УДК 338.14 ***EDN ODZHPI***

Е.С. Митяков, С.П. Луцкан

АДАПТИВНАЯ СИСТЕМА ПОКАЗАТЕЛЕЙ МОНИТОРИНГА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: МАТЕМАТИЧЕСКОЕ И ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ

МИРЭА – Российский технологический университет
Москва, Россия

Выявлена проблема управленческой инертности традиционных систем мониторинга экономической безопасности предприятия. Обосновано, что в условиях высокой динамичности и неопределенности цифровой среды статичность параметров оценки экономической безопасности, фиксируемых на длительный период, приводит к критическому запаздыванию реакции на возникающие угрозы. Предложены методика и архитектура гибридной адаптивной системы показателей, использующей интегральный индекс экономической безопасности предприятия в качестве управляющего сигнала. Научный вклад исследования заключается в разработке двухуровневой модели, разделяющей 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: гибридного динамического взвешивания (сочетание экспертно заданных базовых весов и их автоматизированной корректировки в пределах допустимых диапазонов), адаптации пороговых значений и калибровки через ретроспективное тестирование. Проведено численное моделирование на синтетических данных, которое подтвердило способность системы работать в режиме «автопилота» при возникновении тактических угроз: она временно фокусируется на проблеме, а после ее устранения самостоятельно возвращается к базовым настройкам.

Ключевые слова: экономическая безопасность; мониторинг; гибридная система мониторинга; адаптивная система показателей; управленческая инертность; интегральный индекс экономической безопасности; стратегический контур; тактический контур.

Введение. В современной экономической науке обеспечение экономической безопасности (ЭБ) предприятия традиционно рассматривается через призму ресурсно-функционального подхода как состояние защищенности его жизненно важных интересов и ресурсного потенциала от внутренних и внешних угроз, обеспечивающее устойчивость функционирования и развитие предприятия [1, 2]. Однако в условиях перманентной мак-

роэкономической нестабильности и ускоряющейся цифровизации проблема эффективного мониторинга этого состояния приобретает принципиально новое звучание [3]. Цифровая среда не только порождает новые виды экономических рисков, но и трансформирует сам характер их проявления: скорость реализации угроз возрастает на порядки, что снижает ценность традиционной ретроспективной отчетности [4, 5]. Данные о финансовом и операционном состоянии предприятия нередко устаревают еще до того, как попадают в аналитические контуры управления. Это приводит к функциональному разрыву: системы мониторинга, эффективные в условиях стабильности, оказываются несостоятельными перед лицом высокочастотных угроз, требующих реакции в режиме, приближенном к реальному времени [6, 7].

Научные исследования в данной области прошли значительный эволюционный путь. От анализа отдельных показателей исследователи перешли к построению архитектуры сбалансированных систем и интегральных индексов, агрегирующих данные из различных функциональных сфер. В ряде работ были заложены концептуальные основы для адаптивных подходов к их расчету [8]. В рамках развития данного направления автором ранее были разработаны собственная интеграционная модель оценки [9] и методика расчета интегрального индекса экономической безопасности (ИИЭБ), базирующаяся на гибридной архитектуре сбора данных [10]. Данные исследования позволили сформировать диагностический базис системы мониторинга экономической безопасности предприятия и продемонстрировали потенциал интеграции гетерогенных источников данных [11].

Вместе с тем, практическая реализация накопленного теоретического потенциала сталкивается с проблемой управленческой инертности. В настоящее время роль эксперта остается ключевой, при этом его участие ограничено достаточно редкими сессиями пересмотра настроек, тогда как сами риски формируются и эволюционируют существенно быстрее. Перекалибровка моделей осуществляется в режиме «ручного управления» и требует значительных временных затрат. В условиях, когда значимость индикатора (например, технологического риска) может кардинально измениться в течение нескольких дней под влиянием внешнего шока, возникает критический разрыв между динамикой генерации цифровых рисков и скоростью адаптации системы мониторинга [4].

Целью настоящего исследования является разрешение данного противоречия через разработку методики и архитектуры гибридной адаптивной системы показателей (АСП). В отличие от существующих подходов, предлагаемая концепция предполагает создание двухуровневой модели управления, разделяющей контур мониторинга на стратегический (экспертное определение приоритетов) и тактический (автоматическая калибровка в реальном времени) [12]. Для достижения поставленной цели в работе последовательно решается ряд взаимосвязанных задач: формулиру-

ются принципы построения системы мониторинга с учетом трансформации угроз экономической безопасности предприятия; проводится математическая формализация механизмов двухуровневой адаптации; выполняется сравнительный анализ предложенного подхода с альтернативными моделями; осуществляется имитационное моделирование работы алгоритмов и демонстрация применимости методики на макроэкономических (данные Росстата по отрасли ИКТ [5]) и микроэкономических (открытая отчетность ПАО «ВК» [13]) данных, интерпретированных в качестве прокси-индикаторов.

