Самоловов Д.А., Краснов А.Е. Формализация критерия отказоустойчивости критической информационной инфраструктуры в условиях трансформации киберугроз на основе интеграции показателей конфиденциальности, целостности и доступности // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 6 (68) Ч.1 с. 30–39

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/



УДК 004.056:004.052

ФОРМАЛИЗАЦИЯ КРИТЕРИЯ ОТКАЗОУСТОЙЧИВОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ТРАНСФОРМАЦИИ КИБЕРУГРОЗ НА ОСНОВЕ ИНТЕГРАЦИИ ПОКАЗАТЕЛЕЙ КОНФИДЕНЦИАЛЬНОСТИ, ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ

[1]Самоловов Д.А., [2]Краснов А.Е.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, пр-т Вернадского, д. 78, стр. 4), e-mail: [1]samolovov37@gmail.com, [2]krasnovmgutu@yandex.ru

В статье представлен формализованный критериальный подход к оценке отказоустойчивости критической информационной инфраструктуры в условиях трансформации ландшафта киберугроз и роста значимости информационной безопасности. Актуальность исследования обусловлена необходимостью перехода от фрагментарных и реактивных моделей защиты к интегральным методам анализа устойчивости функционирования систем. Целью работы является разработка интегрального критерия отказоустойчивости на основе показателей конфиденциальности, целостности и доступности, учитывающего взаимосвязь рисков, динамику деградации устойчивости и вероятность отказа элементов. В ходе исследования выполнена формализация структуры критической информационной инфраструктуры как иерархической системы взаимосвязанных активов, предложена модель расчета частных рисков и их агрегирования с учетом взаимозависимости базовых критериев безопасности. Дополнительно разработана динамическая модель изменения устойчивости во времени и учтены механизмы распространения рисков между компонентами инфраструктуры. Практическая значимость работы заключается в возможности применения предложенного критерия для количественной оценки устойчивости, выявления критических состояний системы и обоснования управленческих решений, направленных на повышение надежности и эффективности механизмов информационной безопасности. Полученные результаты позволяют расширить существующие подходы к оценке устойчивости и могут быть использованы при построении систем мониторинга и управления рисками. Предложенный подход также создает основу для дальнейших исследований, направленных на адаптацию моделей к динамически изменяющимся условиям киберугроз и интеграцию интеллектуальных методов анализа.

Ключевые слова: Критическая информационная инфраструктура, отказоустойчивость, устойчивость, конфиденциальность, целостность, доступность.

FORMALIZATION OF THE CRITERION OF FAULT TOLERANCE OF CRITICAL INFORMATION INFRASTRUCTURE IN THE CONTEXT OF CYBER THREAT TRANSFORMATION BASED ON THE INTEGRATION OF CONFIDENTIALITY, INTEGRITY AND ACCESSIBILITY INDICATORS

[1]Samolovov D.A., [2]Krasnov A.E.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue Vernadsky, 78, b. 4), e-mail: [1]samolovov37@gmail.com, [2]krasnovmgutu@yandex.ru

Самоловов Д.А., Краснов А.Е. Формализация критерия отказоустойчивости критической информационной инфраструктуры в условиях трансформации киберугроз на основе интеграции показателей конфиденциальности, целостности и доступности // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 6 (68) Ч.1 с. 30–39

The article presents a formalized criteria-based approach to assessing the fault tolerance of critical information infrastructure in the context of the transformation of the cyber threat landscape and the growing importance of information security. The relevance of the study is due to the need to move from fragmented and reactive protection models to integrated methods for analyzing the stability of systems. The aim of the work is to develop an integrated fault tolerance criterion based on indicators of confidentiality, integrity and accessibility, taking into account the interrelation of risks, the dynamics of stability degradation and the probability of element failure. In the course of the study, the structure of the critical information infrastructure formalized as a hierarchical system of interrelated assets, and a model for calculating private risks and their aggregation proposed, taking into account the interdependence of basic security criteria. Additionally, a dynamic model of stability change over time been developed and the mechanisms of risk propagation between infrastructure components have been taken into account. The practical significance of the work lies in the possibility of applying the proposed criterion to quantify stability, identify critical states of the system and justify management decisions aimed at improving the reliability and effectiveness of information security mechanisms. The obtained results make it possible to expand existing approaches to assessing sustainability and can used in building monitoring and risk management systems. The proposed approach also creates the basis for further research aimed at adapting models to dynamically changing cyber threat conditions and integrating intelligent analysis methods.

