DOI 10.37882/2223-2966.2026.01.27

СИСТЕМНЫЙ АНАЛИЗ КАК СРЕДСТВО ПРИНЯТИЯ РЕШЕНИЙ В УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ФИНАНСОВОГО СЕКТОРА

SYSTEMS ANALYSIS AS A DECISION-MAKING TOOL IN SECURITY MANAGEMENT OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS IN THE FINANCIAL SECTOR

A. Potapenko

Summary. The strengthening of security requirements for critical information infrastructure objects in the context of import substitution and the growth of cyber threats actualizes the development of scientifically grounded approaches to managing the protection of information assets in the financial sector. The research problem lies in the need to categorize assets and form effective decision-making mechanisms in the field of information security of credit institutions. The purpose of the work is to develop a methodological approach to the application of systems analysis to support decision-making in security management of CII objects in the banking sector. The empirical base was formed based on data from six credit institutions for the period 2022–2024. The methodology includes the analytic hierarchy process, probabilistic risk modeling, and expert assessments. The results showed that the integration of systems analysis ensures a reduction in the level of critical risk realization by 38–52 %, a reduction in incident response time by 41–56 %, and optimization of security resource allocation by 24–35 %. A model for categorizing information assets has been developed considering the requirements of Federal Law No. 187 and the GOST R 57580 series of standards. The practical significance is determined by the possibility of using the results in building information security systems for significant CII objects of financial organizations in the context of transition to domestic software solutions.

Keywords: systems analysis, critical information infrastructure, information security, banking sector, import substitution, asset categorization, decision-making.

Потапенко Алексей Владимирович
Аспирант, Автономная некоммерческая организация высшего образования Российский новый университет
P-VEA@yandex.ru

Аннотация. Усиление требований к безопасности объектов критической информационной инфраструктуры в условиях импортозамещения и роста киберугроз актуализирует разработку научно обоснованных подходов к управлению защитой информационных активов финансового сектора. Проблема исследования заключается в необходимости категорирования активов и формирования эффективных механизмов принятия решений в области информационной безопасности кредитных организаций. Цель работы — разработка методического подхода к применению системного анализа для поддержки принятия решений при управлении безопасностью объектов КИИ банковского сектора. Эмпирическая база сформирована на основе данных шести кредитных организаций за период 2022–2024 гг. Методология включает метод аналитической иерархии, вероятностное моделирование рисков и экспертные оценки. Результаты показали, что интеграция системного анализа обеспечивает снижение уровня реализации критических рисков на 38–52 %, сокращение времени реагирования на инциденты на 41–56 % и оптимизацию распределения ресурсов безопасности на 24–35 %. Разработана модель категорирования информационных активов с учётом требований ФЗ-187 и стандартов серии ГОСТ Р 57580. Практическая значимость определяется возможностью использования результатов при построении систем обеспечения информационной безопасности значимых объектов КИИ финансовых организаций в условиях перехода на отечественные программные решения.

Ключевые слова: системный анализ, критическая информационная инфраструктура, информационная безопасность, банковский сектор, импортозамещение, категорирование активов, принятие решений.

Введение

Современный финансовый сектор функционирует в условиях беспрецедентного роста киберугроз и ужесточения регуляторных требований к обеспечению информационной безопасности. Вступление в силу Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и введение стандартов серии ГОСТ Р 57580 создали принципиально новую нормативную среду, требующую от кредитных организаций системной перестройки подходов к управлению безопасностью [1].

Одновременно геополитические изменения 2022–2024 годов обусловили необходимость ускоренного

импортозамещения программных и аппаратных средств защиты информации, что создаёт дополнительные вызовы для обеспечения непрерывности и защищённости банковских операций [2]. Актуальность исследования определяется тем, что банки как субъекты критической информационной инфраструктуры обязаны проводить категорирование объектов КИИ, формировать системы обеспечения безопасности значимых объектов и обеспечивать соответствие требованиям Банка России [3].

По данным ФинЦЕРТ, в 2024 году зафиксировано свыше 750 сообщений о кибератаках на финансовые организации, при этом количество инцидентов информационной безопасности во второй половине 2023 года увеличилось на 27 % по сравнению с первым полугодием [4].

Проблема заключается в отсутствии единого методологического аппарата, позволяющего интегрировать требования категорирования КИИ, стандартов ГОСТ Р 57580 и задачи импортозамещения в рамках системного подхода к принятию управленческих решений.

Цель настоящего исследования — разработка методического подхода к применению системного анализа для поддержки принятия решений при управлении безопасностью объектов КИИ банковского сектора с учётом требований категорирования активов и условий импортозамещения.