Анализ существующих подходов к мониторингу экономической безопасности: от статики к гибридной адаптивности. Эволюция инструментария мониторинга ЭБ неразрывно связана с изменением ландшафта угроз, влияющих на устойчивость и развитие предприятия, а также на состояние его финансовой, информационной и технико-технологической составляющих [1, 2]. В условиях цифровой экономики, характеризующейся высокой волатильностью рынков, появлением киберрисков и сокращением жизненных циклов бизнес-процессов, требования к системам мониторинга трансформируются [3, 4]. Анализ отечественной и зарубежной литературы, а также практики корпоративного управления, позволяет выделить три основных эволюционных этапа развития систем мониторинга, каждый из которых обладает специфическими достоинствами и ограничениями [8, 14].

Исторически первым и наиболее распространенным подходом является использование фиксированных наборов индикаторов с нормативно заданными пороговыми значениями [15]. Данный подход, базирующийся на традиционном финансовом анализе (модели банкротства Э. Альтмана, Р. Таффлера и др.) и нормативных требованиях регуляторов, предполагает сравнение текущих показателей предприятия с жестко заданными константами (например, коэффициент текущей ликвидности больше 2) [16].

Среди достоинств данного подхода выделяются простота интерпретации, методологическая прозрачность, возможность межотраслевого сравнения. Ключевым ограничением является ретроспективный характер анализа. Финансовая отчетность фиксирует уже реализовавшиеся риски, не позволяя идентифицировать угрозу на стадии зарождения [17]. Кроме того, статические пороги не учитывают индивидуальную специфику предприятия и фазу экономического цикла. Следует отметить, что в контексте экономической безопасности подобные модели обеспечивают преимущественно диагностику финансовой составляющей экономической безопасности предприятия, оставляя за рамками репутационные, технологические и информационные риски [18].

В современной российской экономической науке активно развивается направление, признающее необходимость адаптации параметров мониторинга. В работах ряда исследователей обоснована необходимость перио-

дического пересмотра весовых коэффициентов индикаторов и пороговых значений в зависимости от внешних условий [8]. Данный подход можно охарактеризовать как экспертно-адаптивный. Адаптация здесь происходит дискретно: экспертная группа (например, комитет по рискам) собирается с определенной периодичностью (квартал, год), анализирует макроэкономическую ситуацию и директивно меняет настройки модели.

Наряду с высоким качеством семантического анализа при использовании научного подхода, отмечается также возможность учета неформализуемых факторов и стратегическая глубина оценки. Главным уязвимым местом является управленческая инертность. Временной лаг между изменением профиля угроз (например, введением санкций или началом кибератаки) и моментом пересмотра параметров экспертами может составлять месяцы. В условиях цифровизации, когда ущерб может быть нанесен за часы, такая латентность становится критической [14].

На корпоративном уровне крупный бизнес внедряет автоматизированные системы класса GRC (Governance, Risk, and Compliance, системы управления рисками в сфере соблюдения нормативных требований) – решения от SAP, Oracle, IBM [19]. Данные системы реализуют непрерывный мониторинг индикаторов на основе заданных правил. Таким образом, достигается высокая степень автоматизации, реализуется возможность работы с большими данными и обеспечивается интеграция с бизнес-процессами.

При этом внедрение указанных систем сопряжено с высокой стоимостью развертывания и обслуживания. Также актуальной является и т.н. проблема «черного ящика». Алгоритмы проприетарных систем часто закрыты для пользователя, а логика настройки правил и порогов ограничена рамками встроенных конфигураций, что затрудняет учет специфики отдельных предприятий и быстро меняющихся угроз [19]. Кроме того, большинство промышленных GRC-решений ориентированы на комплаенс и регуляторные требования и лишь косвенно затрагивают комплексную экономическую безопасность предприятия [14].

Обоснование необходимости гибридного подхода. Проведенный анализ показывает, что ни один из существующих подходов не решает задачу эффективного мониторинга в условиях высокой неопределенности в полной мере [3, 10]. Наблюдается поляризация методов: либо «медленная» экспертная оценка, либо «быстрая», но часто поверхностная или ригидная автоматизация. Решение проблемы видится в конвергенции подходов – создании гибридной АСП.

Суть предлагаемого подхода заключается в разделении контура управления на два уровня.

1. *Стратегический уровень* (экспертный): задает вектор мониторинга. Эксперты определяют структуру интегрального индекса, базовые прио-

ритеты (веса) и, что критически важно, устанавливают границы допустимой адаптации для автоматизированных механизмов.

2. *Тактический уровень* (автоматизированный): обеспечивает оперативную подстройку. Алгоритмы анализируют поток данных в режиме, приближенном к реальному времени, уточняют пороговые зоны и формируют предложения по корректировке весов внутри границ, заранее заданных экспертами [12].

В табл. 1 дан анализ подходов к построению систем мониторинга экономической безопасности.

Таблица 1.