Keywords: Critical information infrastructure, resilience, sustainability, confidentiality, integrity, accessibility.

Современный этап цифровизации характеризуется ростом зависимости социально-экономических процессов от функционирования критической информационной инфраструктуры (КИИ), что обуславливает повышение требований к ее устойчивости в условиях воздействия угроз информационной безопасности [1]. Развитие киберугроз, их усложнение и межсистемный характер приводят к тому, что традиционные подходы, ориентированные преимущественно на предотвращение инцидентов, не обеспечивают требуемого уровня надежности функционирования КИИ [2]. В этих условиях особую значимость приобретает обеспечение отказоустойчивости как способности системы сохранять работоспособность при реализации угроз и восстанавливаться после нарушений.

Существующие научные подходы к оценке устойчивости систем информационной безопасности базируются на анализе рисков и использовании критериев конфиденциальности, целостности и доступности, позволяющих количественно описать состояние защищенности информационных активов. Однако данные подходы, как правило, ограничиваются оценкой отдельных аспектов безопасности и не формируют интегрального показателя, отражающего способность системы к функционированию в условиях дестабилизирующих воздействий [Зайка 2024]. Это обусловливает необходимость разработки формализованного критерия отказоустойчивости, учитывающего совокупное влияние указанных критериев и их взаимосвязь. Целью настоящей работы является разработка критериального подхода к оценке отказоустойчивости КИИ на основе интегральной оценки показателей конфиденциальности, целостности и доступности. Для достижения поставленной цели решаются задачи формализации частных критериев, построения модели их агрегирования и обоснования применения полученного критерия для оценки устойчивости функционирования систем информационной безопасности.

1. Формализация структуры критической информационной инфраструктуры. Итак, в соответствии с подходом, представленным в работах А.Е. Краснова и соавторов, критическая информационная инфраструктура рассматривается как иерархическая система, состоящая из множества взаимосвязанных активов:

$A = \{A_1, A_2, \dots, A_N\}$,

с заданной структурой связей, представленной в виде ориентированного графа [7]. При этом устойчивость КИИ определяется не только характеристиками отдельных элементов, но и характером их взаимосвязей (независимость, слабая и сильная зависимость, обратная связь), что приводит к необходимости агрегирования показателей устойчивости на различных уровнях иерархии. Так, задача оценки устойчивости сводится к анализу:

- устойчивости отдельных активов;
- устойчивости их агрегатов;
- влияния межкомпонентных связей на распространение рисков.

2. Критериальная модель оценки рисков на основе CIA-подхода. В качестве базовых критериев оценки состояния активов используются показатели:

- конфиденциальности C;
- целостности I;
- доступности A.

Для каждого актива A_n вводятся коэффициенты значимости:

$K_c(A_n), K_i(A_n), K_a(A_n)$.

С целью нормирования используется [7]:

$$k_c(A_n) = \frac{K_c(A_n)}{K_c(A_n)+K_i(A_n)+K_a(A_n)},$$

$$k_i(A_n) = \frac{K_i(A_n)}{K_c(A_n)+K_i(A_n)+K_a(A_n)},$$

$$k_a(A_n) = \frac{K_a(A_n)}{K_c(A_n)+K_i(A_n)+K_a(A_n)}.$$

Риски по каждому критерию определяются как произведение:

$$\mu_c(R|A_n) = k_c(A_n) * \mu_c(T|A_n) * \mu_c(V|A_n),$$

$$\mu_i(R|A_n) = k_i(A_n) * \mu_i(T|A_n) * \mu_i(V|A_n),$$

$$\mu_a(R|A_n) = k_a(A_n) * \mu_a(T|A_n) * \mu_a(V|A_n),$$

где: $\mu(T)$ - степень реализации угрозы,

$\mu(V)$ - степень уязвимости,

а значения лежат в диапазоне $(0; 1)$.

