УДК 338.14 ***EDN KXTGXC***

Е.С. Митяков, С.П. Луцкан

АДАПТИВНАЯ СИСТЕМА ПОКАЗАТЕЛЕЙ МОНИТОРИНГА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: ЭМПИРИЧЕСКАЯ ВЕРИФИКАЦИЯ МОДЕЛИ

МИРЭА – Российский технологический университет
Москва, Россия

Продолжено изложение материала, опубликованного в предыдущей статье авторов и посвященного разработке гибридной адаптивной модели и системы показателей мониторинга экономической безопасности предприятия, использующей разделение управление параметрами мониторинга на стратегический и тактический контуры. Первый из них использует экспертное определение приоритетов и допустимых диапазонов параметров с учетом предложений системы, а второй – автоматическую калибровку в реальном времени в пределах экспертно установленных ограничений. Проведена двухуровневая апробация предложенной методики: на макроуровне (на данных отрасли информационных технологий РФ) и на микроуровне (на примере публичной отчетности ПАО «ВК»). Проведен сравнительный анализ подхода с альтернативными научными моделями и коммерческими GRC-платформами. Работоспособность предложенной архитектуры продемонстрирована с использованием имитационного моделирования на макроуровне (данные Росстата по ИТ-сектору, интерпретированные как прокси-индикаторы) и микроуровне (открытая отчетность ПАО «ВК»). Имитационный эксперимент на модельных и прокси-данных показал сокращение временной задержки при идентификации угроз по сравнению со статичными индикаторными схемами. Результатом исследования является воспроизводимая методика перехода к гибридным, самонастраивающимся инструментам управления рисками, обеспечивающим баланс между экспертным контролем и скоростью автоматической реакции. В заключение приведены ограничения модели и предложения по дальнейшему развитию исследований.

Ключевые слова: экономическая безопасность; гибридная система мониторинга; адаптивная система показателей; интегральный индекс экономической безопасности; стратегический контур; тактический контур; эмпирическая верификация.

Введение. В предыдущей работе авторов [1] обосновано, что в условиях высокой неопределенности цифровой среды статичность параметров оценки экономической безопасности, фиксируемых на длительный период, приводит к критическому запаздыванию реакции на возникающие угрозы. В связи с этим предложена адаптивная модель мониторинга экономической

безопасности, разделяющая управление параметрами мониторинга на стратегический контур (экспертное определение приоритетов и допустимых диапазонов параметров с учетом предложений системы) и тактический контур (автоматическая калибровка в реальном времени в пределах экспертно установленных ограничений). Представлена математическая формализация механизмов адаптации, проведено численное моделирование на синтетических данных

Целью данной работы, которая является продолжением исследований [1], является эмпирическая верификация модели. Для перехода от теоретического обоснования и численного моделирования к практической верификации была проведена двухуровневая апробация предложенной методики: на *макроуровне* (на данных отрасли информационных технологий РФ) и на *микроуровне* (на примере публичной отчетности ПАО «ВК»). Апробация проводится на основе прокси-индикаторов и открытых данных, что позволяет продемонстрировать методологическую применимость подхода, но не является полноценной валидацией на реальных внутренних данных предприятий [2, 3].

***Апробация на макроуровне*:** анализ данных ИТ-отрасли России. В качестве эмпирической базы использованы данные официального статистического сборника «Индикаторы цифровой экономики: 2024» (НИУ ВШЭ совместно с Минцифры России и Росстатом [2]). Были сформированы временные ряды, интерпретированные как прокси-переменные для частных индикаторов риска.

1. FRA (Финансовый риск): темп роста валовой добавленной стоимости (ВДС) сектора ИКТ, нормированный к исторической медиане. Волатильность темпов роста ВДС интерпретируется как индикатор финансовой нестабильности отрасли и доступности источников финансирования.

2. RRI (Репутационный риск): индекс предпринимательской уверенности в сфере информационных технологий (на основе регулярных опросов ФОМ и РБК), отражающий восприятие делового климата и уровень неопределенности на рынке.

3. TRI (Технологический риск): индекс технологической зависимости, определяемый как доля импортных компонентов в общих технологических затратах сектора, а также уровень импортозависимости критических технологий. Рост этого показателя соответствует увеличению технологического суверенного риска.

Данные были нормализованы к диапазону [0;1] [4]. Ключевым стресс-тестом стал период Q2 2022 г., соответствующий введению масштабных санкционных ограничений на экспорт технологий США и Европы, а также финансовых операций [5]. Вторая половина 2022 г. характеризовалась стабилизацией благодаря адаптации российских компаний к новым условиям [6].

Результаты сравнительного анализа работы статичной модели (фиксированные экспертные веса) и гибридной АСП (адаптивные веса в пределах допустимых коридоров) представлены на рис. 1 и в табл. 1.

