

Научная статья

DOI 10.66424/2071-8217-2026-3-11

УДК 338.2:004.056.5

ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ТРЕХУРОВНЕВОГО КАРКАСА БЮДЖЕТИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИЙ МАЛОГО И СРЕДНЕГО БИЗНЕСА

И. В. Мандрица^{1,2*}, В. И. Петренко¹, О. В. Мандрица²

¹Северо-Кавказский федеральный университет, Ставрополь, Россия

²МИРЕА – Российский технологический университет (филиал в Ставрополе), Ставрополь, Россия

✉ *d_artman@mail.ru

ДЛЯ ЦИТИРОВАНИЯ

Мандрица И. В., Петренко В. И., Мандрица О. В. Теоретическое обоснование трехуровневого каркаса бюджетирования информационной безопасности для организаций малого и среднего бизнеса // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 145–161. DOI: 10.66424/2071-8217-2026-3-11

ПОСТУПИЛА 07.05.2026

ПРИНЯТА 24.07.2026

ОПУБЛИКОВАНА 13.10.2026

© Мандрица И. В., Петренко В. И., Мандрица О. В.

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Разработана теоретическая трехуровневая концепция бюджетирования информационной безопасности для малых и средних предприятий, объединяющая: ранее проверенную 16-факторную таксономию угроз, основанную на индексе токсичности TDI и методе Фишера – Дженкса; трехмерное пространство угроз с осями «токсичность × бюджетная нагрузка × частота атак»; кластерно-зависимые функции свертки – ожидаемый годовой убыток (EAL) для массовых угроз (Opportunist), условная стоимость под риском (CVaR) для катастрофических угроз (Apex Predator) и функция бюджетного прогнозирования В_AI для возникающего класса угроз, связанных с искусственным интеллектом. Доказана теорема вертикальной совместимости: результаты уровня I являются частным случаем функций уровня III при вырожденных параметрах. Метод Дельфи применяется исключительно для калибровки весов в рамках метода аналитической иерархии. Эмпирическая проверка основана на данных по 94 малым и средним предприятиям Южного федерального округа, 347 инцидентах за 2022–2025 гг.

КЛЮЧЕВЫЕ СЛОВА

Бюджетирование информационной безопасности, кластеризация киберугроз, ожидаемые годовые потери, условная стоимость под риском, теория экстремальных значений, малый и средний бизнес, метод аналитической иерархии

Original article

DOI 10.66424/2071-8217-2026-3-11

THEORETICAL FRAMEWORK FOR THREE-LEVEL INFORMATION SECURITY BUDGETING IN SMALL AND MEDIUM-SIZED ENTERPRISES

I. V. Mandritsa^{1,2*}, V. I. Petrenko¹, O. V. Mandritsa²

¹North-Caucasus Federal University, Stavropol, Russia

²MIREA – Russian Technological University (Stavropol branch), Stavropol, Russia

✉ *d_artman@mail.ru

FOR CITATION

Mandritsa I. V., Petrenko V. I.,
Mandritsa O. V. Theoretical framework
for three-level information security
budgeting in small and medium-sized
enterprises. *Problems of information
security. Computer systems*.
2026. No. 3, pp. 145–161.
DOI: 10.66424/2071-8217-2026-3-11
(In Russian)

RECEIVED 07.05.2026

ACCEPTED 24.07.2026

PUBLICATION 13.10.2026

ABSTRACT

This paper develops a theoretical three-level information security budgeting framework for small and medium-sized enterprises, integrating: a previously validated 16-factor threat taxonomy based on the Toxicity Index TDI and the Fisher – Jenks method; a three-dimensional threat space with axes “toxicity × budget load × attack frequency”; cluster-dependent convolution functions – Expected Annual Loss (EAL) for mass threats (Opportunist), Conditional Value-at-Risk (CVaR) for catastrophic threats (Apex Predator), and the budgetary anticipation function B_{AI} for the emerging class of AI-threats. The vertical compatibility theorem is proven: level I results are a special case of level III functions under degenerate parameters. The Delphi method is applied exclusively for AHP weight calibration. Empirical validation is based on 94 small and medium-sized enterprises of the Southern Federal District, 347 incidents, 2022–2025.

KEYWORDS

Information security budgeting, clustering of cyber threats, expected annual losses, notional value at risk, theory of extreme values, small and medium-sized businesses, analytical hierarchy method

1. ВВЕДЕНИЕ И ПОСТАНОВКА ПРОБЛЕМЫ

Проблема формирования экономически обоснованного бюджета информационной безопасности для предприятий малого и среднего бизнеса (МСП) не получила законченного теоретического решения ни в классических работах Гордона и Леба [1], ни в их расширениях [2, 3]. Теоретико-игровая линия этих расширений, представленная работой Фильдера с соавторами [3], сопоставляется с предлагаемым каркасом. Модель Гордона – Леба корректно описывает убывающую предельную эффективность защитных вложений, однако предполагает стационарный ландшафт угроз и единственную функцию ущерба – допущения, принципиально нарушаемые в условиях нестационарного киберпространства 2022–2026 гг. [4, 5].

Региональная асимметрия ландшафта киберугроз [6] делает невозможным прямой перенос западных моделей бюджетирования информационной безопасности (ИБ) на российский МСБ без адаптации к локальной таксономии угроз и нормативной базе ФСТЭК. Банк данных угроз (БДУ)

ФСТЭК России содержит 227 формализованных угроз [7], при этом распределение связанного с ними ущерба статистически неоднородно: большинство инцидентов относится к классу Opportunist с субэкспоненциальным распределением потерь, тогда как редкие атаки класса Apex Predator формируют тяжелохвостое распределение [8].

Именно различие статистических режимов ущерба и механизмов бюджетного реагирования делает применение единой линейной свертки ко всему множеству угроз методологически уязвимым: использование одной функции приоритета для всего пространства угроз приводит к потере различий между массовыми и катастрофическими сценариями.

Позиционирование среди современных подходов. Помимо линии Гордона – Леба, экономика ИБ располагает методологией FAIR [9], оценивающей риск отдельного сценария методом Монте-Карло, и теоретико-игровыми моделями «атакующий – защитник» [3, 10]. Ни один из этих подходов не отвечает на вопрос, поставленный в работе: какой совокупный бюджет достаточен для МСП при

Таблица 1 | Сравнительный анализ подходов к экономическому обоснованию бюджета ИБ**Table 1** | Comparative analysis of approaches to the economic justification of the information security budget

Критерий	Гордон – Леб [1–3]	FAIR [9]	Теория игр [3, 10]	ISO 27005 / NIST [11, 12]	Предлагаемый каркас
Критерий достаточности бюджета	Верхняя граница 1/eEAL, без структуры угроз	Нет; оценка риска сценария	Неявный (равновесие)	Нет; процессные требования	Явный, по кластерам (EAL, CVaR, B_AI)
Неоднородность угроз	Единая функция ущерба	Посценарно, без кластеров	Зависит от матрицы игры	Качественные категории	Три статистических режима (EVT)
Требования к данным	Функция уязвимости (ненаблюдаема)	Распределения потерь по сценариям	Функция выигрыша атакующего	Реестры активов и контролей	БДУ ФСТЭК + открытая статистика
Применимость к МСП	Ограничена	Ограничена	Низкая	Высокая, без денежного выхода	Высокая: 94 МСП, 347 инцидентов
Нестационарность ландшафта	Не учитывается	Не учитывается	Повторяющиеся игры (теоретически)	Периодический пересмотр	Функция упреждения B_AI по дрейфу NTI

статистически неоднородном и дрейфующем ландшафте угроз. В табл. 1 пять подходов сопоставлены по критериям, существенным для этой задачи.

Из табл. 1 видно, что явный денежный критерий достаточности, различие статистических режимов ущерба и реакцию на дрейф ландшафта не совмещает ни один из сопоставленных подходов – предлагаемый каркас закрывает именно эту комбинацию, не конкурируя с FAIR и теорией игр на их поле посценарного и стратегического анализа.

