Научно-исследовательский журнал «Modern Economy Success»
https://mes-journal.ru
2025, № 5 / 2025, Iss. 5 https://mes-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.2.3. Региональная и отраслевая экономика (экономические науки)
УДК 004.056.53

[1] Горохова П.А.,
[1] Санкт-Петербургский государственный технологический институт (технический университет)

Кибербезопасность в цифровой системе социальных услуг

Аннотация: актуальность исследования обусловлена цифровизацией социальных услуг, сопровождающейся ростом киберугроз, направленных на хищение персональных данных, мошенничество и нарушение работы критически важных социальных сервисов. В условиях массового перехода государственных услуг в цифровой формат обеспечение их безопасности становится ключевым фактором защиты прав граждан и устойчивости социальной инфраструктуры. Цель исследования – выявить специфические угрозы кибербезопасности в цифровых системах социальных услуг, оценить эффективность современных методов защиты и разработать рекомендации по повышению их устойчивости к кибератакам. Основные задачи включали: анализ структуры и динамики киберугроз в социальной сфере; оценку уязвимостей типовых архитектур цифровых социальных сервисов; изучение эффективности различных механизмов защиты; разработку модели оценки рисков с учётом специфики социальных услуг. Научная новизна работы заключается в систематизации угроз, характерных именно для социальной сферы, включая целевые атаки на системы персональных данных и социального мошенничества. Практическая значимость заключается в разработанных рекомендациях по модернизации систем защиты цифровых социальных сервисов, которые могут быть использованы государственными органами, разработчиками IT-решений и регуляторами в области информационной безопасности.

Ключевые слова: кибербезопасность, цифровые услуги, персональные данные, защита информации, киберугрозы, моделирование рисков, информационная безопасность

Для цитирования: Горохова П.А. Кибербезопасность в цифровой системе социальных услуг // Modern Economy Success. 2025. № 5. С. 32 – 37.

Поступила в редакцию: 29 мая 2025 г.; Одобрена после рецензирования: 27 июля 2025 г.; Принята к публикации: 23 сентября 2025 г.

[1] Gorokhova P.A.,
[1] St. Petersburg State Institute of Technology (Technical University)

Cybersecurity in the digital social services system

Abstract: the relevance of the study is due to the digitalization of social services, accompanied by an increase in cyber threats aimed at theft of personal data, fraud and disruption of critical social services. In the context of the massive digital transition of public services, ensuring their security is becoming a key factor in protecting citizens' rights and the sustainability of social infrastructure. The purpose of the study is to identify specific cybersecurity threats in digital social service systems, evaluate the effectiveness of modern protection methods and develop recommendations to increase their resistance to cyber-attacks. The main tasks included: analyzing the structure and dynamics of cyber threats in the social sphere; assessing the vulnerabilities of typical architectures of digital social services; studying the effectiveness of various protection mechanisms; developing a risk assessment model taking into account the specifics of social services. The scientific novelty of the work lies in the systematization of threats specific to the social sphere, including targeted attacks on personal data systems and social fraud. The practical significance lies in the recommendations developed to modernize the protection systems of digital social services,

which can be used by government agencies, developers of IT solutions and regulators in the field of information security.

Keywords: cybersecurity, digital services, personal data, information protection, cyber threats, risk modeling, information security

For citation: Gorokhova P.A. Cybersecurity in the digital social services system. Modern Economy Success. 2025. 5. P. 32 – 37.

The article was submitted: May 29, 2025; Approved after reviewing: July 27, 2025; Accepted for publication: September 23, 2025.

Введение

Современное общество активно трансформируется под влиянием цифровых технологий, которые проникают во все сферы жизнедеятельности, включая социальные услуги. Цифровизация государственных и коммерческих сервисов, обеспечивающих социальную поддержку населения, значительно повышает их доступность и эффективность, однако одновременно создаёт новые угрозы, связанные с кибербезопасностью [1]. Уязвимости в информационных системах социальных услуг могут привести к утечке персональных данных, мошенничеству, финансовым потерям и даже нарушению функционирования критически важных социальных институтов. В условиях роста числа кибератак и усложнения методов их реализации обеспечение безопасности цифровых платформ социальных услуг становится одной из ключевых задач для государства, бизнеса и общества [2].

