УДК 338.2:657

# СОВРЕМЕННЫЕ ПРАКТИКИ МОНИТОРИНГА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ДЛЯ УСТОЙЧИВОГО РАЗВИТИЯ БИЗНЕСА

Бадретдинова Э.З.[1], студентка гр. ЭУЭ-2-21, IV курс, Уразбахтина Л.Р.[1], к.э.н., доцент

[1]Казанский государственный энергетический университет, г. Казань

В условиях экономической нестабильности, кибератак и глобальных кризисов обеспечение экономической безопасности является необходимым условием развития бизнеса. Компании, которые игнорируют риски, рано или поздно сталкиваются с потерями – от финансовых убытков до репутационных катастроф.

Однако те, кто внедряет систему мониторинга, способны не только выживать в условиях турбулентности, но и использовать кризисы как возможности для роста. Современные инструменты анализа данных, прогнозирования угроз и управления рисками предполагают «цифровую защиту» бизнеса, что приводит к адаптации, защите и росту даже в самых сложных условиях.

Экономическая безопасность – это не просто защита активов или соблюдение бюджета. Это комплексная стратегия, охватывающая все аспекты деятельности компании: от цепочек поставок и финансовых потоков до репутации и лояльности клиентов.

Главная цель экономической безопасности – создать «иммунитет» к потрясениям. Например, страны, которые добиваются экспорта одного ресурса, будь то нефть, газ или редкие металлы, оказываются уязвимыми при падении цен на сырье. Так, Венесуэла, чья экономика на 95% зависела от нефти, столкнулась с гиперинфляцией и сопутствующим коллапсом, когда стоимость барреля упала ниже 30 долл. В то же время Норвегия, также экспортирующая нефть, вышла из кризиса благодаря диверсификации - доходы от ресурсов направляются в суверенный фонд, который инвестирует в акции, недвижимость и инновации во всем мире. Это обеспечивает сохранение стабильности страны даже в периоды кризисов [1].

Одной из ключевых угроз остается кибербезопасность. Современная экономика всё больше опирается на цифровые технологии, а хакерские меры способны парализовать критическую инфраструктуру. В 2021 году взрыв колониального трубопровода в США приведет к остановке поставок топлива на восточное побережье, панике и росту цен. Возможные инциденты совершаются, защита данных, энергосетей и финансовых систем — это вопрос не ИТ-отрасли, а элемента национальной безопасности. Для противодействия такому риску государства ужесточают регулирование. Так,

ЕС вводит директиву NIS2, обязывающую компании сообщать о кибератаках, а Китай разрабатывает собственные операционные системы, чтобы снизить требования со стороны зарубежных технологий.

Еще один вызов — санкционное давление. Ограничения со стороны других стран могут блокировать доступ к рынкам, технологиям и инвестициям. Однако история показывает, что санкции часто стимулируют развитие собственной промышленности. Яркий пример — Иран, который под давлением эмбарго создал собственную фармацевтическую промышленность, обеспечивающую 97% использования технологий за счет местных производств. Россия, столкнувшись с ограничениями в 2014 - 2022 годах, начала активно развивать отрасли экономики, сократив импорт продовольствия с 35% до 20% за десятилетие.

В конечном итоге экономическая безопасность — это не просто защита от угроз, это и стратегия развития. Она позволяет превратить вызовы в возможности, укрепить уверенность и улучшить качество жизни граждан. В мире, где кризисы становятся нормой, только сбалансированный подход, сочетающий инновации, регулирование и международное партнерство, может обеспечить устойчивое будущее.

Угрозы здесь многолики: валютные колебания подрывают рентабельность экспорта, хакерские меры парализуют ИТ-инфраструктуру, санкции перекрывают доступ к рынкам, негативные отзывы в социальных сетях за несколько часов нарушают доверие к бренду. Чтобы справиться с этими вызовами, недостаточно разовых мер. Необходим непрерывный мониторинг, который превращает сырые данные в инсайты, а инсайты – в упреждающие действия.

Такие системы становится инструментами финансовой аналитики. Программные платформы вроде Tableau или Power BI агрегируют данные из ERP-системы, банковских счетов и биржевых котировок, визуализируя основные метрики: ликвидность, долговую нагрузку, маржинальность. Но истинная ценность не в графиках, а в способностях алгоритмов нахождения аномалий. Например, если коэффициент текущей платежеспособности компании начинает падать, система сигнализирует о риске кассовых разрывов, то есть варианты – от оптимизации запасов до реструктуризации кредитов.

В настоящее время в банковском секторе аналогичные инструменты спасают от дефолтов: анализируя кредитный портфель, они прогнозируют вероятность невозврата, сигнализируют о нестабильности в макроэкономических индикаторах и поведенческих данных клиентов [2].