В опубликованных работах авторов [13, 14] разработана 16-факторная модель ранжирования угроз на основе индекса токсичности *TDI* и *F*-критерия Фишера, эмпирически верифицированная на данных 94 МСП ЮФО. Исследование решает задачу теоретического обоснования вертикальной совместимости этой модели с новым трехуровневым каркасом бюджетирования, показывая, что 16-факторная таксономия образует базовый уровень, на котором становится возможным построение кластерно-зависимых функций свертки без логического разрыва между уровнями модели.

2. МАТЕРИАЛЫ И МЕТОДЫ

Источники данных. Эмпирическую базу составляют три независимых источника:

1. Банк данных угроз ФСТЭК России по состоянию на 01.01.2026: 227 угроз с формализованными параметрами *C*, *I*, *A*, *P*, *V*, *S* [7].

Эпидемиологический характер распространения сетевых атак [15] объясняет наблюдаемую асимметрию частот: массовые угрозы класса *Opportunist* распространяются по экспоненциальному закону, тогда как редкие АРТ-сценарии класса *Apex Predator* не подчиняются эпидемиологической динамике.

2. Анонимизированная выборка инцидентов ИБ 94 малых и средних предприятий Южного федерального округа за 2022–2025 гг. (347 верифицированных инцидентов с документально подтвержденным ущербом).

3. Аналитические отчеты: Verizon DBIR 2025 [4], ENISA Threat Landscape 2025 [5], Positive Technologies [16], BI.ZONE [17].

Триада «конфиденциальность – целостность – доступность» (CIA) соответствует

базовой модели контроля безопасности по NIST SP 800-53R5 [11], что обеспечивает совместимость с международными системами оценки рисков.

Методологическая архитектура. Исследование использует иерархическую методологию, объединяющую: кластерный анализ методом Фишера – Дженкса [18] для разбиения пространства угроз на однородные классы; теорию экстремальных значений (EVT) [7] для идентификации типа хвоста распределения ущерба в каждом кластере; метод аналитической иерархии (АНР) Саати [19] для калибровки весовых коэффициентов; метод Дельфи [20] исключительно на этапе весовой калибровки АНР. Однородность распределений проверялась критерием Колмогорова – Смирнова [21]; оценка параметра хвоста выполнялась оценкой Хилла [22].

Современная теория количественного управления рисками [23] подтверждает, что для тяжелохвостых распределений ущерба от киберинцидентов классические моменты распределений недостаточны и требуется аппарат теории экстремальных значений.

3. ТЕОРЕТИЧЕСКИЕ РЕЗУЛЬТАТЫ

Уровень I: 16-факторная модель как аксиоматический фундамент. Разработанный индекс токсичности угрозы *TDI* [13] задает интегральную оценку разрушительного потенциала киберугрозы, выраженную через мультипликативную комбинацию ее формализованных признаков и опирающуюся на параметры БДУ ФСТЭК [7]:

$$TDI = (C + I + A)PV(1 + S), \quad (1)$$

где $C, I, A \in \{0; 1\}$ – бинарные индикаторы нарушения конфиденциальности, целостности и доступности соответственно; $P \in \{1; 2; 3\}$ – потенциал нарушителя (низкий, средний, высокий); $V \in \{1; 2; 2,5; 3\}$ – вектор реализации угрозы (физический, локальный, смешанный, сетевой); $S \in \{0; 1\}$ – сложность объекта воздействия.

Статус индекса зафиксироваем сразу: *TDI* – порядковая скоринговая функция, предназначенная для ранжирования и классификации угроз. Ни вероятность совместной реализации признаков, ни денежная величина ущерба этим индексом не измеряются – денежная оценка выполняется на уровне III, куда результат уровня I входит через принадлежность кластеру.

Множитель 2 при сумме индикаторов, присутствовавший в прежней редакции формулы (1), исключен: любой общий положительный коэффициент сокращается при нормализации, поэтому значения TDI_{norm} , ранжирование 227 угроз и границы кластеров от него не зависят – численная проверка с коэффициентами 2 и 1,5 дает нулевое расхождение нормализованных значений и ранговую корреляцию 1,000. Равенство весов C, I и A отражает принцип недостаточного основания: уровень I оценивает угрозу безотносительно конкретной организации, а дифференциация последствий вынесена в индикатор BRI и в калибровку АНР.

Мультипликативная свертка не требует статистической независимости признаков: *TDI* – детерминированная функция нормативных атрибутов БДУ, а не вероятностная модель. Ранговая корреляция Спирмена между потенциалом P и вектором V по совокупности 227 угроз равна $\rho = -0,08$ ($p = 0,25$), т.е. связь отсутствует; исключение V меняет класс у 31 % угроз, подтверждая информационную избыточность этого признака. Единственная значимая ассоциация между индикаторами целостности и доступности ($\rho = 0,34$; $p < 0,001$) устойчивости разбиения не угрожает: при 2000 случайных наборах весов $wC, wI, wA \in [0,6; 1,5]$ ранговая согласованность с равновесной версией индекса не опускается ниже 0,91 (медиана 0,99), а кластер меняют в медиане 1,3 % угроз (максимум 9,7 %). Произведение порядковых подшкал – устоявшийся прием инженерии оценивания угроз: базовая метрика CVSS определяется произведением подшкал воздействия и эксплуатируемости, заданных на разных носителях [24].

Нормализация TDI к шкале $[0; 100]$ осуществляется методом min-max [13]:

$$TDI_{norm} = 100 \cdot \frac{TDI - TDI_{min}}{TDI_{max} - TDI_{min}}, \quad (2)$$

где TDI_{min} , TDI_{max} – минимальное и максимальное значения индекса по совокупности 227 угроз БДУ ФСТЭК.

Кластеризация нормализованных значений методом Фишера – Дженкса [18] с числом кластеров $k=3$, обоснованным минимумом внутригрупповой дисперсии (критерий «локтя»), позволила выделить три устойчивых класса угроз.

Процедура классификации двухэтапна, поскольку метод Фишера – Дженкса одномерен. Первый шаг отделяет по TDI_{norm} массовый низкотоксичный класс Opportunist; второй разделяет высокотоксичную группу по признаку стационарности – частоте f и скорости роста адаптивного индекса NTI: у Apex Predator частота стабильно низкая и дрейф NTI отсутствует, у Emerging AI частота средняя и NTI монотонно растет. Отнесение угрозы i к классу Emerging AI задает решающее правило:

$$I_{AI}(i) = \mathbb{1}[TDI_{norm,i} \geq \tau] \mathbb{1}\left[\frac{\Delta NTI_i}{\Delta t} \geq \delta^*\right], \quad (3)$$

где $\mathbb{1}[\cdot]$ – индикаторная функция выполнения условия; τ – нижняя граница высокотоксичной группы по разбиению Фишера – Дженкса (по данным табл. 2 $\tau=55$); $\Delta NTI_i/\Delta t$ – эмпирическая скорость роста адаптивного индекса угрозы i , 1/год; δ^* – калибруемый порог скорости дрейфа, 1/год; при $\Delta NTI_i/\Delta t < \delta^*$ высокотоксичная угроза относится к классу Apex Predator.

Пересечение одномерных диапазонов TDI кластеров Apex Predator и Emerging AI – свойство проекции многомерного разбиения на одну ось, а не дефект классификации: дискриминирующей координатой для этой пары служит динамика, а не токсичность. Правило (3) делает разбиение воспроизводимым; принадлежность конкретной угрозы классу опровержима наблюдением ее частотной динамики.

Иерархическая архитектура трехуровневого каркаса опирается на принцип

Г. Саймона о преемственности уровней сложности [25], согласно которому сложные адаптивные системы естественно разлагаются на квазинезависимые подсистемы.

В табл. 2 представлены сводные количественные характеристики трех кластеров угроз, полученные по результатам кластерного анализа 227 угроз БДУ ФСТЭК методом Фишера – Дженкса, включая параметры функций свертки, эмпирические оценки бюджетных долей и метрики согласованности экспертных суждений CR по методу АНР [19]. Метод Фишера – Дженкса относится к классу одномерных алгоритмов оптимальной кластеризации [26], минимизирующих внутриклассовую дисперсию.

Таблица 2 демонстрирует качественно различные статистические режимы ущерба по каждому кластеру, что служит аргументом в пользу дифференцированных функций свертки вместо единой линейной агрегации.