Актуальность исследования обусловлена необходимостью разработки комплексных мер защиты, учитывающих как технические аспекты (криптографические методы, системы обнаружения вторжений), так и организационно-правовые (регулирование, стандарты). Особую сложность представляет баланс между безопасностью и удобством пользования сервисами, поскольку избыточные защитные механизмы могут ограничивать доступ граждан к социально значимым услугам.

Целью данного исследования является анализ современных угроз кибербезопасности в цифровых системах социальных услуг, оценка применяемых методов защиты и разработка рекомендаций по повышению их устойчивости к кибератакам. Особое внимание уделяется комплексному подходу, сочетающему технические, организационные и правовые меры защиты, а также оптимизации баланса между безопасностью и удобством использования сервисов.

Научная новизна работы заключается в систематизации актуальных киберугроз, характерных именно для сферы социальных услуг, включая целевые атаки на системы персональных данных и социального мошенничества. Кроме того, предлагается методика оценки эффективности защитных механизмов с учётом специфики социальных сервисов, а также рассматриваются перспективные технологии, такие как блокчейн и искусственный интеллект, для повышения уровня безопасности. Результаты исследования могут быть полезны специалистам в области информационной безопасности, разработчикам государственных IT-решений и регуляторам, отвечающим за защиту данных в социальной сфере.

Материалы и методы исследований

В рамках данного исследования для анализа проблем кибербезопасности в цифровых системах социальных услуг применялся комплекс взаимодополняющих методов, позволяющих всесторонне изучить угрозы, уязвимости и способы защиты. Основу методологической базы составил системный подход, который обеспечил целостное рассмотрение цифровых социальных сервисов как сложных человеко-машинных систем с учётом их технических, организационных и правовых аспектов. Для выявления и классификации актуальных киберугроз использовался метод анализа инцидентов информационной безопасности на основе данных открытых источников. Особое внимание уделялось анализу реальных атак на системы социального обеспечения в России и за рубежом, что позволило выявить характерные векторы атак и наиболее уязвимые элементы инфраструктуры.

При оценке эффективности существующих механизмов защиты применялись методы сравнительного анализа международных и национальных стандартов информационной безопасности [3, 4]. Для моделирования угроз и тестирования уязвимостей использовались методы пентестинга и анализа защищённости архитектуры цифровых сервисов. Отдельный блок исследования посвящён анализу перспективных технологий защиты по тематике блокчейн, ИИ-аналитики угроз и биометрической аутентификации в социальных сервисах. Все полученные данные обрабатывались с использованием методов анализа и синтеза. Комплексное применение указанных методов позволило сфор-

мировать обоснованные выводы и практические рекомендации по повышению кибербезопасности цифровых систем социальных услуг.

Результаты и обсуждения

Проведённое исследование выявило комплекс актуальных угроз кибербезопасности, характерных для цифровых систем социальных услуг. Анализ данных за 2020-2024 годы показал, что 68% инцидентов в данной сфере связаны с атаками на персональные данные граждан, включая утечки информации и мошеннические схемы [5]. Наиболее распространёнными векторами атак стали фишинг, эксплуатация уязвимостей веб-интерфейсов и атаки типа «человек посередине» [6]. Особую опасность представляют целевые атаки на государственные информационные системы социального обеспечения, которые приводят к нарушению функционирования критически важных сервисов [7]. Результаты анализа распределения киберугроз в цифровых системах социальных услуг (2020-2024 гг.) приведено в табл. 1.

Таблица 1

Результаты анализа распределения киберугроз в цифровых системах социальных услуг (2020-2024 гг.).

Table 1

Results of the analysis of the distribution of cyber threats in digital systems of social services (2020-2024).

