

УДК 338.4

DOI: 10.34670/AR.2026.26.31.098

Организационно-экономический механизм управления уровнем безопасности: алгоритм принятия решений и оптимизация инвестиций

Цибулина Екатерина Владимировна

Аспирант

Московский государственный

технологический университет «СТАНКИН»;

127055, Российская Федерация, Москва, Вадковский переулок, 1;

e-mail: katsibulina@gmail.com

Аннотация

В статье исследуется проблема экономической неэффективности инвестиций в информационную безопасность (ИБ) в условиях цифровой трансформации. Показано, что традиционные подходы к бюджетированию ИБ часто носят реактивный характер и не учитывают зависимость стоимости защиты от уровня цифровой зрелости организации, что приводит как к дефициту средств на критические меры, так и к избыточному финансированию неактуальных направлений. Разработан организационно-экономический механизм управления уровнем безопасности, объединяющий организационный, инструментальный и экономический блоки и адаптированный под уровни цифровой трансформации. Предложен алгоритм принятия управленческих решений, который переводит интегральный индекс безопасности в конкретные инвестиционные сценарии через диагностику, целеполагание, анализ разрыва, выбор корректирующих мер и последующий мониторинг. Обоснована методика расчета возврата на инвестиции (ROI) для превентивных мер защиты в экосистемных бизнес-моделях. На примере финансовой организации (ПАО Сбербанк) проведена оценка экономической эффективности механизма. Расчеты показали, что применение алгоритма позволяет повысить уровень безопасности с 0,625 до 0,800 при оптимизации затрат, обеспечив расчетный ROI защитных мер на уровне 242%. Результаты исследования могут быть использованы руководителями и риск-менеджерами для обоснования бюджетов на ИБ и балансировки рисков цифровизации.

Для цитирования в научных исследованиях

Цибулина Е.В. Организационно-экономический механизм управления уровнем безопасности: алгоритм принятия решений и оптимизация инвестиций // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 6А. С. 1056-1061. DOI: 10.34670/AR.2026.26.31.098

Ключевые слова

Организационно-экономический механизм, управление уровнем безопасности, цифровая трансформация, инвестиционная привлекательность, ROI защиты, риск-ориентированный подход, алгоритм принятия решений, методология исследования, экономическая эффективность.

Введение

В условиях «бесконечного» процесса цифровой трансформации обеспечение безопасности становится одним из ключевых факторов устойчивого развития бизнеса. Однако, по мере усложнения цифровых экосистем (переход от уровня 2 «Интеграция» к уровню 4 «Экосистема»), растут не только технологические риски, но и стоимость их нейтрализации [Попов, Ральникова, 2023].

Актуальность исследования обусловлена противоречием между необходимостью высоких инвестиций в кибербезопасность и ограниченной способностью бизнеса обосновывать эти затраты с точки зрения экономической эффективности [Anderson, Moore, 2023]. Традиционные модели бюджетирования ИБ часто опираются на принцип «сколько осталось в бюджете» или на реакцию на произошедшие инциденты, что ведет либо к дефициту средств на критические меры, либо к избыточному финансированию неактуальных направлений (over-protection).

Проблема исследования заключается в отсутствии единого алгоритма, который связывал бы техническое состояние безопасности (диагностируемое моделями) с экономическими решениями (инвестициями) в зависимости от этапа цифровой зрелости компании.

Цель статьи – разработать организационно-экономический механизм управления уровнем безопасности, позволяющий оптимизировать инвестиционные вложения и максимизировать отдачу от защитных мер.

Научная новизна состоит в следующем:

Предложена структура организационно-экономического механизма, включающая три функциональных блока, адаптированных под уровни цифровой трансформации.

Разработан алгоритм поддержки управленческих решений, переводящий интегральный индекс безопасности в конкретные инвестиционные сценарии.

Обоснована методика расчета ROI (возврата на инвестиции) для превентивных мер защиты в экосистемных бизнес-моделях [Gordon, Loeb, 2022].

Практическая значимость работы заключается в предоставлении руководству финансовых организаций инструмента для расчета оптимального бюджета на ИБ и приоритизации проектов по их вкладу в снижение совокупной стоимости владения рисками [Жукова, 2023].

