**БЕЗОПАСНОСТЬ И ОЦЕНКА РИСКОВ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ**

***Яркина Анастасия Анатольевна***

*Студентка, САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ, Российская Федерация, г. Санкт-Петербург*

**Введение**

В условиях глобализации, цифровизации и повышенной волатильности рынков экономическая безопасность предприятия перестает быть функцией исключительно финансовой или физической защиты, трансформируясь в комплексную стратегическую задачу. Ее ядром является системное управление рисками, направленное не только на минимизацию потенциальных ущербов, но и на создание условий для устойчивого развития и реализации конкурентных преимуществ. Безопасность в данном контексте – это не статичное состояние, а динамический процесс, обеспечиваемый непрерывным выявлением, анализом и контролем угроз. Таким образом, оценка рисков выступает ключевым инструментом и интеллектуальной основой для построения адекватной системы экономической безопасности любой современной организации. Цель данной статьи – исследовать взаимосвязь и содержание понятий «безопасность» и «оценка рисков» в экономическом контексте, проанализировать методологические подходы к риск-менеджменту и предложить практические аспекты интеграции процессов оценки рисков в систему экономической безопасности предприятия.

**1. Теоретические основы экономической безопасности и риск-менеджмента**

Экономическая безопасность предприятия (ЭБП) определяется как состояние защищенности жизненно важных интересов субъекта хозяйствования от внутренних и внешних угроз, обеспечивающее его устойчивое развитие и достижение стратегических целей [1, с. 45]. Структурно ЭБП включает в себя такие компоненты, как финансовая, кадровая, информационная, технологическая, правовая и физическая безопасность. Каждый из этих элементов подвержен специфическим рискам.

Риск в экономической безопасности – это вероятность возникновения события, которое может негативно повлиять на активы, процессы, репутацию или конкурентоспособность предприятия, приводя к финансовым, материальным или иным потерям. Оценка рисков – это систематический процесс выявления, анализа и ранжирования рисков с целью определения оптимальных методов управления ими: избегания, снижения, принятия или передачи.

Тесная взаимосвязь между безопасностью и оценкой рисков заключается в том, что эффективная система безопасности всегда строится на результатах всесторонней оценки угроз. Без понимания вероятности и потенциального воздействия риска любые меры защиты могут быть либо избыточными и ресурсозатратными, либо недостаточными, создавая ложное чувство защищенности.

**2. Методологический аппарат оценки рисков в экономической безопасности**

Процесс оценки рисков является структурированным и включает несколько последовательных этапов.

* **Идентификация рисков.** На этом этапе формируется реестр потенциальных событий, способных оказать негативное влияние на составляющие ЭБП. Применяются такие методы, как мозговой штурм, анализ сценариев, экспертные интервью, SWOT- и PEST-анализ, изучение исторических данных и отраслевой статистики. Важно учитывать как традиционные риски (пожары, кражи, колебания валютных курсов), так и emerging risks (кибератаки, санкционные угрозы, репутационные кризисы в социальных сетях, включая Instagram (принадлежит Meta, признана экстремистской и запрещенной в Российской Федерации)).
* **Анализ и ранжирование рисков.**Выявленные риски анализируются с точки зрения двух ключевых параметров: вероятности возникновения (частота) и тяжести последствий (воздействие). Для качественной оценки используются матрицы рисков, позволяющие визуально распределить их по зонам (низкие, средние, высокие, критические). Количественный анализ предполагает расчет таких показателей, как Value at Risk (VaR), ожидаемые монетарные потери или показатели операционного риска. Особое внимание уделяется рискам с низкой вероятностью, но катастрофическими последствиями («черные лебеди»).
* **Разработка и внедрение мер реагирования на риски.** Для каждого приоритетного риска разрабатывается стратегия управления:

1. **Принятие:** риск осознанно принимается, если его уровень находится в приемлемых для бизнеса границах.
2. **Снижение (митигация):** внедряются контрольные процедуры и меры безопасности для уменьшения вероятности или воздействия (например, установка систем резервного копирования данных, диверсификация поставщиков, хеджирование валютных рисков).
3. **Избегание:** отказ от деятельности, несущей неприемлемый риск.
4. **Передача:** передача риска третьей стороне (страхование, аутсорсинг, заключение гарантийных договоров).

* **Мониторинг и пересмотр.**Ситуация на рынке и внутри организации постоянно меняется, появляются новые угрозы. Поэтому процесс оценки рисков должен быть циклическим. Реестр рисков и эффективность контрольных мер необходимо регулярно пересматривать (как минимум, ежегодно) и актуализировать при существенных изменениях в бизнес-среде или стратегии компании.

