА ИНФРАСТРУКТУРЫ

Keywords: ECONOMIC DATA PROTECTION, CYBERSECURITY, DIGITALIZATION, CYBER THREATS, MALWARE, FINANCIAL SECTOR, INFRASTRUCTURE PROTECTION

http://dx.doi.org/10.21515/1990-4665-208-013

Защита экономических данных становится важнейшей задачей для государственных учреждений, предприятий и финансовых организаций, поскольку утечка или компрометация информации могут привести к значительным экономическим потерям, репутационным рискам и угрозам национальной безопасности. Современные киберугрозы, такие как: хакерские атаки, промышленный шпионаж и вредоносное программное обеспечение, требуют комплексных подходов к защите данных и постоянного совершенствования методов обеспечения кибербезопасности. Эти проблемы особенно актуальны в контексте цифровизации экономики и глобального распространения информационных технологий.

Помимо внедрения технологических решений, эффективная защита экономической информации также требует разработки нормативных актов, формирования культуры информационной безопасности и укрепления международного сотрудничества. Важно отметить, что киберугрозы постоянно меняются, что требует активного использования инновационных технологий и адаптивных стратегий для предотвращения атак.

Систематизация потенциальных опасностей, связанных с утечкой, искажением или недоступностью информации, становится возможной благодаря классификации угроз информационной безопасности. Для разработки эффективных мер защиты многообразие опасностей требует анализа и классификации на основе ряда факторов. Разработка

эффективных средств защиты и более точное прогнозирование возможных нападений становятся возможными благодаря методичному подходу к анализу угроз.

Угрозы информационной безопасности классифицированы на рисунке 1, который отражает множество способов структурирования возможных угроз [2]. Учитываются такие важные факторы, как происхождение угроз, их тип, их воздействие и потенциальный ущерб. Безопасность и надежность информационных систем определяются угрозами конфиденциальности, доступности и целостности информации.


Рисунок 1 – Классификация угроз информационной безопасности

Одним из важнейших факторов повышения эффективности организации является использование цифровых платформ в различных секторах экономики. Тенденции внедрения цифровых технологий в российскую экономику в 2021-2023 гг. представлены на рисунке 2. Очевидно, что цифровизация проникла практически во все сферы жизни,

хотя степень этого распространения сильно варьируется в зависимости от особенностей каждого вида деятельности [3].

Наибольший процент предприятий, внедряющих цифровые платформы, приходился на финансовый сектор (35,1% в 2023 г.), высшее образование (40%) и оптовую и розничную торговлю (31,9%). Причинами этого являются необходимость обработки огромных объемов данных, высокий уровень автоматизации процессов и постоянный рост онлайн-сервисов.

В то же время такие секторы, как государственное управление (9,4%), операции с недвижимостью (8,6%), культура и спорт (7,5% в 2023 г.), имеют низкую степень цифровизации. Способствующими факторами являются уникальные характеристики определенных секторов, меньшая зависимость от цифровых технологий и отсутствие инноваций.

Особое внимание следует уделить динамике расширения цифровизации в конкретных отраслях. Например, в горнодобывающей промышленности (с 11,8% до 14,3%) и сельском хозяйстве (с 10,4% в 2021 г. до 14% в 2023 г.) наблюдалось заметное увеличение доли предприятий, использующих цифровые платформы. Это говорит о том, что даже в исторически консервативных отраслях цифровые решения внедряются постепенно.

Доля предприятий, использующих цифровые платформы, снижается в таких секторах, как технологии и коммуникации (с 21,2% до 18,3%) и энергоснабжение (с 13,7% в 2021 г. до 10,6% в 2023 г.). Это является результатом изменения стратегических приоритетов бизнеса или завершения активной фазы цифровой трансформации.

Таким образом, цифровизация продолжает проникать во все сферы экономики, но скорость и глубина внедрения цифровых платформ сильно различаются [5]. В одних отраслях процесс идет более активно, в то время

как в других требуется дальнейшая поддержка и стимулирование цифровой трансформации.


Рисунок 2 – Доля организаций, использующих цифровые платформы, по видам экономической деятельности (2021–2023 гг.), в % от общего числа организаций [4;6]

Одним из самых больших рисков для цифровой безопасности являются кибератаки, которые могут оказать серьезное влияние на предприятия, государственные учреждения и отдельных пользователей [3]. Поскольку злоумышленники используют широкий спектр стратегий, от использования уязвимостей веб-приложений до атак вредоносных программ и программ-вымогателей, разнообразие методов атаки усложняет защиту информационной системы.