На рис. 1 представлена геометрия трех кластеров в пространстве « $TDI \times$ частота атак». Кластеры статистически разделены (F -критерий Фишера: $F=47,3$, $p<0,001$), что подтверждает эмпирическую неоднородность пространства угроз и служит аргументом в пользу использования различных функций свертки для разных кластеров.

Дополнительная проверка качества разбиения по индексу Калинского – Хараша [27] дает значение $CH=312,7$, что превосходит пороговые значения для трех альтернативных гипотез о числе кластеров ($k=2; 4; 5$).

Рисунок 1 подтверждает: три кластера занимают непересекающиеся области пространства ($TDI \times$ частота), что эмпирически обосновывает невозможность применения единой линейной свертки.

Теория иерархических многоуровневых систем [28] допускает применение разных функций свертки на каждом уровне, что согласуется с обнаруженными в табл. 2 качественно различными статистическими режимами кластеров угроз.

Таблица 2 | Сводные характеристики трех кластеров угроз БДУ ФСТЭК: параметры пространства угроз, функции свертки и бюджетные оценки ($n = 94$ МСП ЮФО, 347 инцидентов, 2022–2025 гг.)

Table 2 | Summary characteristics of the three BDU FSTEC threat clusters: threat space parameters, convolution functions and budget estimates ($n = 94$ SMEs SFD, 347 incidents, 2022–2025)

Кластер угроз	n угроз (БДУ ФСТЭК)	TDI_{norm} , ед.	f – частота, ед.	κ_{obs} , ед.	Закон ущерба	Функция свертки	Доля в бюджете ИБ, %	$EAL/CVaR$, тыс. руб./год	Параметры АНР/Дельфи
Opportunistic (массовые)	120	12–55	0,40–0,99	0,85–1,00	Субэкспоненциальный	$EAL = f TDI A w_1$	55–70	$EAL \approx 840$ (медиана)	$w_1 \in [0,55; 0,70]$ $CR = 0,07$
Apex Predator (катастрофические)	55	56–85	0,01–0,18	0,60–0,80	Тяжелый хвост (Парето $\xi = 2,2$)	$CVaR_{0,95} = VaR \xi / (\xi - 1)$	25–35	$CVaR \approx 8400$ (p95-хвост)	$\alpha = 0,95$ $CR = 0,08$
Emerging AI (формирующиеся)	52	55–80	0,15–0,65	0,40–0,70	Смешанный (нестационарный)	$B_{AI} = \beta_0 \exp(\beta_1 NTD) CVaR$	5–20	$B_{AI} \approx 1260$ (прогноз 2026)	$\beta_0 = 2,5$; $\beta_1 = 2,8$
Итого (вся выборка)	227	—	—	—	$F = 47,3$ $p < 0,001$	Кусочная функция (три кластера)	100	$EAL_{cov} \approx 180$ млрд руб. (МСП ЮФО)	$CR < 0,10$ (АНР-матрица)

Примечания: n – число угроз в кластере по БДУ ФСТЭК [6]; TDI_{norm} – нормализованный индекс токсичности (2); f – скорректированная частота; κ_{obs} – коэффициент наблюдаемости, оценен методом Дельфи [14]; CR – коэффициент согласованности матрицы АНР [13] (критерий $CR < 0,10$); $EAL/CVaR/B_{AI}$ – расчетные значения по выборке МСП ЮФО. Диапазоны TDI_{norm} кластеров Apex Predator и Emerging AI пересекаются как одномерные проекции разбиения, выполненного по трем признакам.

Уровень II: трехмерное пространство угроз. Каждая угроза i отображается в трехмерное пространство R^3 с координатами $(TDI_{norm,i}, BRI_i, f_i)$. Три оси описывают различные исследуемые характеристики угрозы и потому не могут интерпретироваться как взаимозаменяемые показатели одного порядка.

Ось X фиксирует внутреннюю деструктивность угрозы и определяется по формулам (1)–(2) на основе данных БДУ ФСТЭК.

Ось Y отражает потенциальную бюджетную напряженность угрозы для организации и задается расширением TDI до индикатора бюджетного риска BRI [8]:

$$BRI_i = TDI_{norm,i} w_s (1 + \beta EF_i) A_i, \quad (4)$$

где $w_s \in [0,70; 1,40]$ – отраслевой весовой коэффициент; $\beta \in [0; 1]$ – коэффициент

усиления; $EF_i \in [0; 1]$ – экспозиционный фактор; A_i – стоимость (информационного) актива, руб.

Ось Z отражает эмпирическую интенсивность актуализации угрозы в наблюдаемой среде и формируется по данным репрезентативных отчетов с поправкой на систематическую ошибку наблюдаемости [4, 5, 10, 11]:

$$f_i = \lambda_i \kappa_{obs} \quad (5)$$

где λ_i – наблюдаемая частота реализации угрозы i по данным открытых аналитических отчетов [4, 5]; $\kappa_{obs} \in (0; 1]$ – коэффициент наблюдаемости, учитывающий систематическое занижение статистики для скрытых угроз.

Значения κ_{obs} оцениваются методом Дельфи [20] как структурированная

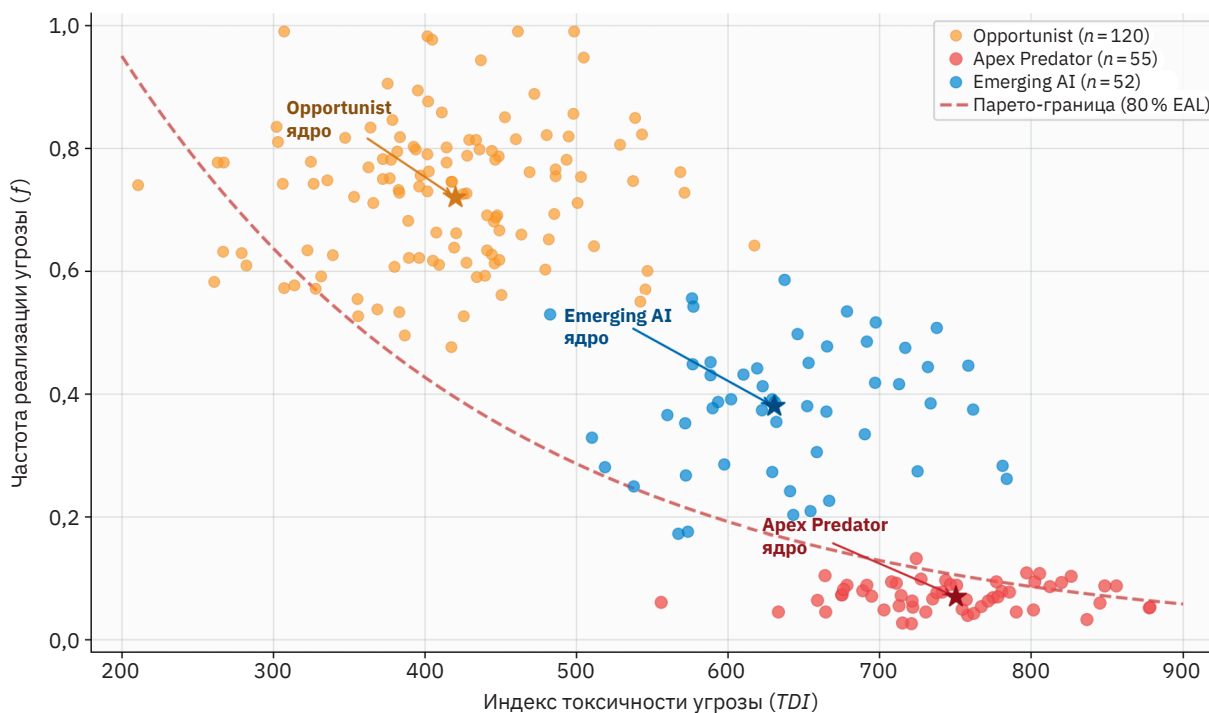


Рис. 1 Кластеризация 227 угроз БДУ ФСТЭК методом Фишера – Дженкса в пространстве « $TDI \times$ частота реализации»¹

Звездочки – центры кластеров; пунктирная линия – Парето-граница (80 % совокупного EAL)

Fig. 1 Clustering of 227 threats from the FSTEC BDU using the Fisher – Jenks method in the “ $TDI \times$ implementation frequency” space

Stars represent cluster centroids; the dashed line represents the Pareto boundary (80 % of the total EAL)

¹ Рассчитано авторами по данным БДУ ФСТЭК [6] и выборки МСП ЮФО.