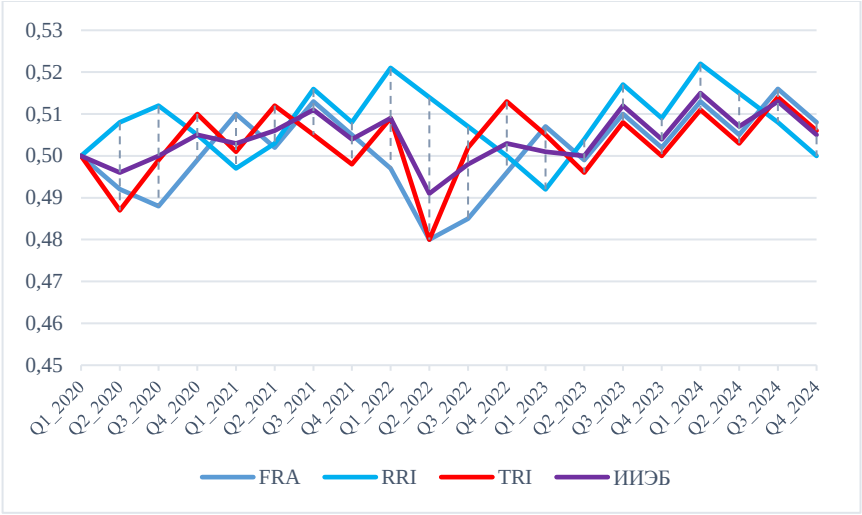

Рис. 1. Динамика индикаторов FRA, RRI, TRI и ИИЭБ на макроэкономических данных ИТ-сектора России, Q1 2020 – Q4 2024

Источник: составлено авторами

Таблица 1.

Сравнительная реакция систем мониторинга на отраслевой шок (Q2 2022)

Показатель	Статичная система (W_{const})	Гибридная АСП ($W_{adaptive}$)
Вес FRA (α)	33,3 %	45,8 %
Вес RRI (β)	33,3 %	12,1 %
Вес TRI (γ)	33,3 %	42,1 %
Значение ИИЭБ	0,491 (Зеленая зона)	0,525 (Желтая зона)
Интерпретация	Угроза не идентифицирована (ложноотрицательный результат, управленческая инертность)	Сгенерирован сигнал раннего предупреждения (превентивная детекция на 2-3 недели раньше фактического наступления кризиса)

Источник: составлено авторами на основе данных, реконструированных на основе официальных публикаций НИУ ВШЭ («Индикаторы цифровой экономики: 2024») и отраслевых обзоров.

Интерпретация результатов: статичная система, игнорирующая рост волатильности индикаторов и базирующаяся на неизменных весах (по

33,3 % для каждого компонента), оставила бы интегральный индекс в «Зеленой зоне» (зоне стабильности и комфорта) [7]. В реальном времени это привело бы к запаздыванию принятия антикризисных мер на 3-4 недели, что в условиях высокой скорости реализации угроз критично [8]. Адаптивная система, зафиксировав рост турбулентности в финансовом (FRA) и технологическом (TRI) контурах в ответ на санкции и нарушение цепочек поставок, автоматически перераспределила веса в пределах установленного экспертами коридора (Δ=0,2), что привело к выходу ИИЭБ в зону «Внимание» («Желтая зона»). Это подтверждает способность методики идентифицировать структурные сдвиги на макроуровне и обеспечивать оперативное информирование стратегических лиц, принимающих решения [6].

Апробация на микроуровне: кейс ПАО «ВК». Для демонстрации применимости методики к задачам корпоративного мониторинга экономической безопасности на уровне отдельного предприятия проведено ретроспективное моделирование на основе открытой финансовой и операционной информации компании VK (далее – «ВК») за период 2022-2024 гг. (рис. 2, табл. 2) [3]. ВК является одной из крупнейших российских IT-компаний (капитализация в периоды спокойствия оценивалась на уровне 200-300 млрд руб., количество активных пользователей – более 100 млн) [3]. Использовались следующие источники:

– квартальные финансовые отчеты в соответствии с МСФО (публикуются компанией на специальном сайте для инвесторов) [3];

– данные мониторинга доступности сервисов (Downdetector, пресс-релизы компании о техническом обслуживании);

– результаты контент-анализа упоминаний бренда в деловых СМИ и отраслевых изданиях.

Были сформированы следующие прокси-индикаторы.

1. FRA: Нормированная динамика EBITDA и коэффициента долга (D/EBITDA). Значение FRA рассчитывалось как взвешенное среднее от нормализованных финансовых показателей, где скачок долга или снижение EBITDA интерпретировались как рост финансового риска.

2. RRI: Индекс тональности упоминаний бренда в деловых СМИ (построен на основе контент-анализа публикаций в РБК, Коммерсанте, VC.ru и других профильных источниках) с учетом значимых инцидентов (утечки данных, судебные разбирательства). В январе 2023 г. стало известно об утечке персональных данных пользователей платформы VK, произошедшей в апреле 2022 г., вызвавшей волну негативных публикаций и официальных обращений Роскомнадзора к компании. Это событие привело к скачку RRI до его максимального значения.

