DOI 10.37882/2223-2974.2025.08.20

ИННОВАЦИОННЫЕ МЕТОДЫ ОЦЕНКИ КИБЕРРИСКОВ НА МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЯХ

INNOVATIVE METHODS FOR CYBER RISK ASSESSMENT IN SMALL AND MEDIUM-SIZED ENTERPRISES

A. Trubin
E. Timofeev

Summary. In the context of digital transformation, small and medium-sized enterprises (SMEs) are among the most vulnerable to cybersecurity threats. This paper analyzes modern cyber risk assessment methods and their applicability to SMEs. Based on a comparison of international and domestic approaches, the study identifies promising models that combine analytical rigor with implementation simplicity. The findings highlight the need for scalable and accessible risk assessment frameworks tailored to resource-constrained organizations with low digital maturity.

Keywords: information security, cyber risks, digitalization, small and medium enterprises, risk assessment methods, risk management, cybersecurity models.

Трубин Александр Евгеньевич
Кандидат экономических наук, доцент, НОЧУ ВО Московский финансово-промышленный университет «Синергия»
niburt@yandex.ru
Тимофеев Евгений Олегович
Аспирант, НОЧУ ВО Московский финансово-промышленный университет «Синергия»
evgentimofeev6@gmail.com

Аннотация. В условиях цифровизации экономики малые и средние предприятия (МСП) становятся одной из наиболее уязвимых категорий организаций в сфере информационной безопасности. Целью настоящего исследования является анализ современных методов оценки киберрисков и их применимости в контексте МСП. На основе сопоставления зарубежных и отечественных подходов выявлены наиболее перспективные методики, сочетающие аналитическую обоснованность с простотой внедрения. Сделан вывод о необходимости разработки адаптированных и воспроизводимых моделей оценки, учитывающих ограниченность ресурсов и низкий уровень цифровой зрелости предприятий малого бизнеса.

Ключевые слова: информационная безопасность, киберриски, цифровизация, малый и средний бизнес, методы оценки, управление рисками, модели кибербезопасности.

В условиях стремительной цифровизации экономики малые и средние предприятия (далее — МСП) становятся активными участниками информационного пространства. При этом они представляют собой одну из наиболее уязвимых категорий организаций перед лицом киберугроз. По данным Global Cybersecurity Outlook 2024, более 40 % всех атак в мировой практике приходится на МСП, при этом большинство из них не имеют ни стратегии реагирования, ни базовых инструментов оценки рисков [14]. Аналогичная ситуация наблюдается и в России: по данным Агентства стратегических инициатив, только треть предприятий малого сектора осуществляют системную работу по управлению информационной безопасностью [1].

Отсутствие должного внимания к вопросам киберустойчивости ведет не только к росту вероятности инцидентов, но и к прямым экономическим потерям. Киберриски трансформируются в фактор дестабилизации бизнес-процессов, приводя к перебоям в работе, дополнительным затратам на восстановление, утрате деловой репутации и снижению инвестиционной привлекательности. Как подчеркивает Ф.А. Кузнецов, в малом бизнесе проблемы информационной безопасности (далее — ИБ) воспринимаются как второстепенные и редко интегрируются в управленческую повестку, что формирует институциональные барьеры для рационального распределения ресурсов [5]. Российские МСП, по мнению Д.А. Плетнева, системно отстают в уровне защищенности: дефицит средств, нехватка квалифицированного персонала и низкий уровень управленческой вовлеченности делают их уязвимыми даже к базовым видам угроз [6].

Наиболее распространённые модели оценки киберрисков традиционно разрабатываются на основе подходов, зафиксированных в таких стандартах, как ISO/IEC 27005 и NIST SP 800-30. Эти документы описывают базовые принципы построения системы управления рисками, включая инвентаризацию активов, анализ угроз, уязвимостей и вероятности наступления инцидентов [2], [12]. Однако их применение требует высококвалифицированного персонала, постоянного обновления данных и развитой ИТ-инфраструктуры. Как отмечают С.В. Гришунин и И.Ю. Пищалкина, сложность и ресурсоемкость этих подходов делают их малоприменимыми в условиях малого бизнеса [3].

Кроме технических и методических ограничений, существенную роль играют управленческие барьеры.

По наблюдению В.Г. Халина и Г.В. Черновой, отсутствие культуры работы с рисками и слабая вовлеченность руководства приводит к тому, что даже упрощенные процедуры оценки угроз не реализуются в управленческой практике [7]. В результате кибербезопасность воспринимается не как элемент стратегического управления, а как внешний технический фактор, что снижает устойчивость предприятия в долгосрочной перспективе.

Между тем, как подчеркивается в докладе Global Cybersecurity Outlook 2024, эффективное управление киберрисками способствует повышению операционной устойчивости, снижению трансакционных издержек и укреплению конкурентных позиций МСП [14]. Это обуславливает актуальность перехода от универсальных стандартов к адаптированным инструментам, ориентированным на практическую применимость, управленческую эффективность и возможность реализации на предприятиях МСП.

Цель настоящего исследования — проанализировать современные методы оценки киберрисков и выявить их применимость в системе управления в малом и среднем бизнесе. В международной практике предлагается ряд решений, сочетающих аналитическую строгость с возможностью адаптации в организациях с низкой ИТ-зрелостью.