Основные категории кибератак, их доля в общем объеме атак и краткое описание механизмов воздействия представлены в таблице 1.

Об уязвимости веб-сайтов и онлайн-сервисов свидетельствует тот факт, что атаки на веб-приложения (26%) составляют наибольшую долю кибератак, что подчеркивает важность регулярной проверки и обновления систем безопасности. Банковским и корпоративным системам серьезно угрожают вредоносные программы (18%) и атаки с помощью приложений (17%), которые часто распространяются с помощью фишинга и программных сбоев.

Компании и государственные организации подвергаются опасности DoS/DDoS-атак (11%), поскольку они препятствуют доступности цифровых сервисов. Программы-вымогатели (9%) и атаки на цепочки поставок (9%) повышают вероятность широкого распространения инфекции и финансовых потерь. Растущая сложность киберугроз требует комплексной защиты, включая обучение персонала, обновление программного обеспечения и применение современных технологий безопасности [1].

Таблица 1 – Основные типы кибератак и их характеристика

| Тип атаки | Доля в общем объеме атак, % | Описание |
|---|---|---|
| Атаки на веб-приложения | 26 | Используют уязвимости веб-сайтов (SQLi, XSS) для несанкционированного доступа к данным или изменения их содержимого. |
| Вредоносное ПО (вирусы, трояны, шпионские программы) | 18 | Распространяется через фишинг, зараженные сайты и ПО, выполняя шпионаж, кражу данных или вывод системы из строя. |
| Атаки на определенные приложения | 17 | Эксплуатируют уязвимости специализированных программ (банковские, корпоративные), позволяя получить доступ к данным. |
| DoS/DDoS-атаки (атаки на отказ в обслуживании) | 11 | Перегружают серверы большим количеством запросов, вызывая сбои или полную недоступность веб-ресурсов. |
| Разведывательные атаки | 10 | Ориентированы на сбор информации о системе, выявление уязвимостей и подготовку дальнейших атак. |
| Атаки программ-вымогателей (Ransomware) | 9 | Шифруют данные жертвы, требуя выкуп за их восстановление, нанося ущерб бизнесу и государственным структурам. |
| Атаки на цепочки поставок (Supply Chain Attacks) | 9 | Внедряют вредоносный код в программное обеспечение или сервисы поставщиков для последующего заражения пользователей. |

Хотя цифровые платформы предоставляют организациям множество возможностей для роста, они также несут в себе ряд угроз, которые ставят под угрозу их финансовую и информационную безопасность [4]. На рисунке 3 представлены риски, связанные с использованием цифровых платформ: информационными и экономическими угрозами для организаций.

Вредоносные программы и кибератаки являются наиболее опасными (65%), что подчеркивает необходимость улучшения защиты данных. Об опасностях хранения данных в цифровых экосистемах свидетельствует уровень утечки частных и конфиденциальных данных, который составляет 61%. Технические неисправности (52%) по-прежнему представляют серьезную угрозу для жизнеспособности бизнеса.

Сбор данных платформами (46%) и потеря деловой информации (39%) свидетельствуют о том, что корпоративная тайна находится под угрозой. Экономические риски, влияющие на конкурентоспособность, отражаются в повышении тарифов на 22% и уходе 19% международных платформ. Организации должны принимать меры кибербезопасности и разумно выбирать платформы, чтобы снизить риски [6].


Рисунок 3 – Анализ рисков, связанных с использованием цифровых платформ: информационные и экономические угрозы для организаций за 2023 г. [4]

Проблемы кибербезопасности имеют важное значение в контексте цифровизации финансовой индустрии. Рост числа атак на банки и другие финансовые учреждения свидетельствует о растущих рисках мошенничества, утечки данных и повреждения критически важной инфраструктуры. Анализ динамики кибератак, их происхождения, финансовых последствий и эффективности внедренных средств защиты важен для определения масштабов этой проблемы [5]. Основные показатели, характеризующие степень киберрисков для институтов национальной финансовой системы России на 2021-2023 гг., представлены в таблице 2.

За три года в целом было совершено еще 260 кибератак, а в 2023 г. – 1587 атак. Основной причиной всплеска стали атаки на СКФО (+74,3) и системообразующие банки (+8,9), что подчеркивает их уязвимость.