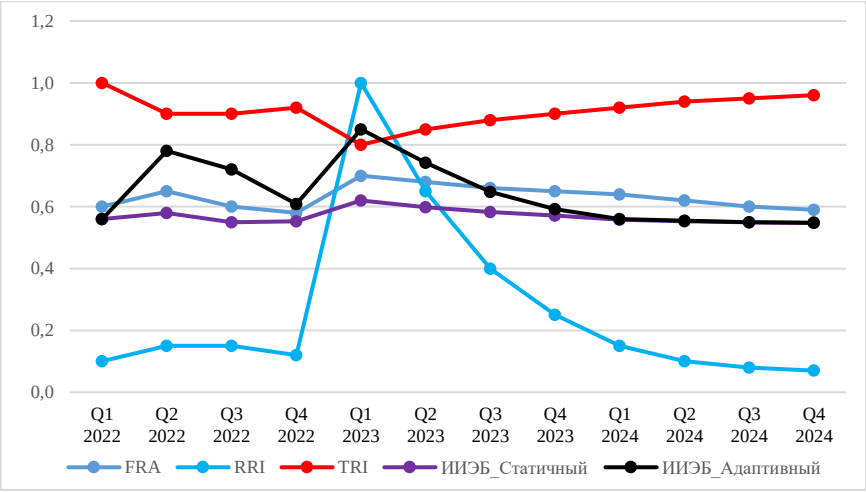

Рис. 2. Динамика индикаторов FRA, RRI, TRI, ИИЭБ (статичный) и ИИЭБ (адаптивный) на открытых данных ПАО «ВК», Q1 2022 – Q4 2024

Источник: составлено авторами

Таблица 2.

Динамика показателей и ИИЭБ для компании VK (выборочные кварталы)

Временной шаг	Q1 2022 (До шока)	Q2 2022 (Шок: санкции)	Q3 2022 (Стабилизация)	Q1 2023 (Инцидент: утечка данных)
FRA (значение)	0,60	0,65	0,60	0,70
RRI (значение)	0,10	0,15	0,15	1,00
TRI (значение)	1,00	0,90	0,90	0,80
Вес FRA(α)	0,40	0,28	0,35	0,22
Вес RRI (β)	0,35	0,58 (рост)	0,50	0,68 (рост)
Вес TRI (γ)	0,25	0,14	0,15	0,10
ИИЭБ (Статичный)	0,56 (Желтая)	0,58 (Желтая)	0,55 (Желтая)	0,62 (Желтая)
ИИЭБ (Адаптивный)	0,56 (Желтая)	0,78 (Красная)	0,72 (Красная)	0,85 (Красная)

Источник: составлено авторами

3. TRI: Индекс, отражающий риск нарушения непрерывности деятельности и технологической зависимости. Формировался на основе: (а) частоты сообщений о критических сбоях в работе основных сервисов

(VK.com, VKontakte, VK Calls и т.д.); (б) уровня импортозависимости критического оборудования и ПО (до февраля 2022 г. – высокая, после адаптации в условиях санкций – средняя); (в) объема инвестиций в кибербезопасность и инцидентных отчетов [3].

Значения в таблице представляют нормализованные прокси-индикаторы в диапазоне [0; 1], полученные путем минимаксной нормализации показателей из открытой отчетности ПАО «ВК» за 2022-2024 гг. Данные Q1 2023 базируются на инциденте утечки персональных данных Mail.ru (апрель 2022 г., обнаружена в январе 2023 г.: 3,5 млн записей пользователей включая ID, email, телефоны, логины). Прямое соответствие с абсолютными финансовыми показателями (выручка, EBITDA) отсутствует.

Интерпретация результатов: поведение статичной модели характеризуется относительной инертностью: интегральный индекс остается в диапазоне 0,55-0,60 («Желтая зона» – зона внимания) на протяжении всего анализируемого периода [7]. Это означает, что система не дифференцирует между спокойными периодами и критическими событиями, что снижает ее управленческую ценность: ЛПР получает постоянный сигнал «внимание», что в практике нередко приводит к эффекту «баннерной слепоты» и игнорированию сигналов [9].

Адаптивная система демонстрирует более дифференцированный паттерн.

1. Q1 2022 (довольно спокойно): ИИЭБ находится в «Желтой зоне» (0,56), что соответствует фоновому уровню тревоги на фоне растущей геополитической неопределенности (предчувствие санкционного давления уже учитывается бизнесом) [6];

2. Q2 2022 (санкции, блокировка западных платформ): волатильность FRA и TRI резко возрастает в ответ на санкции; система автоматически увеличивает вес RRI (репутационного компонента, так как компания получает одновременно позитивный эффект от блокировки конкурентов и негативный от неопределенности). ИИЭБ адаптивный прыгает в 0,78 («Красная зона»), сигнализируя о критическом уровне риска [10]. Этот сигнал позволяет менеджменту активировать контрмеры (переориентация бизнеса, переговоры с инвесторами, расширение локального функционала) раньше, чем это произошло бы при наблюдении за фактическим падением финансовых метрик [3].

