

УДК 004.056:351.861

## Анализ рисков и направлений их устранения для национальной критической информационной инфраструктуры в условиях роста угроз безопасности

И. А. Василенко

АНОО ВО «Университет «Сириус», федеральная территория «Сириус», 354349, Россия

Стремительный рост кибератак, направленных на ключевые компоненты критически важной информационной инфраструктуры России – от банковских систем и энергетических комплексов до сетей телекоммуникаций, – диктует необходимость создания комплексных и адаптивных мер киберзащиты. Основная цель данного исследования – разработка подходов, позволяющих не только эффективно распределять ресурсы для киберзащиты, но и оценивать угрозы с учетом их приоритетов, что особенно актуально для охраны наиболее уязвимых звеньев системы. В работе проведен детальный анализ уязвимостей инфраструктуры, благодаря которому выделены ключевые области риска, требующие первоочередной защиты. Особое внимание уделено необходимости координации между государственным и частным секторами, а также интеграции технологий искусственного интеллекта. Такие технологии позволяют не только повысить точность прогнозирования кибератак, но и улучшить оперативность в их пресечении. Результаты работы акцентируют значимость внедрения адаптивных стандартов и многоуровневого взаимодействия для эффективной защиты критически важных объектов. Именно такой гибкий и координированный подход к кибербезопасности способствует повышению устойчивости национальной инфраструктуры перед лицом растущих киберугроз. Помимо этого внедрение комплексных технологий в сочетании с унифицированными методами открывает возможности для создания гибкой системы защиты, настроенной на быструю адаптацию к возникающим угрозам и поддерживающей постоянное наблюдение за наиболее значимыми объектами.

**Ключевые слова:** киберугрозы, информационная безопасность, критическая инфраструктура, технологии, защита.

### Введение

Государственная критическая информационная инфраструктура (КИИ) представляет собой комплекс взаимосвязанных систем, на которых держатся как стабильность экономики, так и общественный порядок, а вместе с ними – и общая безопасность страны. Эта инфраструктура включает стратегически значимые отрасли: энергетику, здравоохранение, транспортные сети, телекоммуникации и финансовый сектор. Из-за глубокой взаимозависимости, которая за последние годы лишь усилилась, защита этих компонентов стала требовать более интегрированного подхода, так как кибератаки на один из элементов способны привести к серьезным последствиям для всей системы [1].

По данным Центра стратегических разработок в отчете «Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы», рынок кибербезопасности за 2022 г. достиг объема 193.3 млрд руб., увеличившись на 4 % по сравнению с предыдущим годом. Важным аспектом является успешное импортозамещение: несмотря на значительные геополитические вызовы и уход зарубежных

✉ И.А. Василенко: iravas988@yandex.ru

Поступила в редакцию: 17.11.2024

После доработки: 27.01.2025

Принята к публикации: 31.01.2025

поставщиков, отечественные решения уверенно заняли до 70 % рынка, в то время как доля зарубежных продуктов снизилась до 30 % (в 2021 году показатели составляли 61 и 39 % соответственно).

На фоне учащающихся кибератак и растущей значимости рынка кибербезопасности вопрос анализа рисков для КИИ обрел новую актуальность. В этих условиях особое внимание обращается на разработку гибкой и адаптируемой системы защиты, способной оперативно реагировать на изменяющиеся угрозы [2]. Необходимость защиты уже не ограничивается крупными объектами инфраструктуры, поскольку локальные телекоммуникационные центры, коммунальные службы и региональные транспортные узлы представляют собой не менее важные, а порой и более уязвимые звенья в общей системе. Эти элементы могут стать «точками входа» для злоумышленников, что подчеркивает значимость их защиты.

Цель исследования – анализ актуальных рисков, с которыми сталкивается КИИ в условиях возросшей интенсивности кибератак. В рамках исследования планируется сформировать методы, способствующие оптимальному распределению защитных ресурсов и поддерживающие интеграцию межсекторального взаимодействия, включая разработку унифицированной системы классификации рисков.