Кроме того, сумма материального ущерба резко возросла и составила 29,25 млрд руб., из которых более 13,6 млрд руб. пришлось на клиентов. О сложности механизмов противодействия свидетельствует одновременное увеличение затрат на восстановление банковской инфраструктуры на 6,2 млрд руб.

Атаки все чаще совершаются из стран дальнего зарубежья (41,4%), что требует расширения международного сотрудничества в области кибербезопасности. Несмотря на то, что процент зеркальных атак увеличился (64,9%), клиенты банков получают меньшую компенсацию за свои убытки (7,2%), что негативно сказывается на доверии пользователей к финансовой системе [1].

В результате кибератаки становятся все более изощренными и дорогостоящими для финансовых учреждений, что требует активного внедрения современных решений в области безопасности, а также усиления мониторинга и координации деятельности на государственном уровне.

Таблица 2 – Динамика кибератак на институты национальной финансовой системы Российской Федерации в 2021–2023 гг.

| Показатель | 2021 г. | 2022 г. | 2023 г. | Абсолютное отклонение (+,-) |
|---|---|---|---|---|
| 1. Совокупное количество совершенных кибератак на институты национальной финансовой системы, ед.<br>В том числе: | 1327 | 1489 | 1587 | 260 |
| Центральный банк | 5,7 | 6,3 | 7,4 | 1,7 |
| системообразующие банки | 20,4 | 24,8 | 29,3 | 8,9 |
| остальные банки | 985,6 | 1137,9 | 1215,4 | 229,8 |
| небанковские кредитно-финансовые организации (НКФО) | 210,9 | 250,5 | 285,2 | 74,3 |
| 2. География источников кибератак, в % к общему количеству: | 100,0 | 100,0 | 100,0 | - |
| Резиденты РФ | 47,4 | 45,8 | 44,7 | -2,7 |
| Страны СНГ | 15,6 | 14,3 | 13,9 | -1,7 |
| Дальнее зарубежье | 37,0 | 39,9 | 41,4 | 4,4 |
| 3. Совокупный объем нанесенного материального ущерба, млн руб.<br>В том числе: | 19765,3 | 24788,2 | 29254,6 | 9489,3 |
| убытки, причиненные клиентам банков и НКФО | 8987,6 | 11482,3 | 13614,9 | 4627,3 |
| расходы на восстановление дееспособности банковской инфраструктуры | 9412,4 | 13123,1 | 15639,7 | 6227,3 |
| 4. Показатели защищенности институтов национальной финансовой системы | | | | |
| Удельный вес отраженных кибератак, % | 58,2 | 62,4 | 64,9 | 6,7 |
| Уровень возмещения банками убытков от кибератак, % | 9,8 | 8,5 | 7,2 | -2,6 |
| Индекс устойчивости институтов национальной финансовой системы по категориям финансовых институтов: | | | | |
| Центральный банк | 5,2 | 6,1 | 7,0 | 1,8 |
| системообразующие банки | 9,3 | 10,1 | 11,2 | 1,9 |
| остальные банки | 4,2 | 4,7 | 5,1 | 0,9 |
| небанковские кредитно-финансовые организации (НКФО) | 4,6 | 5,1 | 5,6 | 1,0 |

Учитывая, что угрозы с каждым годом становятся все более многочисленными и изощренными, важность киберзащиты и интернет-разведки трудно переоценить. В результате правительственных и корпоративных инициатив затраты на создание технологий для защиты инфраструктуры и данных резко возрастают (рис. 4).

Расходы на инфраструктуру, научно-исследовательские инициативы и киберзащиту демонстрируют устойчивый рост с 2019 по 2023 гг. Например, расходы на интернет-аналитику и кибербезопасность выросли

на 52,6% с 18,7 млрд руб. в 2019 г. до 28,5 млрд руб. в 2023 г. расходы, связанные со строительством центров обработки данных и для государства. Существенно увеличиваются и закупки программного обеспечения и компьютерного оборудования для объектов критически важной инфраструктуры.

Потребность в улучшенной защите необходимой инфраструктуры также отражается на стоимости развития центров обработки данных, которая выросла с 11,5 млрд руб. в 2019 г. до 16,2 млрд руб. в 2023 г. В совокупности эти расходы свидетельствуют о росте расходов на кибербезопасность, что свидетельствует о приверженности правительства укреплению устойчивости финансовой системы России [5].