Сравнительный анализ подходов к построению систем мониторинга экономической безопасности

Критерий сравнения	**Статическая индикаторная система**	**Экспертно-адаптивная система**	**Коммерческие GRC-платформы**	**Предлагаемая гибридная АСП**
Основной принцип	Сравнение факт/план с фиксированными нормативами	Периодический пересмотр параметров экспертной группой	Непрерывный мониторинг на основе жестких правил	Двухуровневое управление: стратегическая верификация + тактическая автокалибровка
Роль эксперта	Определяет нормативы единожды на этапе создания	Периодически (дискретно) актуализирует веса и пороги	Пользователь системы (получает отчеты), настройка требует высокой квалификации персонала	Архитектор системы: задает базовые приоритеты и границы допустимой адаптации [8]
Механизм адаптации	Отсутствует (параметры статичны)	Дискретный, реактивный (по факту осознания изменений)	Параметрический (требует ручного переписывания правил)	Непрерывный, превентивный: корректировка на основе анализа динамики индикаторов [12]
Скорость реакции	Низкая (по факту выхода отчетности)	Средняя (зависит от частоты заседаний комитета)	Высокая (на известные типы угроз)	Высокая (режим, приближенный к реальному времени) [5]
Ключевое ограничение	«Эффект зеркала заднего вида»	Субъективизм и высокая инертность	Высокая стоимость, сложность адаптации	Зависимость от качества данных и цифровой зрелости [19]

Источник: составлено авторами.

Как следует из таблицы, предлагаемая гибридная АСП заполняет пространство между академическими экспертными моделями (глубокими, но медленными) и техническими средствами мониторинга (быстрыми, но шаблонными) [3, 8, 14]. Она позволяет сохранить экономический смысл оценки, обеспечиваемый экспертами, придав ему необходимую в цифровой среде динамичность.

Архитектура и алгоритм функционирования гибридной адаптивной системы показателей. Переход от статичных систем мониторинга к адаптивным требует разработки новой концептуальной основы, способной преодолеть ограничения управленческой инертности при сохранении экономического смысла оценки [1, 2]. Предлагаемая гибридная АСП представляет собой не просто набор индикаторов, а динамическую саморегулируемую среду, функционирующую как контур проактивного управления с обратной связью. В отличие от традиционных подходов, где параметры системы меняются дискретно и вручную, АСП способна в автоматизированном режиме корректировать чувствительность инструментов мониторинга, оставаясь в границах, заранее очерченных экспертами на стратегическом уровне [8, 12].

Центральным элементом, запускающим механизмы адаптации, выступает ИИЭБ предприятия. Отклонение данного индекса, а также составляющих его частных индикаторов, от динамических пороговых значений служит ключевым управляющим сигналом, инициирующим перекалибровку системы [5]. Методический подход к формированию индекса развивает положения ресурсно-функциональной теории экономической безопасности [1, 2], согласно которой уровень защищенности предприятия определяется состоянием его ключевых ресурсов и функциональных подсистем, каждая из которых в цифровой среде подвергается специфическим рискам.

Агрегирование разнородных сигналов в единый показатель осуществляется посредством аддитивной свертки динамических параметров:

$$I_{EBS}=\alpha\cdot FRA+\beta\cdot RRI+\gamma\cdot TRI$$

где FRA (Financial Risk Assessment) – индикатор финансовой устойчивости; RRI (Reputational Risk Index) – индикатор репутационно-информационной безопасности; TRI (Technological Risk Indicator) – индикатор технико-технологической устойчивости.

FRA интерпретируется как финансовая составляющая экономической безопасности предприятия. В отличие от классических моделей, опирающихся только на статические коэффициенты (ликвидности, рентабельности, долговой нагрузки), в АСП данный индикатор формируется на основе анализа временных рядов ключевых финансовых показателей [16]. Первичным шагом выступает расчет нормированных коэффициентов, привязанных к пороговым значениям, рекомендованным в теории финансового анализа и нормативных документах. Далее реализуется модуль выявления

статистических аномалий, который позволяет фиксировать отклонения траектории денежных потоков от исторически сложившейся «нормы» еще до возникновения формального кассового разрыва [20].

RRI отражает информационно-репутационную составляющую экономической безопасности и служит прокси-метрикой состояния нематериальных активов предприятия [17]. В цифровой среде информационные атаки и негативные информационные кампании нередко предшествуют ухудшению финансовых показателей, росту стоимости заимствований и потере ключевых клиентов [4]. В гибридной модели RRI формируется на основе агрегированного анализа тональности информационного поля (новостные публикации, публичные сообщения в соцмедиа и др.) в сочетании с экспертной оценкой значимости отдельных событий (например, крупных судебных дел или резонансных утечек данных) [5]. На этапе обработки текста выполняются очистка и нормализация, устранение дублей, фильтрация по релевантности объекту мониторинга (организация/бренд), после чего тональность/негативность сообщения оценивается нейросетевой моделью класса BERT, адаптированной для русского языка (RuBERT) и дообученной на задаче классификации тональности. Далее значение RRIt агрегируется по скользящему окну как функция доли негативных сообщений, интенсивности упоминаний и веса источника/охвата, что позволяет переводить неструктурированный текстовый поток в числовой временной ряд, пригодный для последующего взвешивания и сравнения с пороговыми зонами [20].