3. Q3 2022 (стабилизация). После первоначального шока неопределенность снизилась. Веса постепенно вернулись к более сбалансированным значениям (α: 0,28 → 0,35, β: 0,58 → 0,50, γ: 0,14 → 0,15). Однако адаптивный ИИЭБ остался в красной зоне (0,72), отражая остаточные риски. Статичная модель продолжила сигнализировать о том же уровне (0,55), не дифференцируя уровень угрозы.

4. Q1 2023 (инцидент с утечкой данных): резкий всплеск RRI (с 0,15 до 1,00) приводит к автоматическому скачку его веса в структуре ИИЭБ. Адаптивная система мгновенно переходит в «Красную зону» (0,85), фиксируя критичность репутационной угрозы (10, 11). Статичная модель, где вес репутации остается постоянным (0,35-0,40), сгладила бы этот пик и сохранила бы значение ИИЭБ в диапазоне 0,58-0,62, недооценив масштаб угрозы и упустив окно для оперативного реагирования (PR-кампания, официальные уведомления, инвестиции в кибербезопасность) [11].

Ключевой вывод: на микроуровне методика демонстрирует сокращение показателя «Время выявления угрозы» на 2-4 недели в сравнении со статичными системами. Это позволяет менеджменту переходить от реактивного управления (тушение уже произошедших кризисов) к превентивному управлению рисками (принятие проактивных мер на стадии роста неопределенности) [9].

Сценарии применения в контуре управления. Практическая ценность гибридной АСП раскрывается при сценарном моделировании реакции системы на типовые классы угроз экономической безопасности предприятия. Рассмотрим два репрезентативных сценария, демонстрирующих различие в реакции автоматизированного и экспертного уровней управления (табл. 3) [9].

Выводы из сценарного анализа: приведенные сценарии демонстрируют, что гибридная АСП не заменяет эксперта и не претендует на «полную автономию», а выступает в роли интеллектуального помощника, фокусируя внимание лиц, принимающих решения (ЛПР), на наиболее уязвимых и динамичных участках периметра экономической безопасности [9].

Тактический контур обеспечивает скорость обнаружения угроз и снижение когнитивной нагрузки для ЛПР, а стратегический – глубокий анализ контекста и принятие обоснованных управленческих решений [12, 13]. Синергия этих двух уровней позволяет достичь баланса между автоматизацией и экспертным суждением, который недостижим ни при чистой автоматизации, ни при чистом экспертном подходе.

Сравнительный анализ АСП с альтернативными подходами. Для определения научной новизны и практической значимости разработанной методики проведен сравнительный анализ с существующими решениями, применяемыми в задачах мониторинга экономической безопасности [12, 14, 15]. Альтернативные подходы классифицированы на три группы: теоретические модели (экспертно-адаптивные), корпоративные платформы управления рисками (GRC) и инструменты бизнес-аналитики (BI). Сравнение проводилось по критериям скорости реакции, гибкости архитектуры, интерпретируемости и уровня зависимости от экспертного фактора [15]. Результаты анализа систематизированы в табл. 4.

Таблица 3.

Сценарии реакции гибридной АСП на внешние и латентные угрозы

Параметр	Сценарий 1: Внешний шок (Технологические санкции)	Сценарий 2: Латентная угроза (Риск утечки интеллектуальной собственности)
Триггер	Рост волатильности индикатора TRI (срыв цепочек поставок, запреты на экспорт оборудования, отказы в доступе к критическому ПО) [2, 6].	Корреляция слабых сигналов: аномальная сетевая активность в корпоративной среде + негативные отзывы сотрудников о карьерных перспективах (выявляется через анализ сайтов с отзывами о работодателях, учитывается уровень текучесть персонала) [2, 16].
Реакция (Тактический уровень)	Автоматическое увеличение веса γ (TRI) в структуре ИИЭБ с базового значения 0,30 до 0,45 (в пределах допустимого коридора Δ=0,2). ИИЭБ переходит из «Желтой» в «Красную» зону.	Система детектирует коррелированный паттерн и формирует сигнал для эксперта о необходимости введения нового временного индикатора (Human Resource Risk, HRI), синтезирующего данные SIEM (система управления событиями безопасности), DLP (система предотвращения утечек данных) и HR-систем (система управления кадрами и рекрутингом) [12].
Реакция (Стратегический уровень)	Экспертный комитет по рискам утверждает интерпретацию сигнала. На основе информации о длительности и масштабе санкций принимается решение о пересмотре стратегии: запуск программы поиска альтернативных поставщиков, диверсификация критических компонентов, ускоренная локализация технологических решений [13].	Служба экономической безопасности подключает отдел кадров и ИТ-службу для анализа сигналов. Решение о введении (или нет) показателя HRI принимается на основе оценки вероятности и масштаба потенциального ущерба. В случае подтверждения угрозы — усиление DLP-контроля, проверка истории доступа к критичным активам, переговоры с потенциальными нарушителями [2, 16].
Результат (период реагирования)	ИИЭБ переходит в «Желтую» зону уже за 2–3 недели до фактического наступления критических сбоев поставок, что позволяет запустить превентивные меры и минимизировать ущерб на уровне 10–15% от потенциального (на основе аналогий с отраслевыми кейсами) [6].	Предотвращение непроизошедшего инцидента на стадии подготовки: раннее обнаружение зарождающейся угрозы позволяет изолировать нарушителя и заблокировать несанкционированный доступ до факта утечки. Потенциальный ущерб в виде потери интеллектуальной собственности оценивается в сотни миллионов рублей [11].