### **Внутренние риски и поведенческий мониторинг в безопасности КИИ**

Стратегически важные для государства системы и сети, образующие национальную КИИ, составляют сложный комплекс, от которого зависит как стабильность экономики, так и общественный порядок с обеспечением безопасности. Различные отрасли – от энергетики и здравоохранения до транспортных и телекоммуникационных систем, а также финансовых сетей, включая банковский сектор, – входят в ее состав. Эти системы оказались переплетены настолько тесно, что их взаимозависимость возрастает, обостряя общий риск [3]. Можно утверждать, что каждый из компонентов КИИ ныне подвержен высокой вероятности атак – как индивидуальных, на конкретные узлы, так и на весь связанный ряд объектов, что создает угрозу глобальных последствий при массивных кибератаках.

С учетом стремительного роста угроз, целенаправленно направленных на элементы национальной критической инфраструктуры, все более важными становятся вопросы углубленного многослойного анализа рисков, а также изучения внутренних факторов, представляющих угрозы. Не менее актуальной задачей остается межсекторальное взаимодействие, способствующее слаженной защите инфраструктурных объектов, – не говоря уже о необходимости адаптироваться к быстро меняющимся технологиям защиты, которые включают все более сложные инструменты [4, 5].

Изучение угроз требует внимания к уязвимостям, распределенным по различным уровням инфраструктуры – от крупных ключевых объектов до менее защищенных звеньев «среднего» и «второстепенного» порядка. В то время как распространенные подходы концентрируются на защите значимых элементов (например, на энергетических и транспортных узлах крупных масштабов), слабые места таких средних инфраструктур, как локальные телекоммуникационные центры, коммунальные службы или региональные транспортные системы, представляются не менее значимыми. Злоумышленники могут использовать эти элементы как «точки входа», предоставляющие доступ к важнейшим частям всей системы [6, 7].

Создание системы классификации рисков позволит повысить эффективность распределения ресурсов, акцентируя внимание и финансовую поддержку тех объектов, которые в настоящее время, предположительно, остаются недооцененными в общей системе обеспечения безопасности.

**1. Внутренние риски: сложности мониторинга и предсказания поведения сотрудников.** Ситуация с внутренними угрозами, напрямую зависящими от действий сотрудников, обладающих доступом к критически важным элементам инфраструктуры, настоятельно требует особого внимания. Сложности в предсказании таких рисков усиливаются из-за правовых и этических ограничений, связанных с необходимостью защиты конфиденциальности. Анализировать поведенческие паттерны сотрудников оказывается непростой задачей, особенно если конфиденциальность их данных продолжает оставаться приоритетной. Ключевым решением здесь может стать разработка поведенческих алгоритмов, способных не просто выявлять аномалии, но и прогнозировать потенциальные риски. Однако, как показывают существующие исследования, такая разработка пока недостаточно глубоко освещает возможности совмещения мониторинга и защиты приватности. Для преодоления этой проблемы была предложена концепция адаптивных моделей, использующих машинное обучение для фиксации аномальных отклонений в поведении сотрудников – при этом, важно подчеркнуть, не затрагивая их личное пространство.

Эти модели способны регистрировать нетипичные паттерны (например, повышенный доступ к данным или попытки передачи информации), но без прямого вмешательства в повседневные задачи сотрудников. Предполагается, что внедрение таких аналитических систем, ориентированных на поведенческие особенности, позволит значительно снизить риски внутренних угроз, не нарушая требований конфиденциальности [1, 3].