TRI соответствует технико-технологической составляющей экономической безопасности. Он характеризует способность предприятия поддерживать непрерывность основных процессов в условиях киберугроз и технологических сбоев. Индикатор агрегирует данные о частоте и длительности простоев критически важных систем, количестве значимых киберинцидентов, уровне зависимости от импортных компонентов и уязвимости производственной инфраструктуры [5, 18]. Для повышения чувствительности используется предиктивный анализ исторических данных о сбоях и инцидентах [21].

Параметры α, β, γ являются адаптивными весовыми коэффициентами, которые в гибридной модели определяются комбинированным методом. На стратегическом уровне базовые веса $(\alpha_{base}, \beta_{base}, \gamma_{base})$ задаются экспертами с применением метода анализа иерархий (МАИ, Т. Саати) [16] либо других процедур согласования мнений, что обеспечивает согласование структуры индекса с приоритетами предприятия и логикой классической теории экономической безопасности [1, 2]. На тактическом уровне система анализирует динамику частных индикаторов (устойчивость тренда, частоту выходов за пороговые значения, масштаб отклонений) и в автоматизированном режиме предлагает корректировки весов в рамках заранее установ-

ленных допустимых интервалов (например, ±20 % от базовых значений) [8]. Архитектурно предлагаемая система является аналитической надстройкой над гибридной моделью сбора данных и реализует принцип непрерывного совершенствования, известный в теории менеджмента как цикл Шухарта–Деминга (PDCA – Планирование, Действие, Контроль, Корректировка) [12]. Адаптация данного классического управленческого цикла к задачам риск-менеджмента позволяет структурировать процесс мониторинга в виде четырех взаимосвязанных функциональных контуров, концептуально приведенных на рис. 1.

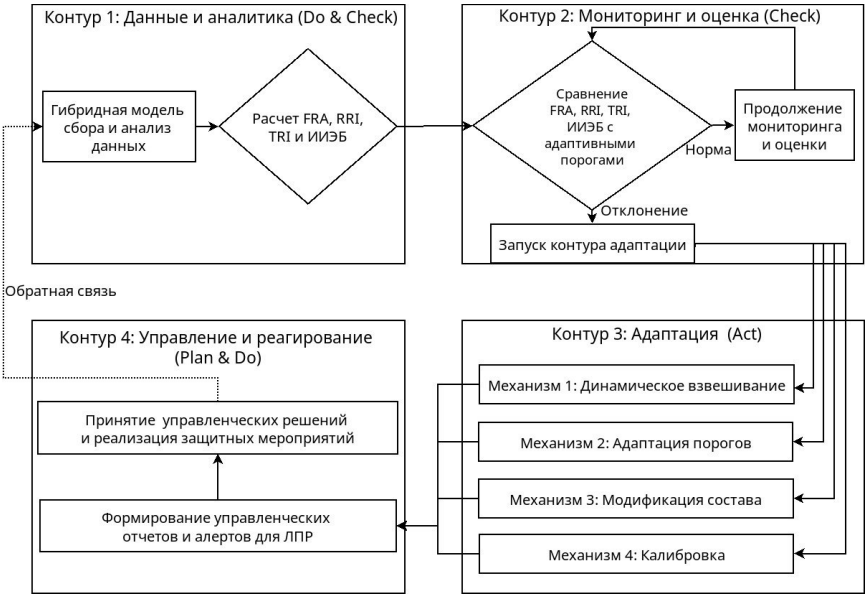

Рис 1. Архитектура и контуры функционирования адаптивной системы показателей

Источник: составлено авторами.

Функционирование системы начинается в контуре «Данные и аналитика» (этап Do), который выступает информационным фундаментом всей архитектуры. На данном этапе обеспечивается непрерывный сбор данных из гетерогенных источников: внутренних информационных систем предприятия (ERP – планирование ресурсов предприятия), CRM – управление взаимоотношениями с клиентами), системы мониторинга ИТ-инфраструктуры [21]), а также внешних источников (официальная статистика, отраслевые обзоры, медиапространство). Здесь же реализуется первичный расчет частных индикаторов FRA, RRI, TRI с заданной периодич-

ностью (день, неделя, квартал), определяемой спецификой предприятия и доступностью данных [10].

Полученные значения передаются во второй контур «Мониторинг и оценка» (этап Check), выполняющий функцию основного сенсора системы. В этом контуре осуществляется непрерывное сопоставление текущих значений ИИЭБ и частных индикаторов с динамическими пороговыми зонами, классифицируемыми как «зеленая», «желтая» и «красная» [8]. Пороговые значения формируются не как фиксированные константы, а как статистически обоснованные «коридоры нормы», определяемые на основе скользящего среднего и стандартного отклонения каждого индикатора с учетом заданного коэффициента толерантности к риску [20]. Важной особенностью архитектуры является параллельный мониторинг как обобщенного индекса, так и отдельных составляющих, что предотвращает «эффект усреднения», когда критический рост одного рискового фактора может быть замаскирован стабильностью других.