Рост расходов на защиту экономических данных и инфраструктуры является необходимым шагом в условиях современных угроз, что отражает стремление обеспечить безопасность национальной финансовой системы и критически важной информации, гарантируя надежность функционирования экономики страны в условиях нарастающих киберугроз [2].

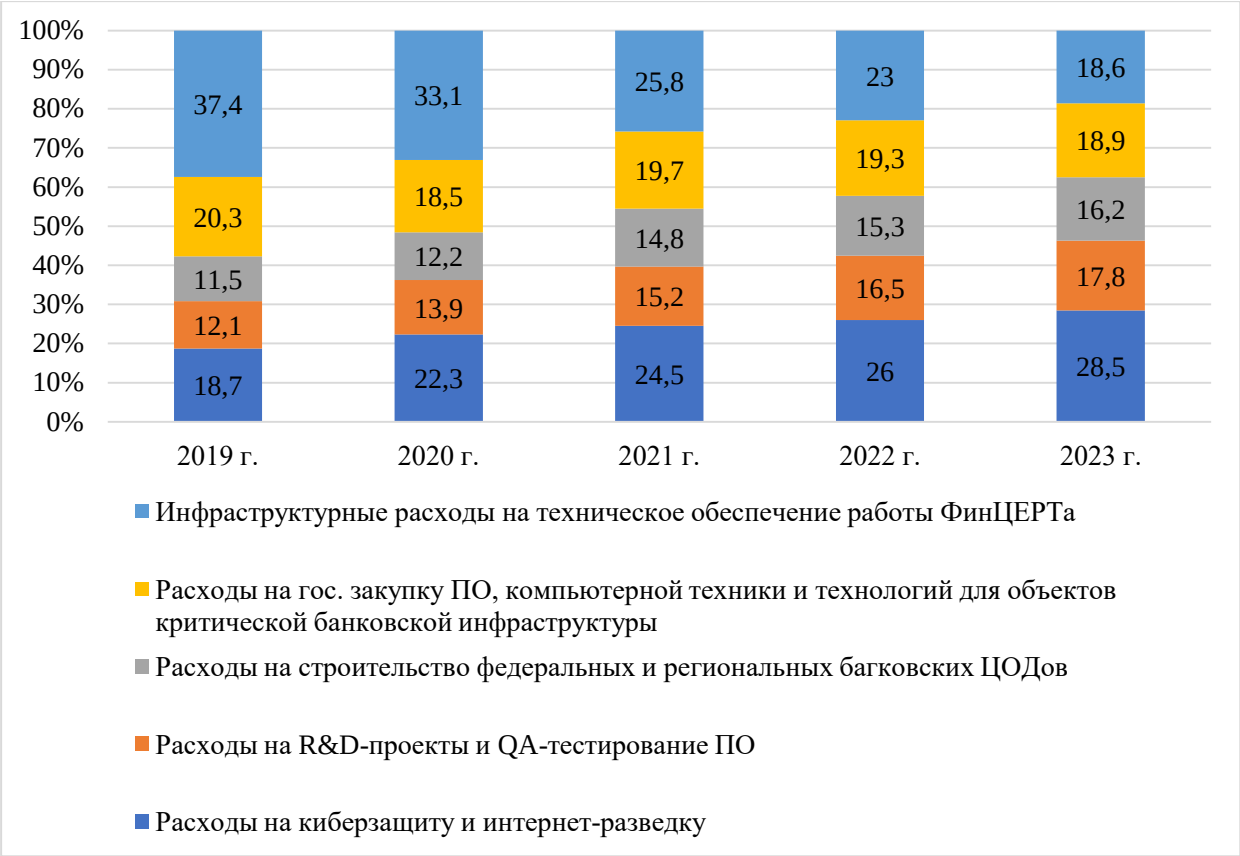


Рисунок 4 – Динамика распределения расходов на киберзащиту, инфраструктуру и технологические разработки в национальной финансовой системе РФ (2019–2023 гг.), % [6]

Эффективное предотвращение атак и защита данных становятся приоритетными задачами в связи с растущими киберрисками в банковском секторе. Передовые алгоритмы защиты и постоянное совершенствование мер кибербезопасности необходимы в связи с современными рисками, включая кибератаки, утечки данных и другие инциденты. Алгоритм предотвращения угроз кибербезопасности финансового сектора представлен на рисунке 5. Он включает в себя важные области и меры предосторожности, которые гарантируют скоординированный подход к защите информации и инфраструктуры [2].