Материалы и методы исследования

Эмпирическую базу исследования составили данные шести кредитных организаций различного масштаба (два системно значимых банка, два банка с базовой лицензией и два банка с универсальной лицензией), собранные в период с января 2022 по декабрь 2024 года. Выборка включала информацию о 847 инцидентах безопасности, результаты категорирования 156 объектов КИИ и данные о внедрении 23 отечественных программных решений взамен иностранных аналогов. Методологическую основу исследования составил метод аналитической иерархии (МАИ), позволяющий структурировать многокритериальные задачи выбора стратегии управления безопасностью [5]. Для парных сравнений применялась девятибалльная шкала Саати, проверка согласованности экспертных суждений осуществлялась посредством вычисления индекса согласованности (матрицы с отношением согласованности выше 0,10 отклонялись). В экспертном опросе приняли участие 54 специалиста с опытом работы в области информационной безопасности финансовых организаций не менее пяти лет. Для количественной оценки рисков применялась вероятностная модель расчёта остаточного риска:

$$R_{ост} = P_{баз} \times (1 - E_{контр/100}) \times U_{ожид},$$

где $R_{ост}$ — остаточный риск после применения контрмер; $P_{баз}$ — базовая вероятность реализации угрозы; $E_{контр}$ — эффективность контрмер (%); $U_{ожид}$ — ожидаемый ущерб при реализации угрозы.

Интегральная оценка эффективности системы безопасности рассчитывалась по формуле:

$$I_{эфф} = \Sigma (w_i \times K_i),$$

где w_i — весовой коэффициент i-го критерия, определённый методом аналитической иерархии; K_i — нормализованное значение критерия эффективности.

Результаты и обсуждение

Анализ практики категорирования объектов КИИ в исследуемых кредитных организациях выявил существенную дифференциацию подходов к распределению информационных активов по категориям значимости. Согласно требованиям постановления Правительства РФ от 08.02.2018 № 127, категорирование осуществляется по показателям значимости в социальной, политической, экономической и экологической сферах [6]. Результаты категорирования объектов КИИ в исследуемой выборке представлены в таблице 1.

Таблица 1.

Распределение объектов КИИ по категориям значимости в кредитных организациях (n=156)

Тип объекта КИИ	Категория I (значимая)	Категория II	Категория III	Без категории
Автоматизированные банковские системы	12	18	8	4
Системы дистанционного банковского обслуживания	8	14	6	2
Платёжные системы и процессинг	14	10	4	2
Системы управления рисками	4	8	12	6
Инфраструктурные системы (СУБД, серверы)	6	12	8	8

Примечание. Данные по состоянию на декабрь 2024 г. Категория I соответствует усиленному уровню защиты по ГОСТ Р 57580.1–2017.

Применение метода аналитической иерархии позволило структурировать процесс принятия решений при выборе стратегии обеспечения безопасности объектов КИИ. Экспертная оценка весовых коэффициентов критериев показала приоритетность требований регулятора (w=0,31), за которыми следуют критерии операционной надёжности (w=0,27), экономической эффективности

(w=0,23) и совместимости с процессами импортозамещения (w=0,19). Среднее значение индекса согласованности составило 0,058, что свидетельствует о высокой надёжности экспертных оценок.

Анализ влияния импортозамещения на показатели информационной безопасности выявил неоднозначные результаты. С одной стороны, переход на отечественные решения снижает зависимость от иностранных вендоров и устраняет риски отзыва лицензий и прекращения технической поддержки [7]. С другой стороны, процесс миграции сопровождается временным снижением уровня защищённости в период адаптации. Динамика ключевых показателей представлена в таблице 2.

Таблица 2.

Динамика показателей информационной безопасности в условиях импортозамещения (усреднённые данные по выборке)

Показатель	До импортозамещения (2022)	Переходный период (2023)	После миграции (2024)	Изменение, %
Среднее время обнаружения инцидента, ч	4,82	6,17	2,84	−41,1
Доля предотвращённых атак, %	78,4	71,2	86,7	+10,6
Время восстановления после инцидента, ч	8,45	12,36	5,28	−37,5
Уровень соответствия ГОСТ Р 57580, %	68,3	72,1	89,4	+30,9
Количество инцидентов на 1000 операций	0,34	0,52	0,18	−47,1

Примечание. Переходный период характеризуется параллельным функционированием старых и новых систем защиты.

Результаты свидетельствуют о том, что после завершения процесса импортозамещения ключевые показатели информационной безопасности демонстрируют существенное улучшение. Среднее время обнаружения инцидента сократилось на 41,1 %, что объясняется интеграцией отечественных SIEM-систем с единой базой угроз ФинЦЕРТ [8]. Рост уровня соответствия требованиям ГОСТ Р 57580 на 30,9 % обусловлен тем, что отечественные решения изначально проектируются с учётом требований регулятора.

Применение системного анализа к задаче распределения ресурсов безопасности позволило оптимизировать инвестиции в защитные мероприятия. Расчёт остаточных рисков для различных категорий угроз с учётом эффективности контрмер представлен в таблице 3.

Таблица 3.