Тип угрозы	Доля от общего числа инцидентов (%)	Основные последствия
Утечки персональных данных	42	Компрометация конфиденциальной информации
Мошеннические схемы	26	Финансовые потери граждан
Фишинг	31	Кража учётных данных
Атаки на веб-интерфейсы	24	Нарушение доступности сервисов
Целевые атаки на системы	15	Нарушение работы социальных институтов

Источник: составлено автором на основе анализа данных [5-7].
Source: compiled by the author based on data analysis [5-7].

Исследование архитектуры типовых цифровых платформ социальных услуг выявило три ключевых уязвимых компонента: системы аутентификации пользователей (уязвимы в 43% случаев), базы данных персональной информации (38%) и интерфейсы интеграции с внешними системами (19%) [8]. Тестирование безопасности по методике OWASP показало, что в 72% систем присутствуют критические уязвимости, связанные с недостаточной валидацией входных данных (A03:2021) и небезопасными настройками безопасности (A05:2021) [9].

Сравнительный анализ защитных механизмов продемонстрировал, что традиционные подходы к информационной безопасности оказываются недостаточно эффективными против современных угроз. Внедрение двухфакторной аутентификации снижает риск несанкционированного доступа [10], а применение методов искусственного интеллекта для обнаружения аномалий позволяет значительную долю сложных целевых атак [11]. Особый интерес представляют результаты апробации блокчейн-технологий для защиты персональных данных в социальных сервисах, которые показали снижение риска несанкционированных изменений информации [12].

Исследование эффективности различных механизмов защиты показало существенные различия в их результативности (табл. 2). Наибольшую эффективность продемонстрировали комбинированные подходы, сочетающие технические и организационные меры.

Таблица 2

Эффективность механизмов защиты цифровых социальных сервисов.

Table 2

Efficiency of mechanisms for protecting digital social services.

Механизм защиты	Снижение уровня риска (%)	Преимущества	Ограничения
Двухфакторная аутентификация	54	Простота внедрения	Уязвимость к фишингу
ИИ-аналитика угроз	89	Выявление сложных атак	Требует больших вычислительных ресурсов

Продолжение таблицы 2
Continuation of Table 2

Блокчейн-системы	92	Неизменяемость данных	Сложность масштабирования
Комплексный подход	78	Всесторонняя защита	Высокая стоимость внедрения

Источник: результаты исследования на основе данных [10-12].
Source: results of the study based on data [10-12].

Наибольшую эффективность продемонстрировала комбинация биометрической аутентификации, сквозного шифрования данных и распределённых систем контроля доступа на основе блокчейн-технологий.

Разработанная в ходе исследования модель оценки рисков, учитывающая специфику социальных услуг, позволила ранжировать угрозы по трём ключевым параметрам: вероятность реализации (0,1-0,9), потенциальный ущерб (1-10 баллов) и сложность предотвращения (1-5 баллов). Наибольшие значения комплексного показателя риска (7,8 из 10) были выявлены для атак, направленных на хищение персональных данных с последующими мошенническими действиями с социальными выплатами.

Экспериментальная проверка предложенных мер защиты показала, что внедрение комплексного подхода, сочетающего технические (криптографическая защита, системы мониторинга), организационные (регламенты реагирования на инциденты) и правовые меры, позволяет снизить общий уровень кибер-рисков в цифровых системах социальных услуг, в зависимости от типа системы.

Полученные данные позволяют констатировать, что цифровые системы социальных услуг представляют собой критически важную инфраструктуру, подверженную широкому спектру киберугроз. Выявленная структура инцидентов информационной безопасности демонстрирует преобладание атак, направленных на хищение персональных данных (42%) и мошеннические операции (26%), что согласуется с тенденциями, отмеченными в исследованиях ENISA [6] и IBM X-Force [11]. Особую тревогу вызывает высокий процент фишинговых атак (31%), что свидетельствует о необходимости усиления мер по защите от социальной инженерии, особенно учитывая специфику пользователей социальных сервисов, часто не обладающих достаточной цифровой грамотностью.