**2. Кооперация между секторами: барьеры для совместной защиты инфраструктуры.** Эффективная защита критически важных инфраструктур невозможна без координации между государственными и частными организациями, и, тем не менее, различия в правовых и организационных нормах существенно препятствуют такому сотрудничеству. Разобщенность ответственности за безопасность между многочисленными ведомствами и частными компаниями приводит к ослаблению общей структуры защиты. Отсутствие унифицированных стандартов для информационного обмена и взаимодействия при реагировании на угрозы снижает способность оперативно противостоять атакам, для нейтрализации которых требуется интеграция на межсекторальном уровне и скоординированные действия. Необходимость в согласовании законодательных и нормативных основ, регулирующих совместные меры безопасности, является, пожалуй, одной из наиболее актуальных и слабо освещенных проблем обеспечения безопасности КИИ. Введение единых протоколов и стандартов, регулирующих взаимодействие частных и государственных структур, а также организация защищенных платформ для оперативного обмена данными о кибератаках позволили бы укрепить систему защиты [8].

**3. Адаптация к новым технологиям защиты: ответ на угрозы, основанные на искусственном интеллекте.** С развитием искусственного интеллекта (ИИ) безопасность подвергается значительным изменениям – как в аспекте защиты, так и в вопросах новых угроз. ИИ позволяет злоумышленникам использовать методы, включающие фишинг, который базируется на анализе поведения пользователей, а также автоматизированное сканирование уязвимостей – эти технологии, очевидно, усложняют задачи специалистов по кибербезопасности. В ответ на подобные вызовы системы защиты также вынуждены эволюционировать, становясь более гибкими и способными к обучению. Отметим, что системы защиты, применяющие ИИ для анализа поведения атакующих, стали постепенно формировать новый стандарт для защиты КИИ. Не дожидаясь фактического проникновения в сети, эти системы не только улавливают действия злоумышленников, но и прогнозируют вероятные векторы атаки, что позволяет оперативно вносить коррективы в защитные механизмы [3, 9]. И хотя концепция адаптивной защиты от угроз, исходящих от ИИ, требует еще немало исследований и испытаний, ее потенциальная ценность бесспорна: она обеспечивает уникальный уровень защиты, позволяя реагировать на угрозы в реальном времени и создавая, по сути, динамическую среду безопасности, способную приспосабливаться к быстро меняющимся условиям [10].

**4. Необходимость в разработке и внедрении новых стандартов.** Необходимость разработки и внедрения усовершенствованных стандартов безопасности становится все более очевидной: вызовы современности требуют гибких и адаптивных решений. Следует признать, что скорость развития киберугроз нередко опережает обновление правовых норм и стандартов защиты, что требует не просто пересмотра, но и радикального переосмысления подходов к регулированию. Эффективность создаваемой системы защиты будет зависеть, прежде всего, от своевременности внедрения этих стандартов, их устойчивости к меняющимся условиям и способности учитывать межсекторальное взаимодействие – столь необходимое в современных условиях [11, 12].

## **Результаты**

Для оценки влияния стандартов на безопасность КИИ и дальнейшей разработки модели рассмотрим шесть основополагающих критериев.

**1. Гибкость и адаптивность стандарта.** Ключевым фактором в современной кибербезопасности является способность к быстрой адаптации к новым типам угроз [11]. Долгосрочные стандарты, несмотря на их устойчивость, часто не успевают за темпом технологических изменений и разработок в сфере атакующих методов. Поэтому требуется создание гибких протоколов, которые будут позволять своевременно актуализировать защитные механизмы, избегая при этом необходимости в полной переработке существующих стандартов.

**2. Интеграция стандартов с инновационными технологиями.** Такие современные технологии, как ИИ, блокчейн и облачные вычисления, требуют разработки стандартов, которые могли бы объединить классические подходы с новыми цифровыми методами защиты. Например, внедрение протоколов на базе ИИ позволяет не только оценивать угрозы, но и задействовать модели, способные к самообучению, что открывает возможности для своевременного обнаружения аномалий и прогнозирования схем атак.