При устойчивом нахождении показателей в зоне «нормы» система функционирует в штатном режиме. При переходе ИИЭБ или частных индикаторов в «желтую» или «красную» зоны активируется третий контур «Адаптация» (этап Act), представляющий собой интеллектуальное ядро системы. Ключевое преимущество гибридного подхода – двухуровневое регулирование параметров мониторинга.

1. Тактический уровень: алгоритмы, опираясь на анализ динамики и статистических характеристик индикаторов (усиление волатильности, увеличение частоты выходов за пороги, накопление аномалий), автоматически уточняют границы пороговых значений и формируют предложения по корректировке весовых коэффициентов в пределах допустимых интервалов.

2. Стратегический уровень: в случае выявления структурных сдвигов (изменение бизнес-модели, появление новых типов угроз, пересмотр нормативной базы), инициируется экспертная верификация настроек системы.

Замыкающий четвертый контур «Управление и реагирование» (этап Plan/Do) транслирует результаты работы системы в формат управленческих решений для лиц, принимающих решения [12]. На данном этапе формируются аналитические отчеты, визуализации и сигналы (алерты), ранжированные по уровню критичности и привязанные к конкретным областям ответственности (финансы, ИТ, служба безопасности, PR). Принятые управленческие меры по минимизации рисков изменяют состояние защищаемого объекта, что фиксируется на новом витке цикла сбора и анализа данных. Таким образом, замыкается контур обратной связи, а система со временем накапливает «опыт», повышая точность и прогностическую ценность мониторинга.

Математическая формализация механизмов адаптации параметров мониторинга. Реализация тактического контура управления в рамках предложенной архитектуры требует разработки формализованного математического аппарата, позволяющего алгоритмизировать процессы принятия решений о корректировке параметров системы. В отличие от «черного ящика» нейросетевых моделей или коммерческих GRC-систем, предлагаемый подход базируется на методах статистического анализа временных рядов, что обеспечивает интерпретируемость результатов и возможность верификации логики адаптации со стороны экспертного сообщества [20].

Ключевыми элементами математической модели выступают алгоритм гибридного динамического взвешивания и методика расчета адаптивных пороговых значений [8].

Алгоритм гибридного динамического взвешивания. Фундаментальная проблема статических моделей заключается в фиксации значимости индикаторов ($w_i=const$) без учета текущей фазы жизненного цикла угрозы [15]. Для устранения данного недостатка разработан алгоритм, корректирующий экспертные веса пропорционально росту неопределенности (волатильности) фактора, но строго в пределах допустимого коридора варьирования.

Расчет динамического веса i-го индикатора в момент времени t осуществляется в три этапа.

На первом этапе вычисляется коэффициент тактической коррекции $K_{adj,i,t}$, отражающий отклонение текущей волатильности индикатора от его нормального (исторического) уровня. В качестве меры волатильности используется стандартное отклонение $\sigma_{i,t}$, рассчитанное в скользящем окне шириной N периодов с исключением единичных выбросов, не подтвержденных в последующих наблюдениях (фильтрация «шумовых» всплесков) [20]:

$$K_{adj,i,t}=1+\lambda\cdot\left(\sigma_{i,t}-\sigma_{i,med}\right)/\sigma_{i,med}$$

где $\sigma_{i,t}$ – текущее стандартное отклонение i-го индикатора; $\sigma_{i,med}$ – медианное значение стандартного отклонения (характеристика «спокойного» состояния системы); λ – коэффициент чувствительности модели (параметр адаптивности), определяющий скорость реакции системы на рост дисперсии данных [5].

Параметр $\sigma_{i,med}$ вычисляется как медиана скользящего стандартного отклонения на базовом историческом периоде T_{base} = 252 дня (один финансовый год).

Значение λ задается экспертно на стратегическом уровне. Диапазон $0,1\leq\lambda\leq0,5$ выбран как компромисс между чувствительностью и устойчивостью. Таким образом, корректирующий коэффициент реагирует не на слу-

чайные одиночные всплески, а на устойчивое отклонение дисперсии индикатора от его «спокойного» состояния.

На втором этапе производится предварительный расчет корректированного веса $\widetilde{w}_{i,t}$

$$\widetilde{w}_{i,t}=w_{base,i}\cdot K_{adj,i,t}$$

На третьем этапе реализуется ключевой принцип гибридного управления – наложение ограничений. Полученный вес не должен выходить за пределы доверительного интервала, установленного экспертами:

$$w_{i,t}=clamp(\widetilde{w}_{i,t},w_{base,i}\cdot(1-\Delta),w_{base,i}\cdot(1+\Delta))$$

где Δ – параметр допустимой глубины адаптации (например, $\Delta=0,2$), соответствующий коридору изменения весов ±20% от базовых значений. Финальные веса $w_{i,t}$ нормируются так, чтобы их сумма равнялась единице.