экспертная оценка ошибки наблюдения. Три оси вместе дают то, чего не дает ни одна из них по отдельности: угроза характеризуется не рангом, а положением в пространстве – и это положение непосредственно транслируется в бюджетное решение.

Концепция сбалансированной системы показателей [29] требует, чтобы управленческое решение опиралось не на единственный агрегированный индикатор, а на согласованную тройку метрик; в предложенной модели роль такой тройки играют TDI , BRI , f .

На рис. 2 показаны проекции трехмерного кластерного пространства, построенного по данным 227 угроз БДУ ФСТЭК и выборки 94 МСП ЮФО. Рисунок 2 позволяет сформулировать три структурных вывода: полярное разделение кластеров Opportunist и Apex Predator во всех ракурсах; переходное положение Emerging AI между обоими полюсами; инвариантность Парето-ядра относительно угла наблюдения.

На рисунке представлен метод четырех ортогональных ракурсов – некий аналог инженерного трехпроекционного чертежа, дополненного четвертым диагональным видом. Он позволяет реконструировать пространственную структуру, которая не считывается из одной визуализации. Метрика Value-at-Risk (VaR) [30], исторически развитая в банковском риск-менеджменте, на уровне II применяется как промежуточная оценка перед переходом к более строгой когерентной мере CVaR.

Ракурс А (ось $TDI \times BRI$) обнажает фундаментальный структурный разрыв: угрозы класса Opportunist концентрируются в левом нижнем квадранте, тогда как угрозы класса Apex Predator занимают правый верхний сектор – при том, что их абсолютная частота в десятки раз ниже.

Этот разрыв составляет содержательное основание для отказа от единой линейной свертки: в линейном случае высокочастотные Opportunist-угрозы систематически вытесняли бы из бюджета редкие, но катастрофические Apex Predator-угрозы.

Ракурс Б (ось частота $\times TDI$) раскрывает динамику дрейфа: вектор смещения Парето-ядра 2023→2025 направлен в сто-

рону увеличения как TDI , так и частоты атак.

Кластер Emerging AI располагается в центральной зоне, что отражает его переходную природу: $NTI(t) = 0,41$ в 2025 г. против 0,18 в 2023 г. – устойчивое смещение в направлении Apex Predator при сохранении текущей траектории.

Уровень III: кластерно-зависимые функции свертки. Единая функция приоритета, наложенная на статистически неоднородное пространство угроз, искажает бюджетную логику – Opportunist-угрозы вытесняют из расчета Apex Predator-угрозы не потому, что важнее, а потому что частотнее. Выход – три отдельные функции свертки, каждая калиброванная под статистический режим своего кластера.

Выбор CVaR обоснован тем, что эта мера принадлежит классу когерентных риск-мер [31], удовлетворяющих аксиомам монотонности, субаддитивности, положительной однородности и трансляционной инвариантности; VaR этим аксиомам не удовлетворяет.

Функция EAL для кластера Opportunist. Для угроз с субэкспоненциальным распределением ущерба математическое ожидание потерь конечно, и ожидаемые годовые потери EAL являются корректной мерой риска в духе модели Гордона – Леба [1]:

$$EAL_i = f_i TDI_{norm,i} A_i w_1, \quad (6)$$

где f_i – скорректированная частота реализации угрозы i по формуле (5); $TDI_{norm,i}$ – нормализованный индекс токсичности по формуле (2); A_i – стоимость информационного актива, руб.; $w_1 \in (0; 1]$ – весовой коэффициент, оцениваемый методом АНР [19] с калибровкой через Дельфи [20].

При $w_1 = 1$ и $f_i = \text{const}$ формула (6) сводится к ранжированию по TDI , что показывает согласованность с базовой 16-факторной моделью уровня I.

Функция CVaR для кластера Apex Predator. Для угроз с тяжелым хвостом распределения ущерба применение EAL приводит к систематическому занижению бюджетных потребностей: при параметре хвоста $\xi < 2$ дисперсия ущерба бесконечна, и оценка Хилла [22] выступает стандартным инструментом оценки ξ по данным выборки.

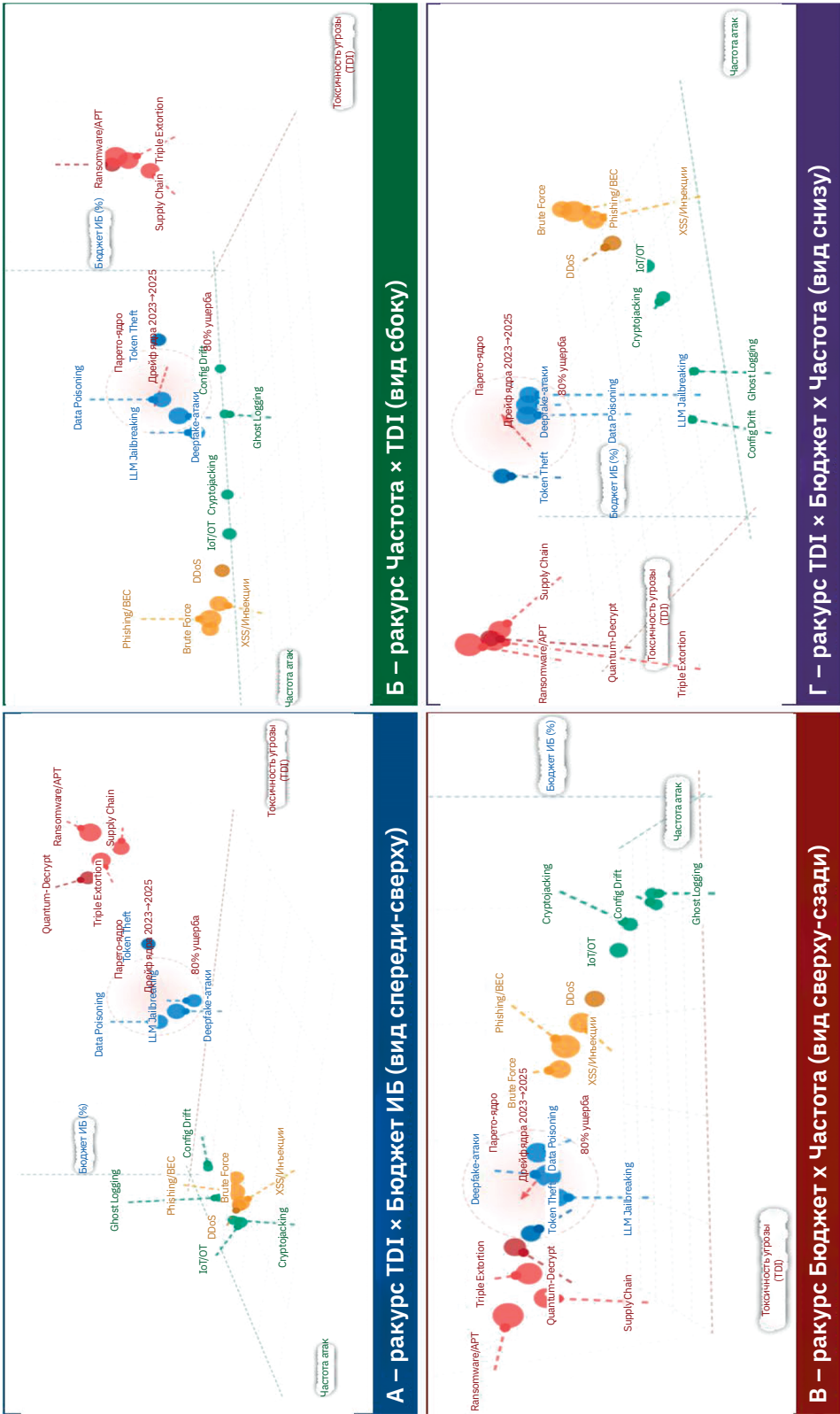


Рис. 2 | Четыре ортогональных ракурса трехмерного пространства угроз ($TDI \times \text{бюджет ИБ} \times \text{частота атак}$)²
Сфера – Парето-ядро (80 % совокупного EAL); стрелка – вектор дрейфа Парето-ядра 2023→2025

Fig. 2 | Four orthogonal perspectives of the three-dimensional threat space ($TDI \times \text{information security budget} \times \text{attack frequency}$)
Sphere is the Pareto core (80 % of the total EAL); arrow is the drift vector of the Pareto core 2023→2025

² 227 угроз БДУ ФСТЭК [7], выборка 94 МСП ЮФО, данные [4, 5, 16].