Источник: составлено авторами

Таблица 4.

Сравнительный анализ гибридной АСП с альтернативными моделями и платформами

Критерий / Подход	Научные модели (экспертно-адаптивные) [12]	Коммерческие GRC-платформы (SAP, Oracle) [15, 16]	BI-инструменты (Tableau, Power BI) [15]	Предлагаемая Гибридная АСП
Скорость реакции	Низкая. Дискретные циклы пересмотра параметров (раз в квартал/год) создают временной лаг.	Средняя. Автоматизация эффективна только в рамках предопределенных правил и сценариев.	Низкая. Зависит от скорости реакции оператора на визуализированные данные.	Высокая. Тактическая автокалибровка осуществляется в режиме, приближенном к реальному времени.
Гибкость архитектуры	Средняя. Требует созыва экспертной комиссии для внесения изменений.	Низкая. Жестко установленные правила, перенастройка требует участия вендора или дорогостоящей разработки.	Высокая для визуализации, но отсутствует аналитическое ядро.	Высокая. Комбинированные алгоритмы позволяют вводить временные индикаторы и адаптировать модель без перепрограммирования ядра.
Интерпретируемость	Высокая. Базируется на понятной экспертной семантике.	Низкая–средняя. Проприетарные алгоритмы часто функционируют как «черный ящик».	Высокая визуально: наглядная инфографика, но выводы формирует человек.	Высокая. Решения прозрачны: они базируются на статистических метриках и экспертных ограничениях.
Зависимость от эксперта	Критическая. Эксперт является единственным источником адаптации.	Средняя. Зависит от качества настройки администратором системы.	Высокая. Качество анализа полностью зависит от компетенций аналитика.	Сбалансированная. Эксперт задает стратегию и границы безопасности, система берет на себя рутину тактической корректировки.
Требования к данным	Низкие. Работает преимущественно с качественными оценками.	Высокие. Требует интеграции с транзакционными системами (ERP) и логами.	Средние. Требует структурированных источников для построения дашбордов.	Высокие. Для работы алгоритмов необходимы потоковые данные; однако на этапе пилота возможна работа с прокси-метриками.
Технологический суверенитет	Не применимо (концепция).	Низкий. Зависимость от зарубежных лицензий и обновлений.	Средний. Зависит от выбранного стека технологий.	Высокий. Методика реализуема на отечественном / open source (программное обеспечение с открытым исходным кодом) стеке и ориентирована на импортозамещение.

Источник: составлено авторами

Проведенный анализ позволяет сделать вывод, что предложенная методика занимает уникальную нишу, выступая интегративным слоем между источниками данных и системой принятия решений. В отличие от научных концепций, АСП предлагает конкретный математический аппарат для автоматизации рутинных процессов мониторинга, снижая нагрузку на экспертов [10, 12]. В отличие от GRC-платформ, она не ограничена жесткими правилами и способна фиксировать новые паттерны угроз (через анализ аномалий) без дорогостоящей доработки кода [4]. А в отличие от BI-инструментов, АСП содержит формализованное аналитическое ядро, которое генерирует конкретные управленческие сигналы, а не просто визуализирует статистику.

Таким образом, АСП не конкурирует с экспертами или существующим ПО, а интегрирует их сильные стороны, дополняя недостающим элементом – механизмом оперативной адаптивности. Это позволяет достичь баланса между скоростью реакции и смысловой интерпретацией событий, что является критическим требованием в условиях цифровой экономики [9, 14]. Практические аспекты внедрения и ограничения исследования. Внедрение адаптивной системы показателей представляет собой комплексный организационно-технический проект, требующий поэтапной реализации [10]. Основные этапы, задачи и сопряженные с ними вызовы систематизированы в табл. 5.

Ограничения исследования. Эффективность предложенной методики напрямую зависит от уровня цифровой зрелости предприятия [14, 15]. Для компаний с низким уровнем автоматизации (отсутствие ERP, неструктурированные данные) применение тактического контура адаптации будет технически затруднено [16]. Кроме того, предложенные алгоритмы, ориентированные на статистические аномалии, наиболее эффективны для выявления угроз, имеющих цифровой след (волатильность финансовых или операционных показателей) [4]. Для обнаружения принципиально новых, «немеряемых» рисков (политические решения, форс-мажор) требуется сохранение роли экспертного стратегического планирования [13].