**3. Поддержка межсекторального сотрудничества.** Эффективность стандартов, регулирующих кибербезопасность, возрастает при их ориентации на обмен данными и согласование ответных действий между частными и государственными организациями. Протоколы такого рода должны отражать интересы всех участников КИИ, предусматривая оперативную координацию на каждом этапе – от момента обнаружения угрозы до ее устранения. Создание единой платформы, обеспечивающей защищенный и быстрый обмен информацией о киберугрозах, способно существенно сократить временные задержки, возникающие при принятии ответных мер, и минимизировать риск внешнего проникновения.

**4. Разработка стандартов с акцентом на оценку рисков и приоритизацию ресурсов.** Ключевой принцип в данном случае – распределение ресурсов пропорционально уровню угроз и значимости отдельных объектов инфраструктуры. Внедрение анализа рисков на разных уровнях позволит сосредоточить защитные усилия на элементах, которые более всего подвержены атакам, что приведет к значительному улучшению общего уровня защищенности.

**5. Введение обязательных процедур для взаимодействия между государственными и частными структурами.** Стандарты, закрепляющие процедуры кооперации, включая унифицированные методы обмена информацией и быстрого реагирования на инциденты, смогут сократить время, требуемое для координации. К тому же такой стандарт должен предусматривать систему обязательного обучения и сертификации сотрудников всех уровней для повышения их компетенции.

**6. Стимулирование внедрения ИИ и иных современных технологий в защиту критически важной инфраструктуры.** Разработка стандартов, использующих возможности ИИ для анализа поведения и прогнозирования угроз, позволит создавать автоматизированные системы реагирования, которые, будучи менее зависимыми от человеческого фактора, значительно повысят оперативность защиты [13].

## Выводы

Проведенный анализ позволяет разработать в дальнейшем современную модель, которая обеспечит возможность объективно оценить стандарты, применяемые к защите критической инфраструктуры, по трем ключевым критериям: адаптивности, технологичности и поддержке межсекторального сотрудничества. Разработка гибких и адаптивных стандартов, ориентированных на всесторонние требования к работе КИИ, и обязательное внедрение взаимодействия между секторами помогут создать комплексную и надежную систему киберзащиты. Подводя итоги анализа, стоит отметить необходимость системного подхода в обеспечении безопасности критической инфраструктуры с акцентом на адаптивность и совместные меры. Реализация предложенных стандартов и мер укрепит устойчивость КИИ к современным угрозам, а также станет гарантией стабильности и безопасности национальной инфраструктуры.

## Финансирование

Работа выполнена без привлечения внешних источников финансирования.

## Конфликт интересов

Конфликт интересов отсутствует.

## Список литературы


1. Maglaras L., Janicke H., Ferrag M.A. Cybersecurity of Critical Infrastructures: Challenges and Solutions // *Sensors*, 2022. V. 22. № 5105. 2022. <https://doi.org/10.3390/s22145105>.
2. Tsantikidou K., Sklavos N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography*, 2024. Vol. 8. № 7. <https://doi.org/10.3390/cryptography8010007>.