В качестве меры риска используется условное математическое ожидание $CVaR$ [32]:

$$CVaR_{\alpha}(X) = E[X | X > VaR_{\alpha}(X)] = VaR_{\alpha} \xi / (\xi - 1), \quad (7)$$

где X – случайная величина ущерба; $\alpha \in \{0,95; 0,99\}$ – уровень доверия; $VaR_{\alpha}(X)$ – квантиль уровня α ; $\xi > 1$ – параметр хвоста Парето, оцениваемый оценкой Хилла [22].

При нормальном распределении ущерба ($\xi \rightarrow \infty$) формула (7) асимптотически сходится к EAL , что обеспечивает математическую совместимость двух функций свертки. На рис. 3 представлено сравнение функций свертки EAL и $CVaR$ для двух типов распределения ущерба.

Рисунок 3 демонстрирует, почему стандартная мера EAL систематически недооценивает катастрофические риски: хвост распределения Apex Predator выходит далеко за пределы, охватываемые EAL .

Функция бюджетного упреждения B_{AI} для кластера Emerging AI. Угрозы класса Emerging AI характеризуются нестацио-

нарностью: их координаты в трехмерном пространстве смещаются во времени в направлении кластера Apex Predator. Скорость смещения фиксируется адаптивным индексом NTI [13], а бюджет упреждения B_{AI} определяется как экспоненциальная функция NTI , умноженная на прогнозное $CVaR$:

$$BAI(t) = \beta_0 \exp(\beta_1 NTI(t)) CVaR_{\alpha}(\hat{X}t + \Delta), \quad (8)$$

где $NTI(t)$ – значение адаптивного индекса угроз, фиксирующего скорость смещения Парето-ядра [13]; β_0, β_1 – параметры нормативно-сценарной калибровки, согласованные с прогнозной 16-факторной моделью 2026 г. ($\beta_0 = 2,5$; $\beta_1 = 2,8$); $CVaR_{\alpha}(\hat{X}t + \Delta)$ – прогнозное условное математическое ожидание ущерба; Δ – горизонт упреждения, кварталы.

Содержательный смысл формулы (8): чем быстрее NTI нарастает, тем раньше и большую долю бюджета необходимо резервировать против угрозы, еще не достигшей критического класса.

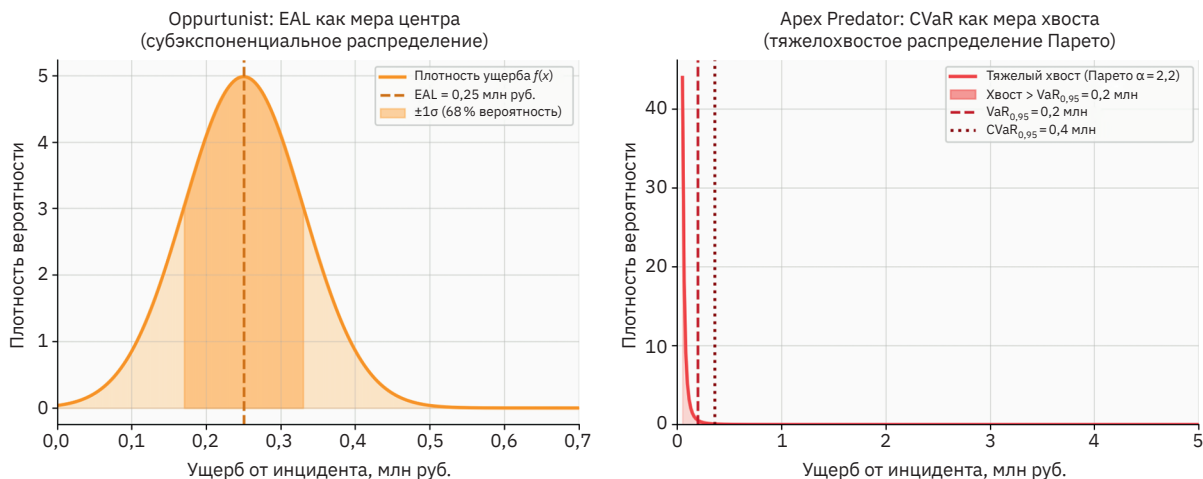


Рис. 3 | Сравнение функций EAL и $CVaR$ для двух типов распределения ущерба. Слева: субэкспоненциальное распределение (Opportunistic) – EAL как мера центра. Справа: тяжелохвостое распределение Парето (Apex Predator) – $CVaR_{0,95}$ как мера хвоста. Параметры: $\mu = 250$ тыс. руб., $\sigma = 80$ тыс. руб. (нормальное); $x_{\min} = 50$ тыс. руб., $\xi = 2,2$ (Парето)³

Fig. 3 | Comparison of EAL and $CVaR$ functions for two types of damage distribution. Left: subexponential distribution (Opportunistic) – EAL as a measure of the center. Right: heavy-tailed Pareto distribution (Apex Predator) – $CVaR_{0,95}$ as a measure of the tail. Parameters: $\mu = 250,000$ rubles, $\sigma = 80,000$ rubles (normal); $x_{\min} = 50,000$ rubles, $\xi = 2.2$ (Pareto)

³ Рассчитано авторами.

Параметры β_0 и β_1 не являются результатом регрессионного оценивания: ряд наблюдений NTI , достаточный для идентификации двухпараметрической экспоненты, к моменту подготовки статьи не накоплен, поэтому коэффициент детерминации к формуле (8) не приводится. Функция (8) интерпретируется как сценарный инструмент резервирования; ее эконометрическое оценивание на накапливаемых данных 2026–2027 гг. составляет следующий этап исследования. Экспоненциальная форма локально аппроксимирует ранний участок кривой с насыщением, и конкурирующей гипотезой выступает логистическая форма:

$$B_{AI}(t) = \frac{B_{\max}}{1 + \exp(-\gamma(NTI(t) - NTI_0))} CVaR_{\alpha}(\hat{X}_{t+\Delta}), \quad (9)$$

где $B_{\max}$ – верхний предел доли бюджета упреждения (насыщение), безразмерный множитель; $\gamma > 0$ – параметр крутизны логистического перехода; NTI_0 – точка перегиба, по сценарным данным близкая к пороговому значению $NTI \approx 0,45$; остальные обозначения соответствуют формуле (7).

При $NTI(t) \ll NTI_0$ формы (8) и (9) практически неразличимы; накопление наблюдений позволит различить их по информационным критериям – выбор формы переведен из области допущений в разряд проверяемых гипотез.

На рис. 4 представлена динамика NTI и доли бюджета на Emerging AI по сценарным данным 2023–2026 гг., иллюстрирующая экспоненциальный характер зависимости (7) и пороговый эффект при $NTI \approx 0,45$.