Для повышения интерпретируемости механизма динамического взвешивания дополнительно применяется контур объяснения, который проверяет, согласуется ли рост/снижение весов $w_{i,t}$ с фактическим вкладом частных индикаторов FRA, RRI, TRI в ухудшение ИИЭБ. В качестве базового инструмента используются интерпретируемые модели (ансамбли деревьев решений), позволяющие оценить важность признаков (feature importance) и получить локальные объяснения (например, SHAP) для конкретного момента времени *t*. Результаты данного контура не подменяют формулу, а используются как механизм контроля качества и как основание для управленческого комментария: «почему система усилила репутационный/технологический/финансовый блок» [20, 21].

Методика расчета адаптивных пороговых значений. Для перехода от дискретных нормативных констант к динамическим зонам контроля применяется вероятностный подход, основанный на анализе статистического распределения значений индикаторов [20]. Границы зон мониторинга формируются как функции от тренда (скользящего среднего) и меры рассеяния (стандартного отклонения) временного ряда.

Верхняя $T_{upper,t}$ и нижняя $T_{lower,t}$ границы коридора «нормы» (Зеленой зоны) в момент времени *t* определяются следующим образом:

$$T_{upper,t}=\mu_t+Z\cdot\sigma_t$$
$$T_{lower,t}=\mu_t-Z\cdot\sigma_t$$

где μ_t – скользящее среднее значение индикатора за период *N* (характеризует текущий тренд); σ_t – скользящее стандартное отклонение; *Z* – коэффициент толерантности к риску.

Экономический смысл параметра *Z* заключается в регулировании уровня консерватизма системы. При *Z*=2 (соответствует доверительной вероятности 95 % при нормальном распределении) система интерпретирует как угрозу только отклонения за рамки естественной вариабельности бизнес-процесса [20]. Значение *Z* устанавливается на стратегическом уровне: для TRI – более жесткие границы (*Z*=1,5), для FRA и RRI – более широкие (*Z*=3). Выход значения индикатора за пределы $T_{upper/lower}$ является

триггером для перехода системы в режим «Тревога» и инициации управляющих воздействий [12].

Представленный математический аппарат формирует прозрачную логику функционирования тактического контура АСП. С одной стороны, использование статистических метрик μ и σ обеспечивает объективность и повторяемость процедур адаптации [20]. С другой стороны, наличие параметров-ограничителей Δ, Z и базовых весов w_{base}, задаваемых экспертами на стратегическом уровне, закрепляет за человеком право окончательного определения структуры и «жесткости» системы мониторинга [2, 8].

Циклический алгоритм функционирования адаптивной системы показателей. Интеграция описанных выше архитектурных контуров и математических моделей в единый процесс формирует циклический алгоритм функционирования АСП. В отличие от линейных процедур внедрения систем безопасности, данный алгоритм описывает постоянно действующий операционный цикл, обеспечивающий проактивный характер мониторинга [12]. В соответствии с приведенным ранее описанием, алгоритм представляет собой контур управления с обратной связью, реализующий модель PDCA (Plan-Do-Check-Act), адаптированную для задач мониторинга экономической безопасности в условиях высокой динамики угроз [12].

Основные этапы операционного цикла и распределение функций между автоматизированными и экспертными механизмами отражены в табл. 2. Представленный алгоритм обеспечивает непрерывность работы АСП и ее постоянное самосовершенствование [12]. После завершения Шага 6 (калибровка) или Шага 5 (оперативное реагирование) система с обновленными параметрами возвращается к Шагу 1, замыкая цикл непрерывного мониторинга. Накопление статистической базы на последовательных витках цикла PDCA позволяет постепенно повышать точность прогностических оценок и снижать долю ложных срабатываний [20]. При этом реализация Шагов 5 и 6 с обязательным участием эксперта гарантирует, что автоматическая адаптация не приведет к утрате экономического смысла модели, обеспечивая синергию скорости алгоритмов и глубины экспертного анализа [2, 8]. Этапы Check–Act в цикле PDCA дополняются процедурой обратной проверки (backtesting): после каждого реализовавшегося негативного события система ретроспективно оценивает, был ли сформирован предупредительный сигнал до момента наступления инцидента. При выявлении пропуска или избыточных ложных срабатываний запускается перекалибровка параметров адаптивных механизмов (веса, пороговые границы, параметры окна) на исторических данных. Для исключения переобучения используется валидация на отложенных интервалах (walk-forward), что обеспечивает воспроизводимость качества мониторинга во времени [20, 21].

Таблица 2.