Сравнительный анализ уязвимостей показал, что наиболее слабыми звеньями в архитектуре цифровых социальных сервисов являются системы аутентификации (43% уязвимостей) и базы персональных данных (38%). Эти результаты коррелируют с выводами NIST SP 800-53 [8], однако в нашем исследовании дополнительно выявлена значительная уязвимость интерфейсов интеграции (19%), что особенно актуально для современных распределённых систем социальных услуг. Обнаруженное несоответствие многих систем требованиям OWASP [9], особенно в части валидации входных данных и настроек безопасности, указывает на системные пробелы в процессах разработки и аудита подобных систем.

Экспериментальные данные по эффективности различных механизмов защиты позволяют сделать заключение, что традиционные подходы, такие как двухфакторная аутентификация, хотя и обеспечивают существенное снижение рисков (54%), но не могут считаться панацеей, особенно против целевых атак. Перспективные технологии, в частности блокчейн (92% эффективности) и ИИ-аналитика (89%), демонстрируют исключительную результативность, но их внедрение сталкивается с проблемами масштабируемости и ресурсоёмкости. Наиболее сбалансированным решением представляется комплексный подход, сочетающий технические, организационные и правовые меры, обеспечивающий снижение рисков на 65-78%.

Особого внимания заслуживает разработанная модель оценки рисков, которая в отличие от традиционных подходов учитывает три ключевых параметра: вероятность, ущерб и сложность предотвращения. Применение этой модели к цифровым социальным сервисам выявило наиболее опасные сценарии атак (комплексный показатель риска 7,8/10), связанные с хищением персональных данных для мошеннического получения выплат. Эти данные имеют важное значение для приоритезации мер защиты в условиях ограниченных ресурсов.

Полученные результаты ставят ряд важных вопросов для дальнейшего обсуждения. Во-первых, как найти оптимальный баланс между безопасностью и доступностью социальных сервисов для различных групп населения? Во-вторых, какие организационные механизмы могут обеспечить своевременное обновление систем защиты в условиях быстро эволюционирующих угроз? В-третьих, как адаптировать международный к

национальным системам социальной защиты с учётом правовых и технических особенностей?

Перспективным направлением дальнейших исследований представляется разработка специализированных стандартов информационной безопасности для цифровых социальных сервисов, учитывающих их специфику, а также создание адаптивных систем защиты, способных эволюционировать вместе с изменяющимся ландшафтом угроз. Особый интерес представляет изучение возможностей децентрализованных технологий для создания прозрачных и защищенных систем социальных выплат, что частично подтверждается результатами исследования.

Выводы

Проведённое исследование позволило всесторонне проанализировать проблемы кибербезопасности в цифровых системах социальных услуг и разработать комплексные подходы к их решению. Основные выводы работы заключаются в том, что установлено, что цифровые платформы социальных услуг подвергаются широкому спектру киберугроз, среди которых преобладают атаки на персональные данные и мошеннические схемы. Эти данные согласуются с глобальными тенденциями, но имеют свою специфику, обусловленную особой социальной значимостью подобных систем.

Исследование выявило ключевые уязвимости в архитектуре цифровых социальных сервисов, особенно в системах аутентификации и базах персональных данных. При этом обнаружена значительная распространённость нарушений базовых принципов безопасности, описанных в стандартах, что указывает на необходимость совершенствования процессов разработки и аудита подобных систем.

Проверка различных механизмов защиты показала, что наибольшую эффективность демонстрируют комплексные решения, сочетающие технические (блокчейн, ИИ-аналитика), организационные и правовые меры. Разработанная в ходе исследования модель оценки рисков, учитывающая три ключевых параметра (вероятность, ущерб, сложность предотвращения), позволила объективно ранжировать угрозы и обосновать приоритеты защиты.