3. Корниенко А.А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры: электронное учебное пособие. СПб.: Петербургский государственный университет путей сообщения Императора Александра I, 2022. 63 с. ISBN 978-5-7641-1837-6.
4. Govea J., Gaibor-Naranjo W., Villegas-Ch W. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems*, 2024. V. 12. № 165. <https://doi.org/10.3390/systems12050165>.
5. Aktayeva A., Makatov Y., Tulegenovna A.K., Dautov A., Niyazova R., Zhamankarin M., Khan S. Cybersecurity Risk Assessments within Critical Infrastructure Social Networks // *Data*, 2023. Vol. 8. № 156. <https://doi.org/10.3390/data8100156>.
6. Alqudhaibi A., Albarrak M., Aloheel A., Jagtap S., Salonitis K. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations // *Sensors*, 2023. Vol. 23. № 4539. <https://doi.org/10.3390/s23094539>.
7. Шмунько М.С., Чуйкова В.В. Обеспечение защиты информации на объектах критической информационной инфраструктуры (КИИ) // *Современные информационные технологии и информационная безопасность: труды III Всероссийской научно-технической конференции* (Курск, 2 февраля 2024 г.). Курск: ЗАО «Университетская книга», 2024. С. 156–159.
8. Maglaras L., Kantzavelou I., Ferrag M.A. Digital Transformation and Cybersecurity of Critical Infrastructures. *Applied Sciences*, 2021. V. 11. № 8357. <https://doi.org/10.3390/app11188357>.
9. De Felice F., Baffo I., Petrillo A. Critical Infrastructures Overview: Past, Present and Future. *Sustainability*. V. 14. № 4. P. 2233. <https://doi.org/10.3390/su14042233>.
10. Akwetey H.M., Danquah P., Koi-Akrofi G.Y., Asampama I. Critical Infrastructure Cybersecurity Challenges: IoT In Perspective. *International Journal of Network Security & Its Applications (IJNSA)*, July 2021. V. 13. № 4. <https://doi.org/10.48550/arXiv.2202.12970>.
11. Izonin I., Hovorushchenko T., Shandilya S.K. Quality and Security of Critical Infrastructure Systems. *Big Data and Cognitive Computing*, 2024. V. 8. № 10. <https://doi.org/10.3390/bdcc8010010>.
12. Науголнова И.А. Менеджмент 4.0: эволюция и инновации в управлении организацией в цифровую эпоху // *Теория и практика общественного развития*, 2023. № 6(182). С. 220–226. <https://doi.org/10.24158/tipor.2023.6.28>.
13. Костина Д.О., Владимиров Д.Т., Коновалов В.В. О возможности применения комплексного ИИ в кибербезопасности // *Труды II Всероссийской научной конференции «Искусственный интеллект в автоматизированных системах управления и обработки данных»* (27–28 апреля 2023 г., г. Москва). М.: Издательский дом КДУ, Добросвет, 2023. С. 400–404.

## Risk analysis and mitigation strategies for national critical information infrastructure amidst growing security threats

I.A. Vasilenko 

Sirius University, Sirius Federal Territory, 354349, Russia

 iravas988@yandex.ru

Received November 17, 2024; revised January 27, 2025; accepted January 31, 2025

The rapid increase in cyberattacks targeting critical components of Russia's information infrastructure – from banking systems and energy complexes to telecommunications networks – underscores the need for comprehensive and adaptive cybersecurity measures. This study aims to develop approaches that enable not only the efficient allocation of cybersecurity resources but also the prioritization of threats based on their criticality, which is especially important for protecting the system's most vulnerable links. A detailed analysis of infrastructure vulnerabilities has been conducted, identifying key risk areas that require prioritized protection. Particular attention is given to the necessity of coordination between public and private sectors, as well as the integration of artificial intelligence technologies. Such technologies enhance both the accuracy of cyberattack forecasting and the efficiency of response actions. The study's findings emphasize the importance of implementing adaptive standards and multi-

level collaboration for the effective protection of critical assets. This flexible, coordinated approach to cybersecurity strengthens the resilience of national infrastructure in the face of escalating cyber threats. Additionally, the integration of comprehensive technologies alongside standardized methods creates the potential for a flexible defense system capable of swiftly adapting to emerging threats and enabling continuous monitoring of critical assets.