Так, риск представляет собой логико-вероятностную оценку воздействия угроз на актив [Краснов 2021].

3. Агрегирование критериев и получение интегрального риска. Поскольку критерии C, I, A являются зависимыми, их объединение осуществляется с учетом корреляции [Краснов 2021]:

$$\mu_{ci}(R|A_n) = \mu_c + \mu_i - \mu_c\mu_i,$$

$$\mu_{cia}(R|A_n) = \mu_c + \mu_i + \mu_a - \mu_c\mu_i - \mu_c\mu_a + \mu_c\mu_i\mu_a.$$

Полученное выражение представляет собой:

- первые слагаемые - независимый вклад критериев;
- последующие - учет парных и тройных корреляций.

Итоговая величина:

$$\mu_{cia}(R|A_n)$$

характеризует интегральный риск актива.

4. Модель распространения рисков и уязвимостей. С учетом взаимосвязанности компонентов КИИ риск агрегированного узла определяется рекурсивно на основе рисков входящих элементов. Дополнительно в [Мосолов 2022] показано, что для анализа уязвимых комбинаций элементов используется комбинаторный подход:

$C_n^k = \frac{n!}{(n-k)!k!}$,

что позволяет определить множество возможных отказов системы и их комбинаций. Вероятность критического отказа фрагмента системы может быть представлена в виде:

$P = \prod p_{\text{отк}} * \prod p_{\text{безотк}}$,

что отражает совместное влияние отказов и безотказной работы элементов на устойчивость системы. Данный подход позволяет выявлять наиболее критические сегменты КИИ, обладающие максимальной уязвимостью.

5. Динамическая модель устойчивости системы. В работах [Кузнецов 2024, Краснов 2024] устойчивость рассматривается как динамический показатель, изменяющийся во времени. Базовая модель изменения уровня устойчивости имеет экспоненциальный характер:

$X_n = X_{n-1} e^{-\Delta t / T}$,

где T - период потери устойчивости,

Δt - временной шаг.

Такая модель отражает естественное снижение устойчивости системы под воздействием угроз. Дополнительно динамика риска описывается дифференциальным уравнением:

$\frac{d\mu}{dt} = -\frac{\mu}{\tau} + \Delta ACT(t)$,

где τ - время релаксации,

ΔACT - результирующая активность угроз и мер противодействия.

Так, устойчивость системы определяется как результат баланса активности угроз и эффективности защитных механизмов.

6. Формирование критерия отказоустойчивости (авторское предложение). На основе рассмотренных моделей предлагается ввести интегральный критерий отказоустойчивости КИИ в виде функции от:

- интегрального риска μ_{cia};
- динамики изменения устойчивости;
- вероятности отказа элементов.

Предлагаемый критерий может быть записан в общем виде:

$K_{fail} = (1 - \mu_{cia}) * e^{-t/T} * (1 - P_{\text{отк}})$,

где μ_{cia} - интегральный риск (CIA),

$e^{-t/T}$ - динамика деградации устойчивости,

$P_{\text{отк}}$ - вероятность отказа критических элементов.

Интерпретация:

- при росте рисков → критерий уменьшается;
- при росте вероятности отказа → система теряет устойчивость;
- при увеличении времени без управления → устойчивость падает.

7. Пример расчета критерия отказоустойчивости КИИ. Для демонстрации работоспособности предложенного критерия рассмотрим условный актив КИИ, для которого заданы значения частных рисков по критериям конфиденциальности, целостности и доступности:

$\mu_c = 0.3, \mu_i = 0.4, \mu_a = 0.5.$

Расчет интегрального риска. С учетом зависимости критериев используем выражение [Краснов 2024]:

$\mu_{cia} = \mu_c + \mu_i + \mu_a - \mu_c\mu_i - \mu_c\mu_a - \mu_i\mu_a + \mu_c\mu_i\mu_a,$

Подставляя значения:

$\mu_{cia} = 0.3 + 0.4 + 0.5 - 0.12 - 0.15 - 0.2 + 0.06 = 0.79.$

Задание параметров модели. Примем:

- период потери устойчивости: $T = 10$;
- вероятность отказа: $P_{\text{отк}} = 0.2$.