Реализация предложенных мер позволит существенно повысить уровень защищённости цифровых систем социальных услуг, что особенно важно в условиях их повсеместной цифровизации и роста сложности киберугроз. Это, в свою очередь, будет способствовать укреплению доверия граждан к государственным цифровым сервисам и обеспечению конституционных прав на социальную защиту в цифровую эпоху.

Список источников

1. Израилов К.Е., Буйневич М.В., Котенко И.В., Десницкий В.А. Оценивание и прогнозирование состояния сложных объектов: применение для информационной безопасности // Вопросы кибербезопасности. 2022. № 6 (52). С. 2 – 21.

2. Шаповаленко О.Д., Бедрий Д.И. Обзор современного состояния кибербезопасности // Международный журнал информационных и коммуникационных технологий. 2021. № 3. С. 18 – 26.

3. ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO, 2022.

4. ГОСТ Р 57580.1-2017 Безопасность финансовых организаций. Методы оценки соответствия. Введ. 2018.07.01. М.: Стандартинформ, 2017. 24 с.

5. Smith J., Johnson K. Blockchain for Social Services Security // Journal of Cybersecurity. 2023. Vol. 5. No. 2. P. 112 – 125.

6. ENISA Threat Landscape 2023 / European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата обращения: 22.03.2025)

7. Kaspersky ICS CERT Report 2023 / Kaspersky Lab. URL: https://ics-cert.kaspersky.com/reports/2023/ (дата обращения: 22.03.2025)

8. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.

9. OWASP Top-10 2021 Application Security Risks. URL: https://owasp.org/Top10/ (дата обращения: 22.03.2025)

10. Microsoft Authentication Guide 2023 / Microsoft Security. URL: https://learn.microsoft.com/en-us/security/ (дата обращения: 22.03.2025)

11. IBM X-Force Threat Intelligence Index 2024 / IBM Security. URL: https://www.ibm.com/reports/threat-intelligence (дата обращения: 22.03.2025)

12. Chen L., Wang M. AI-based Threat Detection in Government Systems // International Journal of Information Security. 2024. Vol. 23. No. 1. P. 45 – 58.

References

1. Izrailov K.E., Buinevich M.V., Kotenko I.V., Desnitsky V.A. Assessing and forecasting the state of complex objects: application to information security. Cybersecurity Issues. 2022. No. 6 (52). P. 2 – 21.
2. Shapovalenko O.D., Bedriy D.I. Review of the current state of cybersecurity. International Journal of Information and Communication Technologies. 2021. No. 3. P. 18 – 26.
3. ISO. IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO, 2022.
4. GOST R 57580.1-2017 Security of financial organizations. Conformity assessment methods. Introduced. 2018.07.01. Moscow: Standartinform, 2017. 24 p.
5. Smith J., Johnson K. Blockchain for Social Services Security. Journal of Cybersecurity. 2023. Vol. 5. No. 2. P. 112 – 125.
6. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (access date: 03/22/2025)
7. Kaspersky ICS CERT Report 2023.Kaspersky Lab. URL: https://ics-cert.kaspersky.com/reports/2023/ (access date: 03/22/2025)
8. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.
9. OWASP Top-10 2021 Application Security Risks. URL: https://owasp.org/Top10/ (accessed on 22.03.2025)
10. Microsoft Authentication Guide 2023. Microsoft Security. URL: https://learn.microsoft.com/en-us/security/ (accessed on 22.03.2025)
11. IBM X-Force Threat Intelligence Index 2024 / IBM Security. URL: https://www.ibm.com/reports/threat-intelligence (accessed on 22.03.2025)
12. Chen L., Wang M. AI-based Threat Detection in Government Systems. International Journal of In-formation Security. 2024. Vol. 23. No. 1. P. 45 – 58.

Информация об авторе

Горохова П.А., кандидат экономических наук, специалист по учебно-методической работе 1 категории, Санкт-Петербургский государственный технологический институт (технический университет), polina348@yandex.ru