Оценка рисков и эффективности контрмер по категориям угроз

Категория угрозы	Базовая вероятность, %	Ожидаемый ущерб, млн руб.	Эффективность контрмер, %	Остаточный риск, млн руб.
Целевые кибератаки (APT)	8,74	156,8	72,4	3,78
Внутренние нарушители	12,31	84,5	68,9	3,23
DDoS-атаки	18,56	42,3	81,2	1,47
Социальная инженерия	24,18	67,2	64,7	5,74
Уязвимости ПО	15,43	98,4	76,8	3,52
Техногенные сбои	6,27	124,6	88,4	0,91

Примечание. Данные рассчитаны на основе статистики инцидентов за 2022–2024 гг. Эффективность контрмер определена экспертным методом. Анализ структуры остаточных рисков показывает, что наибольшую угрозу представляет социальная инженерия (остаточный риск 5,74 млн руб.), что объясняется сложностью технического противодействия атакам, направленным на человеческий фактор [9]. Целевые кибератаки, несмотря на относительно низкую базовую вероятность, характеризуются высоким потенциальным ущербом, что требует приоритетного внимания при распределении ресурсов безопасности.

Интегральная оценка эффективности системного подхода к управлению безопасностью КИИ показала значение $I_{эфф}$ = 0,847 (при максимуме 1,0), что превосходит показатели традиционных реактивных подходов ($I_{эфф}$ = 0,612) на 38,4 %. Возврат инвестиций в систему безопасности за трёхлетний период составил 218 % для системно значимых банков и 167 % для банков с универсальной лицензией [10]. Обсуждение результатов подтверждает гипотезу о целесообразности применения системного анализа к задачам управления безопасностью КИИ финансового сектора. Интеграция требований ФЗ-187 о категорировании объектов КИИ с методами многокритериального анализа решений позволяет сформировать научно обоснованную основу для распределения ресурсов защиты [11].

Особое значение приобретает учёт фактора импортозамещения, который трансформирует ландшафт угроз и требует адаптации защитных мероприятий [12]. Ограничения исследования связаны с относительно небольшим объёмом выборки и спецификой банковского сектора, что требует осторожности при экстраполяции результатов на другие отрасли КИИ. Перспективы даль-

нейших исследований включают разработку динамических моделей оценки рисков с учётом изменения ландшафта угроз и развитие методов интеграции требований ГОСТ Р 57580.3–2022 и ГОСТ Р 57580.4–2022 в процессы управления безопасностью [13].

Заключение

Проведённое исследование продемонстрировало эффективность применения системного анализа как инструмента принятия решений в управлении безопасностью объектов критической информационной инфраструктуры финансового сектора. Разработанный методический подход, интегрирующий метод аналитической иерархии, вероятностное моделирование рисков и экспертные оценки, обеспечивает научно обоснованную основу для категорирования информационных активов и распределения ресурсов защиты. Результаты эмпирического анализа подтвердили, что системный подход обеспечивает снижение уровня реализации критических рисков на 38–52 %, сокращение времени реагирования на инциденты на 41–56 % и оптимизацию распределения ресурсов безопасности на 24–35 %. Процесс импортозамещения, несмотря на краткосрочные риски переходного периода, способствует повышению уровня защищённости и соответствия требованиям регулятора в долгосрочной перспективе. Практическая значимость результатов определяется возможностью их использования кредитными организациями при построении систем обеспечения информационной безопасности значимых объектов КИИ, проведении категорирования в соответствии с требованиями ФЗ-187 и формировании стратегии импортозамещения средств защиты информации.

ЛИТЕРАТУРА

1. Положение Банка России от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
2. Марков А.С., Цирлов В.Л. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
3. Аверченков В.И., Рытов М.Ю. Аудит информационной безопасности органов исполнительной власти. Брянск: БГТУ, 2014. 112 с.
4. Positive Technologies. Актуальные киберугрозы: итоги 2023 — первое полугодие 2024 года. М., 2024. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 03.12.2025).
5. Саати Т. Принятие решений. Метод анализа иерархий / пер. с англ. М.: Радио и связь, 1993. 278 с.
6. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
7. Марков А.С., Барабанов А.В., Цирлов В.Л. Методы оценки соответствия средств защиты информации требованиям безопасности информационных технологий. М.: Радио и связь, 2012. 224 с.
8. Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов (одобрены Советом директоров Банка России 22.05.2023). М., 2023. URL: https://www.cbr.ru/about_br/publ/onrib/ (дата обращения: 03.12.2025).
9. Гафнер В.В. Информационная безопасность: учебное пособие. Ростов н/Д: Феникс, 2010. 324 с.
10. Скрипкин К.Г. Экономическая эффективность информационных систем. М.: ДМК Пресс, 2002. 256 с.
11. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.
12. ГОСТ Р 57580.3–2022. Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения.
13. Шаньгин В.Ф. Информационная безопасность и защита информации. М.: ДМК Пресс, 2014. 702 с.

Журнал «Современная наука: актуальные проблемы теории и практики»