Критерий отказоустойчивости:

$K_{fail} = (1 - \mu_{cia}) * e^{-t/T} * (1 - P_{\text{отк}}),$

$K_{fail} = 0.21 - e^{-t/10} * 0.8 = 0.168 * e^{-t/10}.$

Результаты расчета (для разных моментов времени) представлены в Таблице 1.

Таблица 1 – Расчет критерия отказоустойчивости во времени

t	$(e^{-t/10})$	(K_{fail})
0	1,000	0,168
2	0,819	0,138
4	0,670	0,113
6	0,549	0,092
8	0,449	0,075
10	0,368	0,062
12	0,301	0,051
14	0,247	0,042
16	0,202	0,034

Для анализа изменения отказоустойчивости критической информационной инфраструктуры во времени на основе данных Таблицы 1 построена зависимость критерия K_{fail} от времени функционирования системы при фиксированных значениях интегрального риска и вероятности отказа (Рисунок 1).

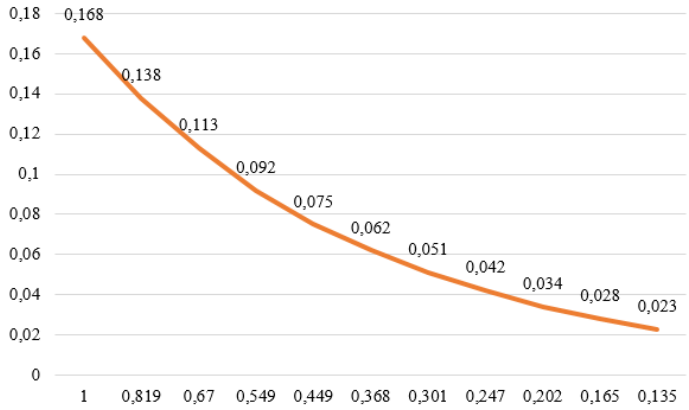


Рисунок 1 – Зависимость критерия отказоустойчивости от времени функционирования системы

Полученная зависимость носит экспоненциальный характер, что отражает естественное снижение устойчивости системы при отсутствии корректирующих воздействий. Установлено, что на начальном этапе снижение критерия происходит наиболее интенсивно, после чего темп деградации уменьшается. Это свидетельствует о необходимости реализации механизмов управления устойчивостью на ранних стадиях развития инцидента для предотвращения значительного снижения отказоустойчивости.

Анализ влияния вероятности отказа. Теперь зафиксируем:

$$t = 5, e^{-0.5} = 0.607$$

$K_{fail} = (1 - 0.79) * 0.607 * (1 - P_{\text{отк}}) = 0.127 * (1 - P_{\text{отк}})$.

В Таблице 2 представлены результаты расчета влияния вероятности отказа.

Таблица 2 - Влияние вероятности отказа

$(P_{\text{отк}})$	(K_{fail})
0,0	0,127
0,1	0,114
0,2	0,102
0,3	0,089
0,4	0,076
0,5	0,064
0,6	0,051
0,7	0,038
0,8	0,025

На основе данных Таблицы 2 построена зависимость критерия отказоустойчивости K_{fail} от вероятности отказа элементов КИИ при фиксированных значениях времени и интегрального риска (Рисунок 2).

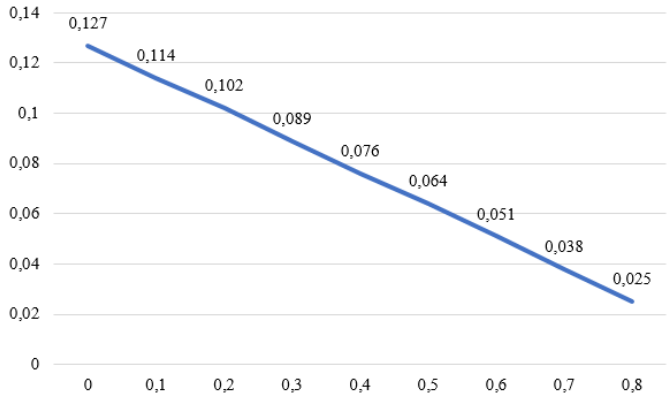


Рисунок 2 – Зависимость критерия отказоустойчивости от вероятности отказа элементов системы

