Григорян Маргарита Сергеевна, Студент, Западный филиал
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации (РАНХиГС)

Числова Дарья Андреевна, Студент, Западный филиал
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации (РАНХиГС)

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ДИАГНОСТИКЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье исследуются подходы к оценке экономической безопасности предприятия в условиях цифровизации. Анализируется влияние современных угроз на функциональные составляющие бизнеса. На основе сравнительного анализа традиционных и инновационных моделей обоснована необходимость построения многоуровневой гибридной аналитической платформы

Ключевые слова: Экономическая безопасность предприятия, функциональные составляющие, пороговые значения, диагностические зоны, цифровые риски, гибридная модель

1. Теоретические основы диагностики экономической безопасности предприятия

Для диагностики уровня экономической безопасности предприятия (ЭБП) используется концепция функциональных составляющих, каждая из которых представляет собой совокупность индикаторов, характеризующих определённую сферу деятельности предприятия. Основные функциональные составляющие включают в себя финансовую (платёжеспособность, устойчивость, ликвидность, автономия, рентабельность), производственную (бесперебойный выпуск продукции, износ фондов, загрузка мощностей, ритмичность), кадровую (текучесть, квалификация, лояльность сотрудников) и технико-технологическую составляющие (сохранение и развитие технологического потенциала, доля нового оборудования, расходы на НИОКР, патенты). Также выделяются рыночная (доля рынка, зависимость от контрагентов), информационная (защита коммерческой тайны и ИТ-систем, уровень киберзащищённости) и правовая составляющие (соблюдение законодательства и правовое сопровождение контрактов). Взаимодействие данных составляющих носит строго системный характер, поскольку ослабление одного элемента неизбежно влияет на другие, что требует комплексной оценки с учётом их взаимосвязей.

Реализация угроз экономической безопасности оказывает комплексное негативное влияние на деятельность хозяйствующего субъекта по следующим направлениям:

1. Финансовые последствия: прямые и косвенные убытки, хищение активов, снижение прибыли и рост издержек на восстановление IT-инфраструктуры, ведущие к потере устойчивости и банкротству.

2. Операционные риски: сбои в бизнес-процессах, остановка деятельности, убытки от невыпущенной продукции или срыв контрактов.

3. Репутационные потери: утрата доверия клиентов, партнеров и инвесторов из-за утечек данных или некачественного продукта.

4. Правовые последствия: штрафы, судебные разбирательства и отзыв лицензий.

5. Социальные риски: снижение мотивации персонала из-за коррупции и рост затрат на поиск кадров.

Ключевым элементом диагностики являются пороговые значения – предельные величины индикаторов, переход за которые означает формирование кризисных тенденций. На основе сопоставления фактических значений с порогами выделяют три диагностические зоны: зону стабильности (риски минимальны), предкризисную зону (необходимы превентивные меры) и кризисную зону (требуется экстренное антикризисное управление). Алгоритм

диагностики включает пять последовательных этапов: идентификация (выбор индикаторов и расчет порогов), мониторинг (сбор данных), анализ (определение текущей зоны), локализация (анализ причин ухудшения показателей) и коррекция (реализация антикризисных мероприятий).

2. Новые вызовы и сравнительный анализ моделей диагностики

Цифровая трансформация экономики приводит к появлению качественно новых цифровых рисков, обнажая недостатки传统ных статичных индикаторов. Главная проблема классических финансовых индикаторов заключается в их ретроспективном характере – они фиксируют результаты уже произошедших событий и не способны предупредить о мгновенно реализующихся угросах (кибератаках). Кроме того, статичные пороги не приспособлены для оценки рисков нарушения непрерывности бизнеса (Business Continuity) при сбоях в ИТ-системах, а в самих моделях наблюдается дисбаланс значимости блоков: для ИТ-компаний и цифровых платформ информационная безопасность играет определяющую роль, в отличие от традиционных сырьевых предприятий.

Эффективность управления ЭБП зависит от точности используемого инструментария. В практике сложились традиционные и инновационные подходы, подробный анализ которых представлен в таблице 1.

В тексте указывается ссылка на таблицу: результаты сопоставления подходов приведены в таблице 1.