Материалы и методы исследования

Разработанный механизм представляет собой динамическую систему, функционирующую по принципу непрерывного цикла (feedback loop) [Brown, Davis, 2023]. В отличие от статичных регламентов, механизм адаптируется к изменениям внешней среды и внутренней цифровой зрелости организации.

Механизм базируется на трех взаимосвязанных блоках:

Организационный блок обеспечивает регламентацию процессов и управление человеческим капиталом.

Ключевые элементы: ролевая модель управления (CISO, комитеты по безопасности), политики ИБ, программы повышения цифровой грамотности.

Специфика для ЦТ: на этапах 0–1 фокус на базовых инструкциях и дисциплине. На этапах 3–4 фокус смещается на культуру безопасности (Security Culture) и управление изменениями, так как технологии внедряются быстрее, чем пишутся регламенты.

Инструментальный блок включает технические средства и технологии защиты.

Ключевые элементы: периметровая защита, SIEM/SOC, системы поведенческой аналитики (UEBA), криптография [NIST Cybersecurity Framework, 2024].

Специфика для ЦТ: переход от реактивных инструментов (антивирусы) к проактивным (AI-based анализ угроз, Zero Trust архитектура) по мере роста уровня цифровой трансформации [ГОСТ Р 57580.1-2021, 2021].

Экономический блок (ядро механизма) обеспечивает связь между безопасностью и финансовыми результатами бизнеса.

Ключевые элементы: расчет совокупной стоимости владения (TCO Security), монетизация рисков, оценка ROI защитных мер.

Задача: доказать, что инвестиции в ИБ – это не статья расходов (Cost Center), а драйвер сохранения стоимости (Value Preserver).

Механизм реализуется через формализованный алгоритм, позволяющий трансформировать данные мониторинга в управленческие команды.

Шаг 1. Диагностика. Оценка текущего значения интегрального индекса безопасности (I_{sec}) с использованием математической модели [Цибулина, 2026].

Шаг 2. Целеполагание. Определение целевого значения I_{sec}^{target} в зависимости от стратегии развития. Например, если компания планирует запускать открытые API-интерфейсы (переход на уровень 3), целевой индекс должен быть не ниже 0,75.

Шаг 3. Анализ разрыва (Gap Analysis). Расчет разрыва $\Delta = I_{sec}^{target} - I_{sec}^{current}$.

Если $\Delta > 0$, иницируется процесс инвестирования.

Если $\Delta \leq 0$, ресурсы перенаправляются на мониторинг и поддержку.

Шаг 4. Выбор рычагов (сценарный анализ). На основе матрицы рисков выбираются наиболее эффективные меры для закрытия разрыва. Приоритизация мер осуществляется по критерию Cost-Benefit Ratio:

$$CBR = (\Delta Risk \times Value_{asset}) / Cost_{measure}$$

где $\Delta Risk$ – снижение вероятности инцидента, $Value_{asset}$ – стоимость защищаемого актива, $Cost_{measure}$ – затраты на внедрение меры.

Шаг 5. Внедрение и мониторинг. Реализация мер и пересчет индекса I_{sec} через заданный период (квартал/год).

Ключевым показателем эффективности механизма является ROI информационной безопасности, рассчитываемый как отношение предотвращенного ущерба к затратам на реализацию механизма:

$$ROI_{sec} = ((L_{expected} - L_{residual}) \times P_{incident} - Cost_{measures}) / Cost_{measures} \times 100\%$$

где:

$L_{expected}$ – ожидаемые потери в случае реализации инцидента (включая прямые убытки, штрафы и репутационный ущерб).

$L_{residual}$ – остаточный ущерб после применения защитных мер.

$P_{incident}$ – вероятность наступления инцидента без защитных мер.

$Cost_{measures}$ – совокупные затраты на внедрение организационно-экономического механизма.

Результаты и обсуждение

Для проверки работоспособности механизма проведен расчет на базе открытых данных ПАО Сбербанк за 2023–2024 гг. [Годовой отчет ПАО Сбербанк за 2023 год, 2024] Организация идентифицирована как находящаяся на Уровне 4 (Экосистема) [Отчет об устойчивом развитии Группы Сбер за 2023 год, 2024].

Исходные данные:

Текущий индекс безопасности (по модели): $I_{sec}^{current} = 0,625$.