Анализ графика показывает практически линейное снижение критерия отказоустойчивости с увеличением вероятности отказа. Данный результат подтверждает, что надежность отдельных компонентов системы оказывает прямое влияние на устойчивость КИИ в целом. При достижении высоких значений вероятности отказа наблюдается критическое снижение K_{fail}, что указывает на необходимость приоритизации мероприятий по повышению надежности ключевых элементов инфраструктуры.

Анализ влияния уровня риска (CIA). Зафиксируем:

$t = 5 => e^{-0.5} = 0.607,$

$P_{\text{отк}} = 0.2,$

Тогда:

$K_{fail} = (1 - \mu_{cia}) * 0.607 * 0.8 = 0.486 * (1 - \mu_{cia}).$

В Таблице 3 отражено влияние интегрального риска.

Таблица 3 - Влияние интегрального риска

(μ_{cia})	(K_{fail})
0,1	0,437
0,2	0,389
0,3	0,340
0,4	0,292
0,5	0,243
0,6	0,194
0,7	0,146
0,8	0,097
0,9	0,049

Для оценки влияния уровня информационных рисков на отказоустойчивость КИИ на основе данных Таблицы 3 построена зависимость критерия K_{fail} от интегрального показателя риска μ_{cia}, агрегирующего критерии конфиденциальности, целостности и доступности.

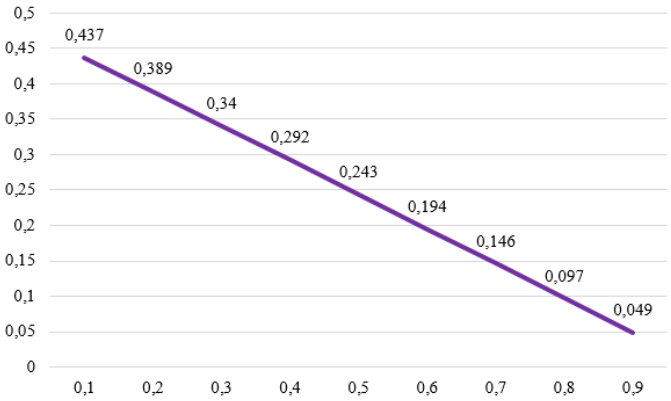


Рисунок 3 – Зависимость критерия отказоустойчивости от интегрального риска (CIA)

Полученные результаты демонстрируют снижение критерия отказоустойчивости при увеличении интегрального риска. Наиболее существенное падение наблюдается в диапазоне высоких значений μ_{cia}, что свидетельствует о высокой чувствительности системы к ухудшению параметров безопасности. Данный факт подтверждает ключевую роль критериев конфиденциальности, целостности и доступности в формировании устойчивости КИИ и обосновывает необходимость их комплексного контроля.

Полученные результаты демонстрируют, что критерий отказоустойчивости является чувствительным к трем ключевым факторам: уровню интегрального риска, вероятности отказа и времени функционирования системы без корректирующих воздействий. При этом наибольшее влияние оказывает интегральный риск, формируемый на основе критериев конфиденциальности, целостности и доступности, что подтверждает корректность выбранного критериального подхода.

В результате проведенного исследования разработан критериальный подход к оценке отказоустойчивости критической информационной инфраструктуры на основе интеграции показателей конфиденциальности, целостности и доступности. На основе анализа работ А.Е. Краснова и соавторов выполнена формализация взаимосвязи между рисками информационной безопасности, устойчивостью системы и вероятностью отказа ее элементов. Сформирован математический аппарат, позволяющий перейти от оценки частных критериев к интегральному показателю отказоустойчивости, учитывающему как структурные особенности КИИ, так и динамику воздействия угроз. Проведенные расчетные эксперименты подтвердили адекватность предложенной модели и ее применимость для анализа устойчивости функционирования систем в условиях дестабилизирующих воздействий. В качестве основных выводов по работе следует отметить:

1. Разработана математическая модель оценки отказоустойчивости КИИ, основанная на агрегировании критериев конфиденциальности, целостности и доступности с учетом их взаимозависимости и влияния на интегральный риск системы.