В рамках данного исследования апробация методики проведена на открытых и прокси-данных [2, 3], что позволяет подтвердить ее концептуальную работоспособность. При этом следует отметить чувствительность системы к калибровочным параметрам (λ, Z, Δ), оптимальные значения которых зависят от исторического профиля волатильности конкретного предприятия и требуют индивидуальной настройки. Статистические методы, лежащие в основе алгоритмов адаптации, эффективны для выявления угроз в рамках исторического распределения, однако события типа «черный лебедь» (техногенные катастрофы, геополитические шоки) находятся за пределами их прогностических возможностей.

Таблица 5.

Этапы внедрения АСП: задачи и ключевые вызовы

Этап	Ключевые задачи	Ожидаемый результат	Основной вызов (ограничение)
1. Диагностика (4-6 недель)	Аудит источников данных, идентификация ключевых рисков. Формирование экспертной группы, определение базовых весов w_{base} методом парных сравнений (МАИ и др.) [17].	Карта рисков, матрица весов, предварительное ТЭО проекта.	Организационный: необходимость консолидации мнений экспертов из разных функциональных блоков, доступ к данным [12, 13].
2. Проектирование (6-12 недель)	Настройка интеграции с источниками (ETL - процессы извлечения, преобразования и загрузки данных), калибровка параметра чувствительности λ и коридоров адаптации Δ. Разработка прототипа [4].	Прототип (MVP) системы, интеграционные шлюзы к ERP/SIEM, тестовый набор данных.	Технический: качество и доступность исторических данных для обучения и настройки статистических моделей [15, 16].
3. Пилотная эксплуатация (3-6 мес.)	Запуск в режиме «тени» (сигналы без управляющих воздействий), валидация алертов, сбор обратной связи от экспертов [18].	Откалиброванная модель. Метрика успеха: снижение времени на реакцию на ≥ 20% по сравнению с базовым состоянием.	Методологический: риск ложных срабатываний на этапе «холодного старта», необходимость ручной валидации и уточнения параметров Z, λ, ΔZ [4].
4. Масштабирование (постоянно)	Интеграция АСП в контур управления, обучение персонала, регламентация процедур реагирования, регулярный пересмотр параметров [9, 12].	Действующая система мониторинга. Регулярные отчеты и алерты для ЛПР.	Культурный: преодоление недоверия персонала к автоматическим сигналам, формирование культуры data-driven управления [15].

Источник: составлено авторами

Для противодействия таким событиям необходимо сохранение стратегического уровня экспертного суждения с возможностью переопределения автоматических сигналов. Полная валидация методики требует проведения пилотных проектов на реальных внутренних данных предприятий

различных секторов, что является направлением дальнейших исследований автора [10].

Заключение. В рамках проведенного исследования решена актуальная научная задача преодоления управленческой *инертности* систем мониторинга экономической безопасности предприятия в условиях цифровизации. Результаты работы позволяют констатировать, что традиционные статические и экспертно-адаптивные модели, базирующиеся на фиксированных параметрах оценки, теряют эффективность в условиях высокой динамики цифровых угроз, генерируя критические риски запаздывания управленческой реакции.

Теоретическая значимость полученных результатов заключается в развитии положений классической ресурсно-функциональной теории экономической безопасности применительно к специфике цифровой экономики. Обосновано, что проекции защиты ключевых ресурсов предприятия – финансового, репутационно-информационного и технико-технологического – могут быть эффективно оцифрованы через систему динамических индикаторов (FRA, RRI, TRI), что обеспечивает сохранение фундаментального экономического смысла оценки при смене технологического инструментария.

Ключевым элементом научной новизны выступает разработанная методика и архитектура гибридной адаптивной системы показателей (АСП). В работе впервые формализован двухуровневый контур управления, разграничивающий зоны ответственности: стратегический уровень, где эксперт определяет базовые веса w_{base}, параметры толерантности к риску (Z) и границы адаптации (Δ); тактический уровень, обеспечивающий автоматизированную калибровку чувствительности системы на основе статистического анализа волатильности данных. Предложенный математический аппарат гибридного взвешивания и адаптации пороговых значений обеспечивает преемственность экспертной логики, одновременно нивелируя субъективизм оперативных оценок.

Практическая применимость методики подтверждена результатами численного моделирования и ретроспективной апробации на открытых данных ИТ-отрасли России (сборники НИУ ВШЭ) и публичной отчетности ПАО «ВК». Эксперименты подтвердили концептуальную состоятельность подхода: внедрение механизмов тактической адаптации позволяет сократить временной лаг идентификации угроз по сравнению со статичными моделями за счет автоматической фокусировки на индикаторах с нарастающей нестабильностью. При этом доказано, что все автоматические корректировки остаются в пределах ограничений, заданных на стратегическом уровне.

В работе объективно определены методологические границы исследования. Апробация, проведенная на прокси-индикаторах и открытых данных, демонстрирует воспроизводимость методики и корректность работы алгоритмов, однако не заменяет полноценную валидацию на внутренних данных. Полная реализация потенциала системы требует проведения пилотного внедрения с интеграцией в корпоративные ERP/SIEM-системы для проспективной оценки эффективности.