Киберугрозы сегодня не менее опасны, чем обычные кризисы. По данным IBM, средний ущерб от утечки данных в 2023 году составил 4,45 млн. долл. Здесь на первый план выходят системы кибербезопасности: SIEM-платформы (информация о безопасности и управление событиями), такие как Splunk или IBM QRadar, которые в режиме реального времени отслеживают аномальную активность в сетях. Они не просто блокируют атаки, а учатся на

них - с помощью машинного обучения алгоритмы предсказывают характер будущих взломов, укрепляя уязвимые узлы.

Для производственных предприятий важны решения ICS/SCADA, защищающие промышленные сети от саботажа. Компании, внедрившие «цифровые двойники» своей IT-инфраструктуры, смогли избежать подобных явлений, тестируя уязвимости в виртуальных средах.

Репутационные риски, которые раньше были второстепенными, теперь считаются способными обрушить капитализацию за несколько дней. Социальные сети становятся полем боя, где фейковые новости или скандальные видео моментально набирают миллионы просмотров. Такие инструменты медиапространства, как Brandwatch или Hootsuite, сканируют упоминания о брендах во всех странах и платформах, измеряя тональность и выявляя кризисные тенденции.

Цепочки поставок, особенно глобальные, уязвимы к десяткам угроз: от последствий катастрофы до аналитических исследований. Пандемия COVID-19 показала, как зависимость от одного региона (например, производства микросхем в Азии) может парализовать автопром. Такие инструменты, как Resilinc или FourKites, используют большие данные и спутниковый мониторинг, чтобы отслеживать статус грузов, прогнозировать задержку и находить альтернативные поставщики [3].

Компании, внедрившие светодиоды, такие как IBM Food Trust, демонстрируют прозрачность цепочек – от производства до полки, что не только снижает риски, но и учитывает доверие потребителей.

Однако самые продвинутые инструменты бесполезны без усилий в единой экосистеме. Разрозненные данные из финансовых, логистических и ИТ-систем создают «слепые зоны», где угроза находится незамеченными дисплеями. Платформы международных данных (например, Talend или Informatica) объединяют источники, создавая 360-градусный обзор рисков.

Важнейший элемент — стресс-тестирование мониторинга. Банки давно используют его для оценки устойчивости к кризисам, но сегодня этот подход проник во все отрасли. Цифровые двойники предприятий позволяют моделировать сценарии: что будет, если курс доллара вырастет на 30%, если ключевой поставщик обанкротится или если новый закон ужесточит экологические нормы.

Нормативное соответствие – еще один пласт экономической безопасности. GDPR, CCPA, ISO 27001 — стандарты, которые являются единственной бюрократией, на деле защищают от штрафов и судебных исков. Инструменты автоматизации соответствия, такие как LogicGate или VComply, отслеживают изменения в законодательстве 200 стран и адаптируют под них политику компании. В фармацевтике, где одобрение регуляторов — ключ к выходу на рынок, это экономит годы и миллионы долларов [4].

Однако внедрение таких систем сталкивается с вызовами. Высокая стоимость, территориальные лидеры, нехватка экспертов — частные барьеры. Здесь помогает поэтапный подход: начать пилотный проект в одном

департаменте, показать рентабельность инвестиций и масштабировать [5]. Когда Unilever внедрила искусственный интеллект для стабилизации поставок, первые тесты были проведены в одном виде (пальмовое масло), а затем расширилась система на 3000 поставщиков.

Таким образом, детерминант быстрого развития бизнеса в современных условиях – это не исключение рисков, а управление ими. Инструменты создают «нервную систему» компании, связывая данные, людей и процессы в едином организме, способном управлять угрозой и эволюционировать.

## Список литературы:

1. Афанасьев, М. В. Диверсификация как процесс обеспечения устойчивости экономики в условиях санкций / М. В. Афанасьев, Л. Р. Уразбахтина // Эффективные системы менеджмента: Качество. Циркулярная экономика. Технологический суверенитет : Сборник научных статей XI Международного научно-практического форума, Казань, 22–24 ноября 2023 года. – Казань: Издательство "Познание", 2024. – С. 41-43.

2. Калинина Г.В., Андреев В.В., Литвинова О.В., Федорова Л.П. Теоретические понятия экономической безопасности организации // Вестник Российского университета кооперации. 2022. № 3 (25). С. 52-55.

3. Хусаинова, Е. А. Зарубежный опыт повышения экономической безопасности и адаптация к российским условиям / Е. А. Хусаинова, Э. Р. Тимергазизова // Экономика и управление: проблемы, решения. – 2024. – Т. 5, № 5(146). – С. 44-49.

4. Малиновская Н.А., Нагаслаева И.О. Исследование системы мониторинга социально-экономического развития региона // Известия Юго-Западного гос. ун-та. Серия «Экономика. Социология. Менеджмент». 2024. № 2. С. 48-56.

5. Попова О.А., Малиновская Н.А., Нагаслаева И.О. Анализ системы мониторинга социально-экономического развития региона // Вестник ЗабГУ. Экономические науки. 2023. № 1 (116). С. 142-150.