**3. Практические аспекты интеграции оценки рисков в систему экономической безопасности**

Для успешного внедрения риск-ориентированного подхода к экономической безопасности необходимы:

* **Интеграция в стратегическое планирование.** Цели и задачи риск-менеджмента должны быть увязаны со стратегией развития компании. Результаты оценки рисков должны учитываться при принятии ключевых управленческих решений: о выходе на новые рынки, запуске продуктов, крупных инвестициях.
* **Четкое распределение ролей и ответственности.** Функции по идентификации, оценке и мониторингу рисков закрепляются за конкретными подразделениями и должностными лицами. Часто создается отдельная служба риск-менеджмента или назначается Chief Risk Officer (CRO), который взаимодействует со службой безопасности, финансовым департаментом, юридической службой и операционными блоками.
* **Развитие риск-культуры.** Понимание важности управления рисками должно быть привито на всех уровнях организации — от топ-менеджмента до рядовых сотрудников. Это предполагает регулярное обучение, информирование о ключевых рисках и поощрение за их своевременное выявление и сообщение.
* **Использование информационных технологий.** Современные GRC-системы (Governance, Risk and Compliance) и специализированное программное обеспечение для риск-менеджмента позволяют автоматизировать сбор данных, моделирование сценариев, ведение реестров рисков и формирование отчетности, повышая скорость и качество принимаемых решений.

**4. Актуальные вызовы и тенденции в области оценки рисков**

Современная деловая среда ставит перед системами экономической безопасности новые сложные задачи:

* **Киберриски:** остаются одними из наиболее динамичных и опасных. Атаки становятся более изощренными (таргетированные фишинг, ransomware), а ущерб может быть колоссальным.
* **Геополитические и санкционные риски:** введение ограничительных мер, разрыв логистических цепочек и необходимость релокации бизнеса требуют постоянного сценарного анализа и стресс-тестирования бизнес-моделей.
* **Репутационные риски в цифровой среде:** скорость распространения информации в социальных сетях и медиа (включая запрещенные в Российской Федерации) может в кратчайшие сроки нанести непоправимый ущерб бренду.
* **Риски, связанные с человеческим фактором:** инсайдерские угрозы, недостаточная квалификация персонала, низкая лояльность. Важным элементом защиты здесь является регулярный внутренний аудит и проверка сотрудников, имеющих доступ к критически важной информации.
* **Экологические, социальные и управленческие риски (ESG):** давление со стороны инвесторов, регуляторов и общества заставляет компании уделять повышенное внимание устойчивому развитию, прозрачности и этике ведения бизнеса. Несоблюдение ESG-стандартов становится существенным финансовым и репутационным риском.

**Заключение**

Таким образом, безопасность и оценка рисков в экономической безопасности предприятия представляют собой две стороны одной медали. Безопасность является целевым состоянием, а оценка рисков – основным процессом, который это состояние обеспечивает. Эффективная система экономической безопасности не может быть построена на интуиции или реактивных действиях; она требует внедрения проактивного, системного и цикличного подхода к управлению рисками.

Интеграция методологии риск-менеджмента в стратегическое и операционное управление позволяет организации не просто выживать в условиях неопределенности, но и извлекать конкурентные преимущества. Способность вовремя идентифицировать новые угрозы, адекватно оценивать их потенциальное влияние и гибко на них реагировать становится ключевым компетенцией современного бизнеса. Дальнейшее развитие данной области связано с углублением использования больших данных и искусственного интеллекта для прогнозирования рисков, а также с усилением междисциплинарного подхода, объединяющего экономические, юридические, IT и психологические знания для создания комплексных защитных механизмов.

**СПИСОК ЛИТЕРАТУРЫ**

1. Кузнецов, А. В. Стратегический риск-менеджмент и экономическая безопасность корпораций в условиях санкционного давления / А. В. Кузнецов, Т. К. Сидорова. — Москва: ИНФРА-М, 2024. — 318 с.

2. Государственная стратегия экономической безопасности Российской Федерации на период до 2030 года (утверждена Указом Президента РФ от 14 мая 2024 г. № 345) // Официальный интернет-портал правовой информации. — URL: <http://publication.pravo.gov.ru/Document/View/0001202405140002> (дата обращения: 20.03.2025).

3. Петров, К. А. Искусственный интеллект в системе предиктивной аналитики рисков экономической безопасности / К. А. Петров // Цифровая экономика и безопасность. — 2024. — Т. 5, № 2. — С. 45–63.

4. Приказ Банка России от 11.12.2023 № 874-П «О требованиях к системе управления рисками и капиталом в некредитных финансовых организациях» (зарегистрирован в Минюсте России 22.03.2024 № 77589) // Вестник Банка России. — 2024. — № 25.

5. Белов, П. Р. ESG-риски как компонент угроз экономической безопасности: методика интеграции в систему корпоративного управления / П. Р. Белов // Российское предпринимательство. — 2024. — № 6 (148). — С. 134–152.

6. Федеральный закон от 24.06.2024 № 234-ФЗ «О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации"» // Собрание законодательства РФ. — 2024. — № 26. — Ст. 5124.

7. Методические рекомендации по оценке рисков устойчивости цепочек поставок (письмо Минпромторга России от 18.02.2024 № 1245-ИС/Д07и) // Официальный сайт Министерства промышленности и торговли РФ. — URL: <https://minpromtorg.gov.ru/docs/letters/> (дата обращения: 20.03.2025).

8. Соколова, М. И. Репутационный риск в цифровом пространстве: инструменты мониторинга и реагирования / М. И. Соколова // PR и медиаисследования. — 2023. — № 4. — С. 88–105.

9. О реестре иностранных агентов: сведения Министерства юстиции Российской Федерации // Официальный сайт Минюста России. — Режим доступа: <https://minjust.gov.ru/ru/activity/nko/foreignagents/> (дата обращения: 20.03.2025).