Перспективы дальнейших исследований лежат в плоскости: расширения эмпирической базы для калибровки параметров адаптации (λ,Δ,Z) под отраслевую специфику реального сектора; разработки протоколов интеграции АСП в промышленные GRC-платформы; углубленного изучения механизмов модификации состава индикаторов на основе оценки их информационной ценности.

Полученные результаты формируют методическую основу для качественной трансформации корпоративных систем управления рисками, обеспечивая переход от реактивной фиксации событий к проактивному мониторингу и баланс между скоростью алгоритмической обработки данных и глубиной экспертного анализа.

Поступила в редакцию 11.11.2025
Принята к публикации 12.01.2026

Библиографический список

[1] Митяков Е.С., Луцкан С.П. Адаптивная система показателей мониторинга экономической безопасности предприятия: математическое и численное моделирование // Развитие и безопасность. 2026. № 1. С. 16-33.

[2] Индикаторы цифровой экономики: 2024: статистический сборник / Абашкин В.Л., Абдрахманова Г.И., Вишневский К.О., Гохберг Л.М. и др. М.: ИСИЭЗ ВШЭ, 2024. 276 с.

[3] Отчеты и материалы ПАО «ВК» [Электронный ресурс]. 2025. Режим доступа: https://vk.company/ru/investors/results/ (дата обращения: 20.01.2026).

[4] Tian X., Tian Z., Khatib S.F.A., Wang Y. Machine learning in internet financial risk management: A systematic literature review // PLOS ONE. 2024. Vol. 19. No. 4. Article e0300195.

[5] Ровенская А.В., Воробьева Е.Ю. К вопросу обеспечения экономической безопасности в условиях развития цифровой экономики // ЭФО: Экономика. Финансы. Общество. 2023. № 1 (5). С. 102-114.

[6] Песоцкий А.А. Экономика России против санкционных угроз: взгляд из 2025 года // Общество: политика, экономика, право. 2025. № 4. С. 125-131.

[7] Городецкий А.Е. Экономическая безопасность в условиях глобализации // Экономика и управление. 2018. № 4 (150). С. 45-56.

[8] Банк России. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году [Электронный ресурс]. М.: Банк России, 2024. Режим доступа: https://www.cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf (дата обращения: 20.01.2026).
[9] Deming W.E. Out of the Crisis. Cambridge, MA: MIT Press, 1986. 507 p.
[10] Луцкан С.П. Совершенствование методов сбора и анализа данных для мониторинга экономической безопасности в условиях цифровизации // Инновационная экономика: информация, аналитика, прогнозы. 2025. № 6. С. 181-193.
[11] IBM. Cost of a Data Breach Report 2025 [Electronic resource]. 2025. URL: https://www.ibm.com/reports/data-breach (дата обращения: 20.01.2026).
[12] Митяков Е.С., Митяков С.Н. Адаптивный подход к вычислению обобщенного индекса экономической безопасности // Современные проблемы науки и образования. 2014. № 2. С. 415.
[13] Митяков Е.С. Ключевые элементы методологии и инструментария мониторинга экономической безопасности регионов России // Фундаментальные исследования. 2018. № 8. С. 84-88.
[14] Балог М.М., Бабкин А.В., Гаджиев М.М. Экономическая безопасность в контексте цифровизации: подходы, тенденции и угрозы // Национальные интересы: приоритеты и безопасность. 2024. Т. 20. № 6. С. 1040-1060.
[15] Grima S. (Ed.). Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. Bingley: Emerald Publishing, 2023. 236 p.
[16] Тадвайзер (TAdviser). Искусственный интеллект (рынок России) [Электронный ресурс]. 2024. Режим доступа: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_(рынок_России) (дата обращения: 20.01.2026).
[17] Saaty T.L., Vargas L.G. Decision Making with the Analytic Network Process: Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks. 2nd ed. New York: Springer, 2018. 512 p.
[18] Луцкан С.П. Модель оценки экономической безопасности в эпоху цифровой трансформации экономики // Инновационная экономика: информация, аналитика, прогнозы. 2024. № 5. С. 225-233.

E.S. Mityakov, S.P. Lutskan

ADAPTIVE INDICATOR SYSTEM FOR MONITORING ENTERPRISE ECONOMIC SECURITY: EMPIRICAL VERIFICATION OF THE MODEL

MIREA – Russian Technological University
Moscow, Russia

Abstract. This article continues the discussion presented in the authors' previous publication, which introduced a hybrid adaptive model and an indicator system for monitoring enterprise economic security. The proposed approach separates monitoring parameter management into strategic and tactical loops. The strategic loop relies on expert-de-

fined priorities and permissible parameter ranges, informed by system-generated recommendations, while the tactical loop enables real-time automated calibration within the expert-established boundaries.The methodology was validated at two levels: macro (using data from the Russian information technology sector) and micro (based on public financial reports of PJSC “VK”). A comparative analysis was conducted against alternative academic models and commercial GRC platforms. The feasibility of the proposed architecture was demonstrated through simulation modeling at both levels: macro-level simulations employed Rosstat data on the IT sector interpreted as proxy indicators, while micro-level validation used publicly available reports from PJSC “VK”. Simulation experiments on synthetic and proxy data showed a reduction in time lag for threat identification compared to static indicator-based schemes. The study delivers a reproducible methodology for transitioning toward hybrid, self-tuning risk management tools that balance expert oversight with the speed of automated response. The paper concludes with a discussion of the model’s limitations and suggestions for future research directions.