Рисунок 5 – Алгоритм предотвращения угроз кибербезопасности финансового сектора: ключевые направления и мероприятия [сост. авторами]

Таким образом, защита экономических данных и кибербезопасность становятся приоритетными задачами для предприятий, финансовых институтов и государственных учреждений в контексте глобализации информационных технологий и цифровизации экономики. Современные киберугрозы угрожают как национальной безопасности, так и экономической стабильности. Поскольку эти угрозы становятся все более многочисленными и сложными, важно постоянно совершенствовать средства защиты, создавать передовые технологические решения и применять комплексные стратегии кибербезопасности.

Растущие расходы на киберзащиту и инфраструктуру, наряду с увеличением инвестиций в научно-исследовательские проекты и развитие

центров обработки данных, свидетельствуют о стремлении правительства и бизнеса обеспечить надежную защиту критически важной инфраструктуры и данных. Эти факторы, наряду с анализом динамики кибератак, статистикой их последствий и значительными финансовыми потерями в результате атак, подтверждают высокую актуальность данного вопроса.

Защита экономических данных и кибербезопасность становятся важнейшими составляющими устойчивости национальной финансовой системы. Внедрение сложных алгоритмов и активное использование новейших технологий позволяют эффективно противостоять растущим угрозам, обеспечивая безопасность и стабильность экономики в условиях глобальных изменений.

**Список литературы:**

1. Бабалакова, С. Цифровая экономика и кибербезопасность: современные угрозы и защита данных / С. Бабалакова, Ш. Бегалиев // Матрица научного познания. – 2023. – № 9-1. – С. 223-225.

2. Ноздрин, С. А. Киберпреступность как угроза экономической безопасности Российской Федерации / С. А. Ноздрин // Вестник Академии права и управления. – 2023. – № 2(72). – С. 80-84.

3. Носова, С. С. ИИ как мультипликатор роста кибербезопасности бизнеса / С. С. Носова, А. Н. Норкина, Н. В. Морозов // Экономика и предпринимательство. – 2023. – № 6(155). – С. 723-728.

4. Росстат. — Режим доступа: https://23.rosstat.gov.ru/storage/mediabank/IKT(1).htm (дата обращения: 21.02.2025).

5. Синица, С. А. Киберугрозы цифровой экономики России / С. А. Синица // Экономика и бизнес: теория и практика. – 2023. – № 11-3(105). – С. 65-70.

6. Федеральная служба государственной статистики России. Использование информационно-коммуникационных технологий в России: 2021–2023 гг. / Росстат. — Режим доступа: https://rosstat.gov.ru/folder/154849?print=1 (дата обращения: 21.02.2025).

**References**

1. Babalakova, S. Cifrovaya e`konomika i kiberbezopasnost`: sovremenny`e ugrozy` i zashhita danny`x / S. Babalakova, Sh. Begaliev // Matricza nauchnogo poznaniya. – 2023. – № 9-1. – S. 223-225.

2. Nozdrin, S. A. Kiberprestupnost` kak ugroza e`konomicheskoj bezopasnosti Rossijskoj Federacii / S. A. Nozdrin // Vestnik Akademii prava i upravleniya. – 2023. – № 2(72). – S. 80-84.

3. Nosova, S. S. II kak mul`tiplikator rosta kiberbezopasnosti biznesa / S. S. Nosova, A. N. Norkina, N. V. Morozov // E`konomika i predprinimatel`stvo. – 2023. – № 6(155). – S. 723-728.

4. Rosstat. — Rezhim dostupa: https://23.rosstat.gov.ru/storage/mediabank/IKT(1).htm (data obrashheniya: 21.02.2025).

5. Sinicza, S. A. Kiberugrozy` cifrovoj e`konomiki Rossii / S. A. Sinicza // E`konomika i biznes: teoriya i praktika. – 2023. – № 11-3(105). – S. 65-70.

6. Federal`naya sluzhba gosudarstvennoj statistiki Rossii. Ispol`zovanie informacionno-kommunikacionny`x texnologij v Rossii: 2021–2023 gg. / Rosstat. — Rezhim dostupa: https://rosstat.gov.ru/folder/154849?print=1 (data obrashheniya: 21.02.2025).