Таблица 1

Сравнительный анализ моделей оценки экономической безопасности предприятия

Параметр	**Индикаторный подход**	**Ресурсно-функциональный подход**	**Риск-ориентированный подход**	**Программмно-целевой подход**
Объект оценки	Финансовые и операционные коэффициенты	Эффективность использования ресурсов по блокам	Пары «вероятность – ущерб»	Выполнение целевых программ
Учёт специфики	Низкий (шаблонные пороги)	Средний (через веса блоков)	Высокий (индивидуальные карты)	Высокий (индивидуальные программы)
Прогности-ческая сила	Низкая (запаздывающие показатели)	Средняя (текущее состояние)	Высокая (ориентация на будущее)	Низкая (оценка прошлого)
Трудо-ёмкость	Низкая (простой, дешёвый)	Высокая (требует аналитиков)	Очень высокая (сложный, дорогой)	Средняя

Каждая из представленных методик имеет свои достоинства и недостатки. Индикаторный подход нагляден и прост, но отличается жёсткостью порогов и неприменим для внезапных кризисов. Ресурсно-функциональный подход обеспечивает комплексность, но страдает субъективностью весов. Риск-ориентированный подход обладает высокой гибкостью и прогностической силой, однако приводит к «ложной конкретности» при дефиците данных. Программно-целевой подход успешно интегрируется в бюджет, но субъективен при оценке предотвращённого ущерба.

3. Формирование гибридной модели мониторинга и выводы

Современные условия диктуют необходимость перехода от изолированных методик к построению многоуровневых, синтетических систем мониторинга, где методы дифференцируются в зависимости от управленческих целей. Для целей внешнего контроля или экспресс-анализа достаточно использовать индикаторный подход с отраслевой корректировкой порогов. На уровне стратегического управления предпочтителен ресурсно-

функциональный анализ, позволяющий защитить внутренний потенциал предприятия. Для оперативного реагирования на цифровые риски необходимо внедрять элементы риск-ориентированного подхода на базе данных о реальных инцидентах.

В качестве базовой аналитической платформы рекомендуется использовать ресурсно-функциональный подход Е.А. Олейникова. Для преодоления его статичности наполнение каждого блока должно осуществляться с помощью динамических индикаторов и риск-ориентированных инструментов. В части киберрисков индикаторную базу необходимо усиливать гибридными моделями, включающими бинарные триггеры критических событий (факт взлома, утечка данных) и риск-ориентированные методы оценки влияния инцидентов на непрерывность бизнеса.

Данный методологический синтез позволит менеджменту своевременно идентифицировать переход угроз в качественный кризис, оперативно локализовать триггеры негативных явлений, эффективно маневрировать ресурсами и гарантировать стабильное долгосрочное развитие бизнеса в турбулентной среде

Список литературы:

1. Олейников, Е. А. Экономическая и национальная безопасность: учебник / Е.А. Олейников. – Москва: Экзамен, 2004. – 768 с.

2. Экономическая безопасность России: общий курс: учебник / под ред. В. К. Сенчагова. – 5-е изд. – Москва: БИНОМ. Лаборатория знаний, 2015. – 815 с. (Базовый источник для раздела 1.3 о пороговых значениях и макроиндикаторах).

3. Баранова, Н. В. Трансформация системы обеспечения экономической безопасности предприятия в условиях цифровизации / Н. В. Баранова // Вестник экономического анализа. – 2023. – No 2. – С. 45–52.

4. Карпова, С. В. Риск-ориентированный подход к оценке экономической безопасности хозяйствующих субъектов / С. В. Карпова, Д. А. Иванов // Вопросы экономики и права. – 2024. – No 4 (190). – С. 89–95.

5. Королев, М. И. Экономическая безопасность фирмы: теория, практика, выбор стратегии: монография / М. И. Королев. – Москва: Экономика, 2011. – 284 с.

6. Сидорова, Е. Е. Мониторинг киберугроз как элемент информационной составляющей экономической безопасности предприятия / Е. Е. Сидорова // Экономика и управление: научно-практический журнал. – 2025. – No 1. – С. 112–118.

7. Уразгалиев, Ш. С. Экономическая безопасность: учебник и практикум для вузов / Ш.С. Уразгалиев. – 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2023. – 725 с.

8. Чернова, Г. В. Управление рисками: учебное пособие / Г.В. Чернова, А.А. Кудрявцев. – Москва: Проспект, 2022. – 160 с