Циклический алгоритм функционирования Гибридной АСП

Шаг	Название этапа	Ключевые действия	Уровень управления / Механизмы
1	Сбор и расчет (Do)	Непрерывный сбор данных из гетерогенных источников. Нормирование и расчет текущих значений ИИЭБ и частных индикаторов (FRA, RRI, TRI) [5]	Автоматический. Контур 1: Данные и Аналитика
2	Оценка состояния (Check)	Сравнение текущих значений с динамическими пороговыми зонами («Зеленая», «Желтая», «Красная»), рассчитанными на основе скользящего среднего μ_t и стандартного отклонения σ_t с учетом коэффициента толерантности к риску Z [8]	Автоматический. Контур 2: Мониторинг и Оценка (Механизм 2)
3	Идентификация режима (Check)	Определение режима функционирования системы: «Штатный» (все в норме), «Внимание» (рост волатильности), «Тревога» (выход за порог) [20]	Автоматический. Контур 2: Мониторинг и Оценка
4	Тактическая адаптация (Act)	При режимах «Внимание» или «Тревога»: запуск алгоритма расчета предложений по корректировке весов $w_{i,t}$ в пределах допустимого коридора Δ [9, 10]	Гибридный (Тактический). Контур 3: Адаптация (Механизм 1)
5	Управленческое реагирование (Plan)	Генерация отчетов и алертов для ЛПР. Принятие решений по купированию угрозы (хеджирование, смена поставщика, PR-реакция) [12]	Экспертный. Контур 4: Управление и Реагирование
6	Стратегическая калибровка (Act)	Периодически или после инцидента: ретроспективное тестирование на исторических и инцидентных данных. Оценка адекватности базовых весов w_{base}, параметра Z и состава индикаторного набора [2, 8]	Гибридный (Стратегический). Контур 3: Адаптация (Механизм 3)

Источник: *составлено авторами*.

Численное моделирование работы механизмов адаптации. Для демонстрации работоспособности математического аппарата тактического контура было проведено численное моделирование на синтетических данных. Эксперимент призван визуализировать реакцию алгоритма гибридного взвешивания на внезапный внешний шок при заданных экспертных ограничениях.

Были сгенерированы три временных ряда, имитирующих динамику частных индикаторов (FRA, RRI, TRI) на горизонте 100 временных шагов

(условных дней). Базовое состояние: Временные ряды имеют нормальное распределение с низкой волатильностью (σ<0,1), что соответствует штатному режиму функционирования предприятия. Инцидент: На 70-й день в ряд индикатора репутационного риска (RRI) искусственно внесен аномальный всплеск (рост амплитуды колебаний), имитирующий информационную атаку – целенаправленный вброс негатива в медиапространство. Настройки АСП: Базовые веса установлены экспертно: $w_{base}(FRA)$=0,35, $w_{base}(RRI)$=0,35, $w_{base}(TRI)$=0,30. Параметр допустимой глубины адаптации установлен на уровне Δ=0,5 (широкий коридор для стресс-теста), что позволяет весам отклоняться до ±50% от номинала.

Результаты моделирования приведены на рис. 2.

Рис. 2. Визуализация сгенерированных временных рядов

Источник: составлено авторами.

Результаты реакции системы на смоделированный инцидент представлены в табл. 3.

Таблица 3.

Результаты численного моделирования адаптации весовых коэффициентов

Веса / Время	Волатильность FRA (σ)	Волатильность RRI (σ)	Волатильность TRI (σ)	Вес FRA (α), %	Вес RRI (β), %	Вес TRI (γ), %
69 дней (до атаки)	0,05	0,06	0,04	33,1	35,8	31,1
70 дней (пик атаки)	0,05	0,25	0,04	24,5	53,5	22,0
90 дней (стабилизация)	0,05	0,07	0,04	32,8	36,4	30,8

Источник: составлено авторами.

В период с 1-го по 69-й шаг система функционировала в стационарном режиме, веса колебались незначительно вокруг базовых значений. На 70-й день (начало атаки) волатильность индикатора RRI резко возросла (с 0,06 до 0,25) [20].

Срабатывание тактического контура.

1. *Детекция*: алгоритм зафиксировал статистическую аномалию в канале RRI.

2. *Адаптация*: механизм динамического взвешивания (Механизм 1) начал повышать значимость репутационного фактора, чтобы сфокусировать внимание системы на источнике угрозы.

3. *Ограничение*: вес RRI вырос с 35,8 до 53,5 %. Важно, что, несмотря на продолжающийся рост волатильности, вес не превысил критических значений (не стал монопольным), так как сработал механизм экспертных ограничений. Система перераспределила приоритеты, снизив веса «спокойных» факторов (FRA и TRI), но сохранила контроль над ними.

Рост веса RRI (и, как следствие, его вклада в интегральный индекс) привел к тому, что ИИЭБ превысил адаптивный порог и сгенерировал сигнал «Тревога» значительно раньше, чем это сделала бы статичная модель [10]. После имитации принятия управленческих мер (шаги 76-89) негативный информационный фон снизился. Как видно из табл. 3 (шаг 90), по мере падения волатильности RRI механизм адаптации автоматически вернул весовые коэффициенты к сбалансированным значениям (вес RRI снизился до 36,4 %).

Таким образом, моделирование подтверждает способность системы работать в режиме «автопилота» при возникновении тактических угроз: она временно фокусируется на проблеме, а после ее устранения самостоятельно возвращается к базовым настройкам, не требуя ручной перекалибровки.

Поступила в редакцию 11.11.2025
Принята к публикации 21.12.2025

Библиографический список

[1] Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. 1994. № 12. С. 4-13.