Keywords: economic security; hybrid monitoring system; adaptive indicator system; composite economic security index; strategic loop; tactical loop; empirical verification.

References

[1] Mityakov, E. S., Lutskan, S. P. (2026). [Adaptive system of indicators for monitoring the economic security of an enterprise: mathematical and numerical modeling]. *Razvitie i bezopasnost* [Development and Security]. No. 1, pp. 16-33. (In Russ.).

[2] Abashkin, V. L., Abdrakhmanova, G. I., Vishnevsky, K. O., Gokhberg, L. M., et al. (2024). *Indikatory tsifrovoi ekonomiki: 2024: statisticheskii sbornik* [Digital Economy Indicators: 2024: Statistical Collection]. Moscow: ISIEZ HSE, 276 p. (In Russ.).

[3] VK Group. (2025). [Reports and materials]. [Electronic resource]. Available at: https://vk.company/ru/investors/results/ (date accessed 20.01.2026).

[4] Tian, X., Tian, Z., Khatib, S. F. A., Wang, Y. (2024). Machine learning in internet financial risk management: A systematic literature review. *PLOS ONE*. Vol. 19, No. 4, Article e0300195.

[5] Rovenskaya, A. V., Vorobieva, E. Yu. (2023). [On ensuring economic security in the context of digital economy development]. *EFO: Ekonomika. Finansy. Obshchestvo* [EFO: Economics. Finance. Society]. No. 1 (5), pp. 102–114. (In Russ.).

[6] Pesotskiy, A. A. (2025). [Russian economy against sanction threats: a view from 2025]. *Obshchestvo: politika, ekonomika, parvo* [Society: Politics, Economics, Law]. No. 4, pp. 125–131. (In Russ.).

[7] Gorodetskiy, A. E. (2018). [Economic security in the context of globalization]. *Ekonomika i upravlenie* [Economics and Management]. No. 4 (150), pp. 45-56. (In Russ.).

[8] Bank of Russia. (2024). [Review of major types of cyberattacks in the financial sector in 2024]. [Electronic resource]. Moscow: Bank of Russia. Available at: https://www.cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf (date accessed 20.01.2026).

[9] Deming, W. E. (1986). *Out of the Crisis*. Cambridge, MA: MIT Press, 507 p.

[10] Lutskan, S. P. (2025). [Improvement of data collection and analysis methods for monitoring economic security in the context of digitalization]. *Innovatsionnaya ekonomika: informatsiya, analitika, prognozy* [Innovative Economy: Information, Analytics, Forecasts]. No. 6, pp. 181–193. (In Russ.).

[11] IBM. (2025). *Cost of a Data Breach Report 2025*. [Electronic resource]. Available at: https://www.ibm.com/reports/data-breach (date accessed 20.01.2026).

[12] Mityakov, E. S., Mityakov, S. N. (2014). [Adaptive approach to calculating the generalized index of economic security]. *Sovremennye problemy nauki i obrazovaniya* [Modern Problems of Science and Education]. No. 2, p. 415. (In Russ.).

[13] Mityakov, E. S. (2018). [Key elements of methodology and tools for monitoring economic security of Russian regions]. *Fundamentalnye issledovaniya* [Fundamental Research]. No. 8, pp. 84–88. (In Russ.).

[14] Balog, M. M., Babkin, A. V., Gadzhiev, M. M. (2024). [Economic security in the context of digitalization: approaches, trends and threats]. *Natsionalnye interesy: prioritety i bezopasnost* [National Interests: Priorities and Security]. Vol. 20, No. 6, pp. 1040–1060. (In Russ.).

[15] Grima, S. (Ed.). (2023). *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management*. Bingley: Emerald Publishing, 236 p.

[16] TAdviser. (2024). [Artificial Intelligence (Russian Market)]. [Electronic resource]. Available at: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_(рынок_России) (accessed: 20.01.2026).

[17] Saaty, T. L., Vargas, L. G. (2018). *Decision Making with the Analytic Network Process: Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks*. 2nd ed. New York: Springer, 512 p.

[18] Lutskan, S. P. (2024). [Economic security assessment model in the era of digital transformation of the economy]. *Innovatsionnaya ekonomika: informatsiya, analitika, prognozy* [Innovative Economy: Information, Analytics, Forecasts]. No. 5, pp. 225–233. (In Russ.).