**Keywords:** cyber threats, information security, critical infrastructure, technologies, protection.

## References

1. Maglaras L., Janicke H., Ferrag M.A. Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors*, 2022, vol. 22, no. 5105. <https://doi.org/10.3390/s22145105>.
2. Tsantikidou K., Sklavos N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography*, 2024, vol. 8, no. 7. <https://doi.org/10.3390/cryptography8010007>.
3. Korniyenko A.A. Sistema trebovaniy k obespecheniyu bezopasnosti avtomatizirovannykh sistem i znachimyykh ob"ektov kriticheskoy informatsionnoy infrastruktury: elektronnoe uchebnoe posobie [System of requirements for ensuring the security of automated systems and critical information infrastructure objects: electronic textbook]. St. Petersburg: St. Petersburg State University of Railway Transport of Emperor Alexander I, 2022, 63 p. ISBN 978-5-7641-1837-6. EDN GESBXD (in Russian).
4. Govea J., Gaibor-Naranjo W., Villegas-Ch W. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems*, 2024, vol. 12, no. 165. <https://doi.org/10.3390/systems12050165>.
5. Aktayeva A., Makatov Y., Tulegenovna A.K., Dautov A., Niyazova R., Zhamankarin M., Khan S. Cybersecurity Risk Assessments within Critical Infrastructure Social Networks. *Data*, 2023, vol. 8, no. 156. <https://doi.org/10.3390/data8100156>.
6. Alqudhaibi A., Albarrak M., Aloseel A., Jagtap S., Salonitis K. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. *Sensors*, 2023, vol. 23, no. 4539. <https://doi.org/10.3390/s23094539>.
7. Shmunko M.S., Chuykova V.V. Obespechenie zashchity informatsii na ob'ektakh kriticheskoy informatsionnoy infrastruktury (KII) [Ensuring Information Security at Critical Information Infrastructure (CII) Facilities]. *Sovremennyye informatsionnyye tekhnologii i informatsionnaya bezopasnost'* [Modern Information Technologies and Information Security]. Proceedings of the 3rd All-Russian Scientific and Technical Conference, Kursk, February 2, 2024. Kursk: ZAO «Universitetskaya kniga», 2024, pp. 156–159 (in Russian).
8. Maglaras L., Kantzavelou I., Ferrag M.A. Digital Transformation and Cybersecurity of Critical Infrastructures. *Applied Sciences*, 2021, vol. 11, no. 8357. <https://doi.org/10.3390/app11188357>.
9. De Felice F., Baffò I., Petrillo A. Critical Infrastructures Overview: Past, Present and Future. *Sustainability*, vol. 14, no. 4. P. 2233. <https://doi.org/10.3390/su14042233>.
10. Akwetey H.M., Danquah P., Koi-Akrofi G.Y., Asampama I. Critical Infrastructure Cybersecurity Challenges: IoT In Perspective. *International Journal of Network Security & Its Applications (IJNSA)*, July 2021, vol. 13, no. 4. <https://doi.org/10.48550/arXiv.2202.12970>.
11. Izonin I., Hovorushchenko T., Shandilya S.K. Quality and Security of Critical Infrastructure Systems. *Big Data and Cognitive Computing*, 2024, vol. 8, no. 10. <https://doi.org/10.3390/bdcc8010010>.
12. Naugolnova I.A. Menedzhment 4.0: evolyutsiya i innovatsii v upravlenii organizatsiy v tsifrovuyu epokhu [Management 4.0: evolution and innovations in organizational management in the digital era]. *Teoriya i praktika obshchestvennogo razvitiya* [Theory and Practice of Social Development], 2023, no. 6(182), pp. 220–226. <https://doi.org/10.24158/tipor.2023.6.28>. EDN KESNPN (in Russian).
13. Kostina D.O., Vladimirov D.T., Kononov V.V. O vozmozhnosti primeneniya kompleksnogo II v kiberbezopasnosti [On the possibility of applying integrated AI in cybersecurity]. *Trudy II Vserossiyskoy nauchnoy konferentsii «Iskusstvennyy intellekt v avtomatizirovannykh sistemakh upravleniya i obrabotki dannykh» (27–28 aprelya 2023 g., g. Moskva)* [Proc. II All-Russian Scientific Conference «Artificial Intelligence in Automated Management Systems and Data Processing» (April 27–28, 2023, Moscow)]. Moscow, Izdatel'skiy dom KDU, Dobrosvet Publ., 2023, pp. 400–404. EDN QMRRDW (in Russian).