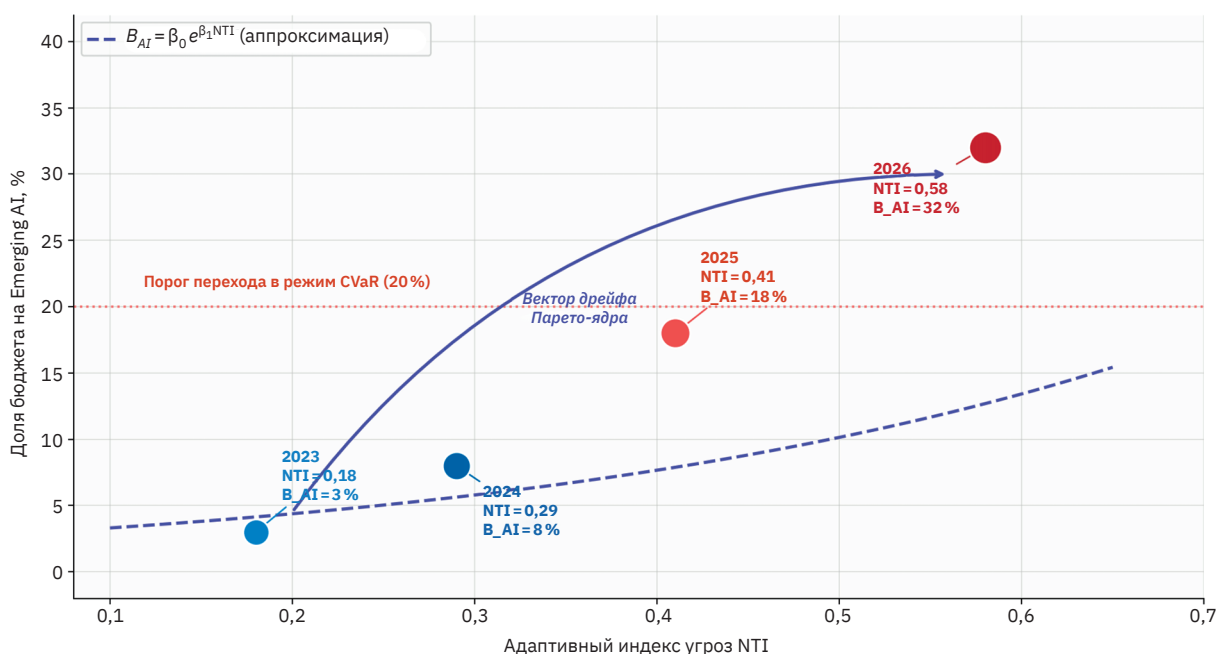


Рис. 4 | Динамика адаптивного индекса NTI и доли бюджета на Emerging AI в 2023–2026 гг.⁴
Точки – сценарные значения прогнозной модели; пунктирная кривая – аппроксимация $B_{AI} = 2,5 \exp(2,8NTI)$; горизонтальная пунктирная линия – порог 20 %, при превышении которого рекомендуется переход на функцию $CVaR$

Fig. 4 | Dynamics of the adaptive NTI index and the share of the budget allocated to Emerging AI in 2023–2026
The dots represent scenario values from the forecast model; the dashed curve is an approximation of $B_{AI} = 2.5 \exp(2.8NTI)$; the horizontal dashed line is the 20 % threshold, exceeding which it is recommended to switch to the $CVaR$ function

⁴ Рассчитано авторами по данным выборки и [4, 5, 10].

Рисунок 4 иллюстрирует нелинейный характер роста бюджетных потребностей на Emerging AI: при $NTI > 0,45$ функция B_{AI} входит в режим ускоренного роста, что соответствует переходу угроз из формирующегося класса в зону Apex Predator.

Нелинейный характер роста бюджета на класс Emerging AI при $NTI > 0,45$ согласуется с моделями выпуклой оптимизации динамики распространения вредоносного ПО [33], где плотность инфицирования входит в защитные расходы по нелинейному закону.

Теорема о вертикальной совместимости уровней. Утверждение. Пусть для угрозы i класса Opportunist выполняется: $w_1 = 1, f_i = \text{const}, \kappa_{obs} = 1$.

Тогда $EAL_i = f_i TDI_{normi} A_i$, что пропорционально TDI_{normi} при фиксированном A_i .

Следовательно, ранжирование угроз по EAL при указанных условиях совпадает с ранжированием по TDI , воспроизводя результат 16-факторной модели уровня I в предельном частном случае.

Аналогично при $\xi \rightarrow \infty$ и нормальном распределении ущерба $CVaR_\alpha(X) \rightarrow E[X] = EAL$, т.е. функция Уровня III для кластера Apex Predator сходится к функции для кластера Opportunist.

Вся система функций свертки – одно параметрическое семейство: при $\xi \rightarrow \infty$ и $w_1 = 1$ новые функции коллапсируют в 16-факторную модель. Расширение не отменяет базовый уровень – оно включает его как частный случай.

Такое свойство соответствует общему принципу преемственности научных моделей: расширенная конструкция признается теоретически состоятельной, если в предельных условиях она воспроизводит результаты базового уровня, что соответствует принципу преемственности иерархических систем [34]. Выполнение этого условия позволяет говорить об отсутствии логического разрыва между уровнем I и III.

4. РОЛЬ МЕТОДА ДЕЛЬФИ: СТРОГОЕ РАЗГРАНИЧЕНИЕ

Метод Дельфи [20] в каркасе выполняет единственную функцию – калибровку па-

раметров там, где прямое измерение технически невозможно: веса w_1-w_3 в матрице АНР [19]; коэффициент наблюдаемости κ_{obs} для скрытых угроз и уровень доверия α в $CVaR$ как управленческая переменная аппетита к риску. Угрозы как таковые этим методом не измеряются ни на одном уровне каркаса – это принципиальное ограничение, а не упущение.

Первый этап – оценка весовых коэффициентов w_1, w_2, w_3 в матрице попарных сравнений АНР; верифицируемость обеспечивается коэффициентом согласованности $CR < 0,10$. Второй этап – оценка коэффициента наблюдаемости κ_{obs} для скрытых угроз (5). Третий этап – выбор уровня доверия α в $CVaR$ (7) как управленческого параметра аппетита к риску.

Оси пространства угроз измеряются независимо от метода Дельфи: ось X – по нормативной базе БДУ ФСТЭК [7]; ось Y – по эмпирическим данным выборки 94 МСП; ось Z – по открытым аналитическим отчетам [4, 5, 16, 17] с поправкой κ_{obs} . Такое разграничение соответствует стандартной научной практике использования экспертных методов исключительно там, где прямое измерение невозможно [20].

Предложенный трехуровневый каркас совместим с международным стандартом ISO/IEC 27005:2022 [12] в части управления рисками информационной безопасности и может быть встроен в систему менеджмента ИБ организации без структурных конфликтов.

5. ОБСУЖДЕНИЕ

Первый теоретический вклад работы – Гордон и Леб [1], а вслед за ними Фильдер с соавторами [3], исходят из молчаливого допущения об однородности угроз – оно нигде не проверяется, просто берется по умолчанию. $F=47,3$ при $p<0,001$ означает, что это допущение неверно для реальных данных МСП ЮФО. Практическое следствие конкретно: организация, использующая единую линейную свертку, систематически недофинансирует защиту от Apex Predator-угроз – именно тех, которые при реализации стоят на порядок дороже.

Второй вклад – формализация функции бюджетного упреждения B_{AI} (8), связывающей скорость дрейфа Парето-ядра (NTI) с прогнозным $CVaR$. Литература по динамическим когерентным риск-мерам формализует пересчет меры риска во времени по мере поступления информации о процессе потерь [35, 36]; функция B_{AI} решает смежную, но не тождественную задачу – аргументом бюджетной функции служит скорость изменения внешнего индикатора ландшафта (дрейф NTI), а не фильтрация самого процесса потерь. Элемент новизны состоит в связывании бюджета упреждения с наблюдаемой скоростью миграции кластера угроз внутри кластерно-зависимого каркаса для МСП.

Третий вклад – теорема вертикальной совместимости, показывающая, что 16-факторная таксономия [13, 14] выступает частным случаем нового каркаса. Тем самым обеспечивается преемственность научного результата: ранее накопленный эмпирический материал сохраняет аналитическую значимость и включается в расширенную модель без повторного сбора данных.

6. ЗАКЛЮЧЕНИЕ

Трехуровневый каркас бюджетирования ИБ для МСП решает задачу, которую классические модели обходили стороной:

как распределить бюджет, когда угрозы статистически неоднородны. Доказано, что 16-факторная таксономия угроз на основе TDI и метода Фишера – Дженкса не вступает в методологический конфликт с функциями свертки EAL , $CVaR$ и B_{AI} , а выступает их необходимым фундаментом.

Три функции соотносятся с различными статистическими и управленческими типами угроз: массовыми субэкспоненциальными, катастрофическими тяжелохвостыми и динамически смещающимися AI -угрозами. Метод Дельфи применяется исключительно для калибровки весов АНР, что повышает воспроизводимость расчетов и делает процедуру калибровки параметров методологически прозрачной.