Целевой индекс для экосистемы: $I_{sec}^{target} = 0,800$.

Разрыв: $\Delta = 0,175$.

На основе анализа структуры разрыва были выбраны три приоритетные меры (Таблица 1).

Таблица 1 - План корректирующих мер и экономический эффект

Направление разрыва	Предлагаемая мера (Механизм)	Затраты (Cost_measures), млрд руб.	Ожидаемое снижение потерь (L_expected – L_residual), млрд руб.	Влияние на I_sec
Человеческий фактор	Масштабная программа обучения и геймификации («Цифровая гигиена 2.0»)	0,2	1,5 (снижение фишинга)	+0,05
Внутренние угрозы	Внедрение поведенческой аналитики (UEBA)	0,5	2,5 (предотвращение инсайда)	+0,04
Устойчивость	Резервирование критических микросервисов	1,2	2,5 (избежание простоя экосистемы)	+0,03
ИТОГО	Комплексное применение механизма	1,9	6,5	+0,12

Расчет эффективности. Подставив значения в формулу (1):

$ROI_{sec} = (6,5 - 1,9) / 1,9 \times 100\% \approx 242\%$

Анализ результатов. Применение организационно-экономического механизма позволило не только выявить критический разрыв в уровне безопасности, но и сформировать обоснованный инвестиционный портфель. Показатель ROI 242% свидетельствует о высокой экономической целесообразности превентивных мер. Без применения механизма (при стихийном реагировании на угрозы) затраты на ликвидацию инцидентов могли бы превысить инвестиции в защиту в 3–4 раза.

Разработанный механизм решает задачу балансировки между амбициями цифровой трансформации и допустимым уровнем риска.

Ключевые преимущества подхода:

Дифференциация затрат: механизм не требует одинаковых инвестиций на всех этапах. Для уровня 0 (Автоматизация) он рекомендует минимальные базовые меры, экономя ресурсы. Для уровня 4 (Экосистема) он обосновывает высокие затраты на устойчивость.

Интеграция с бизнесом: перевод рисков на язык финансов (формула ROI) позволяет говорить с советом директоров на одном языке.

Адаптивность: алгоритм предусматривает регулярный пересчет, что критически важно в условиях «бесконечной» трансформации [Regulation (EU) 2022/2554 (DORA), 2022].

Ограничения: точность расчета ROI зависит от качества оценки вероятности инцидентов ($P_{incident}$), которая часто базируется на исторических данных, не всегда отражающих новые векторы атак (например, с использованием генеративного ИИ) [World Economic Forum, 2024].

Заключение

Организационно-экономический механизм управления уровнем безопасности представляет собой завершённый инструмент, позволяющий финансовым организациям перейти от реактивной защиты к превентивному управлению рисками. Апробация на примере ПАО Сбербанк подтвердила, что инвестиции в оптимизацию уровня безопасности экономически оправданы и способны генерировать значительный предотвращённый ущерб при высоком показателе ROI. Дальнейшие исследования могут быть направлены на автоматизацию сбора данных для расчёта индекса I_{sec} в реальном времени с использованием технологий Big Data.

Библиография

1. Годовой отчет ПАО Сбербанк за 2023 год. М., 2024.
2. ГОСТ Р 57580.1-2021. Обеспечение информационной безопасности организаций банковской сферы. 2021.
3. Жукова Т.В. Экономическая оценка эффективности инвестиций в кибербезопасность // Экономический анализ. 2023. № 3. С. 445–461.
4. Отчет об устойчивом развитии Группы Сбер за 2023 год. М., 2024.
5. Попов Д.В., Ральникова К.В. Оценка уровня цифровой трансформации организации // Цифровая экономика. 2023. № 3. С. 65–75.
6. Цибулина Е.В. Математическое моделирование зависимости уровня безопасности организации от этапа цифровой трансформации // 2026. В печати.
7. Anderson R., Moore T. The economics of cybersecurity // International Journal of Critical Infrastructure Protection. 2023. Vol. 40. P. 1–15.
8. Brown M., Davis K. Integrating security-by-design into digital transformation strategies // Journal of Cybersecurity. 2023. Vol. 9. P. 1–18.
9. Gordon L.A., Loeb M.P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. 2022. Vol. 25. P. 1–34.
10. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024.
11. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). 2022.
12. World Economic Forum. The Global Risks Report 2024. Geneva: WEF, 2024.