[2] Бекасова Е.Н. Практический подход в экспертной оценке экономической безопасности предприятия // Экономика и бизнес: теория и практика. 2021. № 8 (78). С. 9-13.

[3] 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.

[4] 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).
[5] Индикаторы цифровой экономики: 2024: статистический сборник / В.Л. Абашкин и др. М.: ИСИЭЗ ВШЭ, 2024. 276 с.
[6] Песоцкий А.А. Экономика России против санкционных угроз: взгляд из 2025 года // Общество: политика, экономика, право. 2025. № 4. С. 125-131.
[7] 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.
[8] Митяков Е.С., Митяков С.Н. Адаптивный подход к вычислению обобщенного индекса экономической безопасности // Современные проблемы науки и образования. 2014. № 2. С. 415.
[9] Луцкан С.П. Модель оценки экономической безопасности в эпоху цифровой трансформации экономики // Инновационная экономика: информация, аналитика, прогнозы. 2024. № 5. С. 225-233.
[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] Митяков Е.С. Ключевые элементы методологии и инструментария мониторинга экономической безопасности регионов России // Фундаментальные исследования. 2018. № 8. С. 84-88.
[12] Deming W.E. Out of the Crisis. Cambridge, MA: MIT Press, 1986. 507 p.
[13] Отчеты и материалы ПАО «ВК» [Электронный ресурс]. 2025. Режим доступа: https://vk.company/ru/investors/results/ (дата обращения: 20.01.2026).
[14] Grima S. (Ed.). Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. Bingley: Emerald Publishing, 2023. 236 p.
[15] Городецкий А.Е. Экономическая безопасность в условиях глобализации // Экономика и управление. 2018. № 4 (150). С. 45-56.
[16] 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.
[17] IBM. Cost of a Data Breach Report 2025 [Electronic resource]. 2025. URL: https://www.ibm.com/reports/data-breach (дата обращения: 20.01.2026).
[18] Самойлов М.А., Кондрашова Н.Г. Взаимосвязь экономической и информационной безопасности российской организации // Экономика и бизнес: теория и практика. 2023. № 10-2 (104). С. 132-134.
[19] 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).
[20] 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.
[21] Chen P., Ji M. Deep learning-based financial risk early warning model for listed companies: A multi-dimensional analysis approach // Expert Systems with Applications. 2025. Vol. 283. Article 127746.

E.S. Mityakov, S.P. Lutskan

ADAPTIVE INDICATOR SYSTEM FOR MONITORING ENTERPRISE ECONOMIC SECURITY: MATHEMATICAL AND NUMERICAL MODELING

MIREA – Russian Technological University
Moscow, Russia

Abstract. The problem of managerial inertia inherent in traditional enterprise economic security monitoring systems has been identified. It is substantiated that, under conditions of high dynamism and uncertainty in the digital environment, the static nature of economic security assessment parameters–fixed for extended periods–leads to critical delays in responding to emerging threats. As a solution, a methodology and architecture for a hybrid adaptive indicator system are proposed, employing an integral index of enterprise economic security as a control signal. The scientific contribution of the study lies in the development of a two-level model that separates monitoring parameter management into a strategic loop (expert determination of priorities and permissible parameter ranges, incorporating system-generated suggestions) and a tactical loop (automatic real-time calibration within expert-defined constraints). Mathematical formalization of adaptation mechanisms is presented, including hybrid dynamic weighting (combining expert-assigned baseline weights with their automated adjustment within permissible ranges), threshold value adaptation, and calibration via retrospective testing. Numerical modeling on synthetic data confirmed the system's capability to operate in "autopilot" mode upon emergence of tactical threats: it temporarily focuses on the problem at hand and, following its resolution, autonomously reverts to baseline settings.

Keywords: economic security, monitoring, hybrid monitoring system, adaptive indicator system, managerial inertia, integral index of economic security, strategic loop, tactical loop.

References

[1] Abalkin, L. I. (1994). [Economic security of Russia: threats and their reflection]. *Voprosy Ekonomiki* [Problems of Economics]. No. 12, pp. 4-13. (In Russ.).

[2] Bekasova, E. N. (2021). [A practical approach to expert assessment of enterprise economic security]. *Ekonomika i biznes: teoriya i praktika* [Economics and Business: Theory and Practice]. No. 8 (78), pp. 9-13. (In Russ.).

[3] 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.).

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

[5] Abashkin, V. L., Abdrakhmanova, G. I., Vishnevskiy, 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.).

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

[8] 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.).

[9] 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.).

[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] 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.).

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

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

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

[15] 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.).

[16] 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.

[17] 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).

[18] Samoylov, M. A., Kondrashova, N. G. (2023). [Interrelation between economic and information security of a Russian organization]. *Ekonomika i biznes: teoriya i praktika* [Economics and Business: Theory and Practice]. No. 10–2 (104), pp. 132–134. (In Russ.).

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

[20] 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.

[21] Chen, P., Ji, M. (2025). Deep learning-based financial risk early warning model for listed companies: A multi-dimensional analysis approach. *Expert Systems with Applications*. Vol. 283, Article 127746.