Модель имеет границы применимости, которые важно обозначить явно. Параметры β_0 и β_1 функции B_{AI} заданы сценарно по прогнозной 16-факторной модели 2026 г., их эконометрическое оценивание на накапливаемых наблюдениях 2026–2027 гг. составляет следующий этап исследования, а перенос на другие регионы или отрасли требует самостоятельной калибровки.

Оценка Хилла устойчива при $n > 50$ наблюдений в хвосте; при меньших выборках параметр ξ следует рассматривать как нижнюю оценку. Эти ограничения не снижают применимость каркаса, но задают условия, при которых расчеты сохраняют статистическую корректность.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. Gordon L. A., Loeb M. P. The economics of information security investment // ACM Transactions on Information and System Security. 2002. Vol. 5. № 4. P. 438–457. DOI: 10.1145/581271.581274.
2. Böhme R., Schwartz G. Modeling cyber-insurance: towards a unifying framework // Proceedings WEIS. 2010. P. 1–21.
3. Fielder A., Panaousis E., Malacaria P. et al. Decision support approaches for cyber

- security investment // *Decision Support Systems*. 2016. Vol. 86. P. 13–23. DOI: 10.1016/j.dss.2016.02.012.
4. Verizon. 2025 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 12.04.2026).
 5. ENISA Threat Landscape 2025. URL: <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf> (дата обращения: 12.04.2026).
 6. **Kshetri N.** *Cybercrime and Cybersecurity in the Global South*. Houndmills: Palgrave Macmillan, 2013. 264 p. DOI: 10.1057/9781137021946.
 7. Банк данных угроз безопасности информации ФСТЭК России. URL: <https://bdu.fstec.ru/threat> (дата обращения: 17.04.2026).
 8. **Embrechts P., Klüppelberg C., Mikosch T.** *Modelling Extremal Events for Insurance and Finance*. Berlin: Springer, 1997. 648 p. DOI: 10.1007/978-3-642-33483-2.
 9. **Freund J., Jones J.** *Measuring and Managing Information Risk: A FAIR Approach*. Oxford: Butterworth-Heinemann, 2015. 408 p. DOI: 10.1016/C2013-0-09966-5.
 10. **Rass S., Schauer S., König S., Zhu Q.** *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*. Cham : Springer, 2020. 297 p. DOI: 10.1007/978-3-030-46908-5.
 11. NIST. *Security and Privacy Controls for Information Systems and Organizations: NIST SP 800-53 Rev. 5*. Gaithersburg, MD: NIST, 2020. DOI: 10.6028/NIST.SP.800-53r5.
 12. ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection Guidance on managing information security risks*. Geneva: ISO, 2022. 75 p.
 13. **Мандрица И. В., Антонов В. В., Мандрица О. В., Бугаева А. В.** Индекс Парето как критерий адаптивного бюджетирования информационной безопасности // *Правовая информатика*. 2026. № 1. С. 16–30. DOI: 10.24412/1994-1404-2026-1-00-02. EDN: MZJQEI.
 14. **Mandritsa I., Grobova T., Petrenko V., Mandritsa O.** Risk-based Pareto Approach to the Training of Information Security Specialists Based on a Sixteen-factor Threat Model // *International Journal of Open Information Technologies*. 2026. Vol. 14. № 5. P. 20–26. EDN: LLIBVY.
 15. **Lelarge M.** *Economics of malware: Epidemic risks model, network externalities and incentives* // 47th Annual Allerton Conference on Communication, Control, and Computing. IEEE, 2009. P. 1353–1360. DOI: 10.1109/ALLERTON.2009.5394946.
 16. Positive Technologies. Актуальные киберугрозы 2025: итоги года. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/> (дата обращения: 17.04.2026).
 17. BI.ZONE. Материалы. URL: <https://bi.zone/expertise/research/> (дата обращения: 17.04.2026).
 18. **Jenks G. F.** The data model concept in statistical mapping // *International Yearbook of Cartography*. 1967. Vol. 7. P. 186–190.
 19. **Saaty T. L.** *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980. 287 p.
 20. **Dalkey N., Helmer O.** An experimental application of the Delphi method // *Management Science*. 1963. Vol. 9. № 3. P. 458–467. DOI: 10.1287/mnsc.9.3.458.
 21. **Kolmogorov A. N.** Sulla determinazione empirica di una legge di distribuzione // *Giornale dell'Istituto Italiano degli Attuari*. 1933. Vol. 4. P. 83–91.
 22. **Hill B. M.** A simple general approach to inference about the tail of a distribution // *The Annals of Statistics*. 1975. Vol. 3. № 5. P. 1163–1174. DOI: 10.1214/aos/1176343247.
 23. **McNeil A. J., Frey R., Embrechts P.** *Quantitative Risk Management: Concepts, Techniques and Tools: Revised Edition*. Princeton: Princeton University Press, 2015. 720 p.
 24. FIRST. *Common Vulnerability Scoring System version 3.1: Specification Document*. URL: <https://www.first.org/cvss/v3.1/specification-document> (дата обращения: 17.04.2026).
 25. **Simon H. A.** *The Architecture of Complexity: Hierarchical Systems* // *Proceedings of the American Philosophical Society*. 1962. Vol. 106. № 6. P. 467–482.
 26. **Hartigan J. A.** *Clustering Algorithms*. New York: John Wiley & Sons, 1975. 351 p.
 27. **Caliński T., Harabasz J.** A dendrite method for cluster analysis // *Communications in Statistics*. 1974. Vol. 3. № 1. P. 1–27. DOI: 10.1080/03610927408827101.
 28. **Mesarović M. D., Macko D., Takahara Y.** *Theory of Hierarchical, Multilevel, Systems*. New York: Academic Press, 1970. 294 p.
 29. **Kaplan R. S., Norton D. P.** *The Balanced Scorecard: Translating Strategy into Action*. Boston: Harvard Business School Press, 1996. 322 p.

30. **Linsmeier T. J., Pearson N. D.** Value at Risk // *Financial Analysts Journal*. 2000. Vol. 56. № 2. P. 47–67. DOI: 10.2469/faj.v56.n2.2340.
31. **Artzner P., Delbaen F., Eber J.-M., Heath D.** Coherent Measures of Risk // *Mathematical Finance*. 2001. Vol. 9. № 3. P. 203–228. DOI: 10.1111/1467-9965.00068.
32. **Rockafellar R. T., Uryasev S.** Optimization of conditional value-at-risk // *Journal of Risk*. 2000. Vol. 2. № 3. P. 21–41. DOI: 10.21314/JOR.2000.038.
33. **Pal R., Golubchik L.** Analyzing self-defense investments in Internet security under cyber-insurance coverage // 30th IEEE International Conference on Distributed Computing Systems. IEEE, 2010. P. 339–347. DOI: 10.1109/ICDCS.2010.79.
34. **Anderson P. W.** More is Different: Broken Symmetries and the Nature of the Hierarchical Structure of Science // *Science*. 1972. Vol. 177. № 4047. P. 393–396. DOI: 10.1126/science.177.4047.393.
35. **Riedel F.** Dynamic coherent risk measures // *Stochastic Processes and their Applications*. 2004. Vol. 112. № 2. P. 185–200. DOI: 10.1016/j.spa.2004.03.004.
36. **Acciaio B., Penner I.** Dynamic risk measures / eds. G. Di Nunno, B. Øksendal // *Advanced Mathematical Methods for Finance*. Berlin: Springer, 2011. P. 1–34. DOI: 10.1007/978-3-642-18412-3_1.