Organizational and Economic Mechanism for Managing the Level of Security: Decision-Making Algorithm and Investment Optimization

Ekaterina V. Tsibulina

Postgraduate Student,
Moscow State Technological University "STANKIN",
127055, 1, Vadkovskiy lane, Moscow, Russian Federation;
e-mail: katsibulina@gmail.com

Abstract

The article examines the problem of economic inefficiency of investments in information security (IS) in the context of digital transformation. It is shown that traditional approaches to IS budgeting are often reactive in nature and do not take into account the dependence of the cost of protection on the level of digital maturity of the organization, which leads both to a shortage of funds for critical measures and to excessive financing of irrelevant areas. An organizational and economic mechanism for managing the level of security has been developed, combining organizational,

instrumental, and economic blocks and adapted to the levels of digital transformation. A management decision-making algorithm is proposed that translates the integral security index into specific investment scenarios through diagnostics, goal setting, gap analysis, selection of corrective measures, and subsequent monitoring. The methodology for calculating return on investment (ROI) for preventive protection measures in ecosystem business models is substantiated. Using the example of a financial organization (PJSC Sberbank), the economic efficiency of the mechanism was assessed. Calculations showed that the application of the algorithm allows increasing the level of security from 0.625 to 0.800 while optimizing costs, ensuring a calculated ROI of protective measures at the level of 242%. The results of the study can be used by managers and risk managers to justify IS budgets and balance the risks of digitalization.

For citation

Tsibulina E.V. (2026) Organizatsionno-ekonomicheskiiy mekhanizm upravleniya urovnem bezopasnosti: algoritm prinyatiya resheniy i optimizatsiya investitsiy [Organizational and Economic Mechanism for Managing the Level of Security: Decision-Making Algorithm and Investment Optimization]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (6A), pp. 1056-1061. DOI: 10.34670/AR.2026.26.31.098

Keywords

Organizational and economic mechanism, security level management, digital transformation, investment attractiveness, security ROI, risk-oriented approach, decision-making algorithm, research methodology, economic efficiency.

References

1. Anderson, R., & Moore, T. (2023). The economics of cybersecurity. *International Journal of Critical Infrastructure Protection*, 40, 1–15.
2. Brown, M., & Davis, K. (2023). Integrating security-by-design into digital transformation strategies. *Journal of Cybersecurity*, 9, 1–18.
3. Gordon, L. A., & Loeb, M. P. (2022). The economics of information security investment. *ACM Transactions on Information and System Security*, 25, 1–34.
4. GOST R 57580.1-2021. (2021). Obespecheniye informatsionnoy bezopasnosti organizatsiy bankovskoy sfery [Information security of banking sector organizations].
5. NIST Cybersecurity Framework (CSF) 2.0. (2024). National Institute of Standards and Technology.
6. Popov, D. V., & Ralnikova, K. V. (2023). Otsenka urovnya tsifrovoy transformatsii organizatsii [Assessment of the level of digital transformation of an organization]. *Tsifrovaya ekonomika* [Digital Economy], *3*, 65–75.
7. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). (2022).
8. Sberbank PJSC. (2024). Godovoy otchet PAO Sberbank za 2023 god [Sberbank PJSC Annual Report for 2023]. Moscow.
9. Sber Group. (2024). Otchet ob ustoychivom razvitii Gruppy Sber za 2023 god [Sber Group Sustainability Report for 2023]. Moscow.
10. Tsibulina, E. V. (2026). Matematicheskoye modelirovaniye zavisimosti urovnya bezopasnosti organizatsii ot etapa tsifrovoy transformatsii [Mathematical modeling of the dependence of an organization's security level on the stage of digital transformation]. (In press).
11. World Economic Forum. (2024). The Global Risks Report 2024. WEF.
12. Zhukova, T. V. (2023). Ekonomicheskaya otsenka effektivnosti investitsiy v kiberbezopasnost' [Economic assessment of the effectiveness of investments in cybersecurity]. *Ekonomicheskiiy analiz* [Economic Analysis], *3*, 445–461.