2. Установлено, что отказоустойчивость КИИ определяется совокупным влиянием интегрального риска, вероятности отказа элементов и времени функционирования системы, при этом наибольшее влияние оказывает уровень информационного риска.

3. Подтверждено, что предложенный критерий отказоустойчивости позволяет количественно оценивать устойчивость КИИ и выявлять критические условия ее деградации, что обеспечивает возможность обоснования управленческих решений по повышению надежности и устойчивости функционирования системы.

Список литературы

1. Родионов М. А., Егоров Е. Ю. защита критической информационной инфраструктуры как необходимое условие обеспечения экономической безопасности России // Экономика и бизнес: теория и практика. 2024. №3-2 (109). С. 77-81.
2. Мальцев М.С., Кулакова Н.С. Защита сети значимых объектов критической информационной инфраструктуры (КИИ) АСУТП // Вестник магистратуры. 2023. №10-2 (145). С. 40-42.
3. Зайка В. М. Обеспечение безопасности объекта критической информационной инфраструктуры // Вестник науки. 2024. №10 (79). С. 750-758.
4. Мосолов А.С., Краснов А.Е., Урбан Н.А. О применении метода анализа уязвимостей технологического процесса производственного объекта для обеспечения информационной безопасности асу тп с учётом взаимосвязи компонентов // Безопасность информационных технологий = IT Security. Том 29. № 3. 2022. С. 38-52.
5. Кузнецов А. С., Краснов А. Е. Информационное обеспечение импульсного управления устойчивостью систем информационной безопасности // Information Science. Information Security. Mathematics. 2024. № 2. С. 99–108.
6. Краснов А. Е., Кузнецов А. С., Смирнов В. М. Модель импульсного управления устойчивостью системы информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 80–90.
7. Краснов А. Е., Мосолов А. С., Феоктистова Н. А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий = IT Security. 2021. Т. 28. № 1. С. 106–120.
8. Бакшеев А.С., Лившиц И.И. Разработка методики контроля уровня защищенности информации объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2023. №2 (54). С. 85-98.

References

1. Rodionov M. A., Egorov E. Yu. Protection of critical information infrastructure as a necessary condition for ensuring Russia's economic security // Economy and business: theory and practice. 2024. No. 3-2 (109). pp. 77-81.
2. Mal'tsev M. S., Kulakova N. S. Protection of the network of significant objects of critical information infrastructure (CII) of automated process control systems // Bulletin of the Magistracy. 2023. No. 10-2 (145). pp. 40-42.
3. Zayka V. M. Ensuring the security of a critical information infrastructure facility // Bulletin of science. 2024. No. 10 (79). pp. 750-758.
4. Mosolov A. S., Krasnov A. E., Urban N. A. On the Application of the Vulnerability Analysis Method for the Technological Process of an Industrial Facility to Ensure Information Security

of an APCS Taking into Account the Interrelationships of Components // IT Security. Vol. 29. No. 3. 2022. pp. 38-52.

5. Kuznetsov A. S., Krasnov A. E. Information Support for Impulse Control of the Stability of Information Security Systems // Information Science. Information Security. Mathematics. 2024. No. 2. pp. 99-108.
6. Krasnov A. E., Kuznetsov A. S., Smirnov V. M. A Model of Impulse Control of the Stability of an Information Security System // Bulletin of the Russian State University for the Humanities. Series "Computer Science. Information Security. Mathematics". 2024. No. 1. pp. 80-90.
7. Krasnov A. E., Mosolov A. S., Feoktistova N. A. Assessing the Resilience of Critical Information Infrastructures to Information Security Threats // Information Technology Security = IT Security. 2021. Vol. 28. No. 1. pp. 106–120.
8. Baksheev A. S., Livshits I. I. Development of a Methodology for Monitoring the Level of Information Security of Critical Information Infrastructure Facilities // Cybersecurity Issues. 2023. No. 2 (54). pp. 85-98.