REFERENCES

1. **Gordon L. A., Loeb M. P.** The economics of information security investment. *ACM Transactions on Information and System Security*. 2002. Vol. 5. No. 4, pp. 438–457. DOI: 10.1145/581271.581274.
2. **Böhme R., Schwartz G.** Modeling cyber-insurance: towards a unifying framework. *Proceedings WEIS*. 2010, pp. 1–21.
3. **Fielder A., Panaousis E., Malacaria P. et al.** Decision support approaches for cyber security investment. *Decision Support Systems*. 2016. Vol. 86, pp. 13–23. DOI: 10.1016/j.dss.2016.02.012.
4. Verizon. 2025 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/reports/dbir/> (accessed: 12.04.2026).
5. ENISA Threat Landscape 2025. URL: <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf> (accessed: 12.04.2026).
6. **Kshetri N.** *Cybercrime and Cybersecurity in the Global South*. Houndmills: Palgrave Macmillan, 2013, 264 p. DOI: 10.1057/9781137021946.
7. Bank of information security threats data (BDU) Federal Service for Technical and Export Control of Russia (FSTEC). URL: <https://bdu.fstec.ru/threat> (accessed: 17.04.2026). (In Russian)
8. **Embrechts P., Klüppelberg C., Mikosch T.** *Modelling Extremal Events for Insurance and Finance*. Berlin: Springer, 1997, 648 p. DOI: 10.1007/978-3-642-33483-2.
9. **Freund J., Jones J.** *Measuring and Managing Information Risk: A FAIR Approach*. Oxford: Butterworth-Heinemann, 2015, 408 p. DOI: 10.1016/C2013-0-09966-5.
10. **Rass S., Schauer S., König S., Zhu Q.** *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*. Cham: Springer, 2020, 297 p. DOI: 10.1007/978-3-030-46908-5.
11. NIST. *Security and Privacy Controls for Information Systems and Organizations: NIST SP 800-53 Rev. 5*. Gaithersburg, MD: NIST, 2020. DOI: 10.6028/NIST.SP.800-53r5.
12. ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection Guidance on managing information security risks*. Geneva: ISO, 2022, 75 p.
13. **Mandritsa I. V., Antonov V. V., Mandritsa O. V., Bugaeva A. V.** Pareto index as a criterion for adaptive information security budgeting. *Legal Informatic*. 2026. No. 1, pp. 16–30. DOI: 10.24412/1994-1404-2026-1-00-02. (In Russian)
14. **Mandritsa I., Grobova T., Petrenko V., Mandritsa O.** Risk-based Pareto Approach to the Training of Information Security Specialists Based on a Sixteen-factor Threat Model. *International Journal of Open Information Technologies*. 2026. Vol. 14. No. 5, pp. 20–26. EDN: LLIBVY.
15. **Lelarge M.** Economics of malware: Epidemic risks model, network externalities and

- incentives. 47th Annual Allerton Conference on Communication, Control, and Computing. IEEE, 2009, pp. 1353–1360. DOI: 10.1109/ALLERTON.2009.5394946.
16. Positive Technologies. Relevant cyber threats 2025: Year-end summary. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/> (accessed: 17.04.2026). (In Russian)
 17. BI.ZONE. Materials. URL: <https://bi.zone/expertise/research/> (accessed: 17.04.2026). (In Russian)
 18. Jenks G. F. The data model concept in statistical mapping. *International Yearbook of Cartography*. 1967. Vol. 7, pp. 186–190.
 19. Saaty T. L. The Analytic Hierarchy Process. New York: McGraw-Hill, 1980, 287 p.
 20. Dalkey N., Helmer O. An experimental application of the Delphi method. *Management Science*. 1963. Vol. 9. No. 3, pp. 458–467. DOI: 10.1287/mnsc.9.3.458.
 21. Kolmogorov A. N. Sulla determinazione empirica di una legge di distribuzione. *Giornale dell'Istituto Italiano degli Attuari*. 1933. Vol. 4, pp. 83–91.
 22. Hill B. M. A simple general approach to inference about the tail of a distribution. *The Annals of Statistics*. 1975. Vol. 3. No. 5, pp. 1163–1174. DOI: 10.1214/aos/1176343247.
 23. McNeil A. J., Frey R., Embrechts P. Quantitative Risk Management: Concepts, Techniques and Tools: Revised Edition. Princeton: Princeton University Press, 2015, 720 p.
 24. FIRST. Common Vulnerability Scoring System version 3.1: Specification Document. URL: <https://www.first.org/cvss/v3.1/specification-document> (accessed: 17.04.2026).
 25. Simon H. A. The Architecture of Complexity: Hierarchical Systems. *Proceedings of the American Philosophical Society*. 1962. Vol. 106. No. 6, pp. 467–482.
 26. Hartigan J. A. Clustering Algorithms. New York: John Wiley & Sons, 1975, 351 p.
 27. Caliński T., Harabasz J. A dendrite method for cluster analysis. *Communications in Statistics*. 1974. Vol. 3. No. 1, pp. 1–27. DOI: 10.1080/03610927408827101.
 28. Mesarović M. D., Macko D., Takahara Y. Theory of Hierarchical, Multilevel, Systems. New York: Academic Press, 1970, 294 p.
 29. Kaplan R. S., Norton D. P. The Balanced Scorecard: Translating Strategy into Action. Boston: Harvard Business School Press, 1996, 322 p.
 30. Linsmeier T. J., Pearson N. D. Value at Risk. *Financial Analysts Journal*. 2000. Vol. 56. No. 2, pp. 47–67. DOI: 10.2469/faj.v56.n2.2340.
 31. Artzner P., Delbaen F., Eber J.-M., Heath D. Coherent Measures of Risk. *Mathematical Finance*. 2001. Vol. 9. No. 3, pp. 203–228. DOI: 10.1111/1467-9965.00068.
 32. Rockafellar R. T., Uryasev S. Optimization of conditional value-at-risk. *Journal of Risk*. 2000. Vol. 2. No. 3, pp. 21–41. DOI: 10.21314/JOR.2000.038.
 33. Pal R., Golubchik L. Analyzing self-defense investments in Internet security under cyber-insurance coverage. 30th IEEE International Conference on Distributed Computing Systems. IEEE, 2010, pp. 339–347. DOI: 10.1109/ICDCS.2010.79.
 34. Anderson P. W. More is Different: Broken Symmetries and the Nature of the Hierarchical Structure of Science. *Science*. 1972. Vol. 177. No. 4047, pp. 393–396. DOI: 10.1126/science.177.4047.393.
 35. Riedel F. Dynamic coherent risk measures. *Stochastic Processes and their Applications*. 2004. Vol. 112. No. 2, pp. 185–200. DOI: 10.1016/j.spa.2004.03.004.
 36. Acciaio B., Penner I. Dynamic risk measures. Eds. G. Di Nunno, B. Øksendal. *Advanced Mathematical Methods for Finance*. Berlin: Springer, 2011, pp. 1–34. DOI: 10.1007/978-3-642-18412-3_1.

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

МАНДРИЦА Игорь Владимирович – д-р экон. наук, профессор, Северо-Кавказский федеральный университет, Россия, 355017, Ставрополь, пл. Ленина, 3А, к. 6; главный научный сотрудник, МИРЕА – Российского технологического университета (филиал в Ставрополе), Россия, 355035, Ставрополь, пр-т Кулакова, д. 8
E-mail: d_artman@mail.ru
ORCID: 0000-0001-9911-1584

MANDRITSA Igor V. – Doctor of Economics, Professor, North-Caucasus Federal University, Russia, 355017, Stavropol, Lenin Square, 3A, bldg. 6; Chief Researcher, MIREA – Russian Technological University (Stavropol branch), Russia, 355035, Stavropol, Kulakova ave., 8

ПЕТРЕНКО Вячеслав Иванович – канд. техн. наук, доцент, заведующий кафедрой, Северо-Кавказский федеральный университет, Россия, 355017, Ставрополь, пл. Ленина, 3А, к. 6
E-mail: vipetrenko@ncfu.ru
ORCID: 0000-0003-4293-7013

PETRENKO Vyacheslav I. – Candidate of Engineering Sciences, Associate Professor, Head of Department, North-Caucasus Federal University, Russia, 355017, Stavropol, Lenin Square, 3A, bldg. 6

МАНДРИЦА Ольга Владимировна – канд. экон. наук, доцент, заведующая кафедрой, МИРЕА – Российского технологического университета (филиал в Ставрополе), Россия, 355035, Ставрополь, пр-т Кулакова, д. 8
E-mail: man_olga@mail.ru
ORCID: 0000-0002-0364-1239

MANDRITSA Olga V. – Candidate of Economics, Associate Professor, Head of Department, MIREA – Russian Technological University (Stavropol branch), Russia, 355035, Stavropol, Kulakova ave., 8