Одним из таких решений является комбинация методов SWARA (Step-wise Weight Assessment Ratio Analysis) и BWM (Best–Worst Method), направленная на формализацию экспертных оценок значимости факторов риска и поддержку управленческих решений в области распределения ресурсов информационной безопасности. В работе А. Сукумара, Х. А. Махдираджи и В. Джафари-Садеги (2023) данный подход применен к онлайн-компаниям МСП. Методика позволяет построить иерархию угроз, которая служит основанием для приоритизации мер защиты. Ее достоинствами являются воспроизводимость, невысокие требования к технической базе и применимость в условиях ограниченного доступа к точным статистическим данным [13].

Альтернативный вектор представлен моделью RCVaR (Real Cyber Value at Risk), предложенной М.Ф. Франко и др. (2023). Она адаптирует принципы финансового анализа риска (VaR) для расчета потенциального ущерба от киберинцидентов с учетом специфики отрасли и масштаба бизнеса. Такой подход позволяет предприятию формировать экономически обоснованную стратегию кибербезопасности, выстраивая баланс между вероятностью ущерба и объемом инвестиций в защиту [10].

Значимым ориентиром является и разработанная Национальным институтом стандартов и технологий США (National Institute of Standards and Technology, NIST) методологическая основа NIST Cybersecurity Framework (далее — CSF), которая, хотя и не содержит прямого инструментария оценки рисков, представляет собой фундамент для построения системы управления информационной безопасностью. Ее адаптированная версия для малого бизнеса способствует систематизации организационных решений, разработке внутренних регламентов и оптимизации операционных процессов [12].

Проект DETECTA 2.0, основанный на использовании цифровых двойников и технологий машинного обучения, предлагает технологически продвинутую платформу предиктивной диагностики и защиты. Данный подход демонстрирует высокий потенциал в рамках концепции Индустрии 4.0. Однако в условиях МСП его реализация требует высокой цифровой зрелости и привлечения внешней экспертной поддержки [11].

Cyber Risk Tool for Irish SMEs (Cyber Risk Assessment Tool for Irish Small Business Owners) — методика, разработанная М. Кертин в рамках исследования Munster Technological University (2024), предназначена для оценки киберрисков в малых предприятиях Ирландии [9]. Она адаптирована под владельцев бизнеса без ИТ-специализации и позволяет быстро определить уязвимые зоны и уровень цифровой зрелости. Диагностический инструмент создавался с участием фокус-групп и применяется как часть управленческого самоаудита.

Российская практика демонстрирует более ограниченный инструментарий. Наиболее целостным решением можно считать методику Р.Д. Хамидуллина, в которой реализована оценка уязвимостей и расчет допустимого риска с использованием KPI. При адаптации под специфику малого бизнеса она может служить основой для регулярной оценки и контроля параметров ИБ с управленческой точки зрения [8].

Практико-ориентированные решения, такие как платформа Security Vision CRS, обеспечивают автоматизацию оценки рисков, однако не сопровождаются открытой методологической базой и потому не рассматриваются как научно верифицированные. Предложение коробочных продуктов киберстрахования (например, от СОГАЗ, Ингосстрах) играет скорее вспомогательную роль, позволяя компенсировать финансовые последствия инцидентов, но не формируя инструментарий для их предотвращения или оценки [4].

Таким образом, зарубежные решения демонстрируют более широкую проработанность и ориентированы на поддержку управленческих решений в сфере киберустойчивости. В то время как российская практика сосредоточена на точечных инициативах, не обеспечивающих полного цикла оценки и планирования. Для эффективной трансформации ИБ из затратной функции в элемент

Таблица 1.

Сравнение зарубежных и российских инструментов оценки киберрисков в МСП

Название метода	Тип / форма реализации	Применимость к МСП	Краткая характеристика
SWARA + BWM	Мультикритериальный анализ, экспертные оценки	Высокая	Позволяет ранжировать угрозы по значимости на основе опросов; требует минимальных ресурсов
RCVaR	Количественная оценка, сценарный анализ	Средняя	Прогноз убытков от кибератак на основе статистики; нужен доступ к отраслевым данным
NIST CSF	Фреймворк, организационный подход	Высокая (при адаптации)	Универсальная модель управления ИБ; требует адаптации под уровень зрелости
Ирландская методика (2024)	Национальный инструмент, онлайн-интерфейс	Высокая (для микробизнеса)	Простой интерфейс для самооценки рисков; доступен без ИТ-отдела
DETECTA 2.0	Цифровой двойник, ML-модель	Низкая	Технологически сложное решение; не апробировано в МСП
Методика Хамидуллина	KPI-модель, расчет допустимого риска	Средняя (требует адаптации)	Предназначена для корпоративного центра; может быть адаптирована при наличии ИТ-службы

Источник: составлено автором на основе [10], [11] [13].

устойчивого развития необходимы воспроизводимые и масштабируемые модели, интегрированные в систему стратегического управления МСП.

Для систематизации ключевых различий представим сравнительное сопоставление зарубежных и отечественных решений, ориентированных на потребности МСП (табл. 1).

Проведенный анализ выявил, что зарубежные подходы к оценке киберрисков демонстрируют значительно более высокую степень методологической зрелости и ориентации на управленческие цели. Методы SWARA–BWM и RCVaR позволяют формализовать процедуры принятия решений и моделировать последствия киберинцидентов, а NIST CSF обеспечивает структурное регулирование процессов безопасности. Их особенностью является баланс между аналитической обоснованностью и доступностью для внедрения в организациях с базовой цифровой инфраструктурой.

Российская практика, напротив, остается фрагментарной: существующие разработки ориентированы либо на крупный корпоративный сектор, либо не прошли практическую апробацию в малом бизнесе. Методика Р.Д. Хамидуллина представляет собой потенциальную основу для внутреннего контроля, но требует адаптации. Коммерческие решения, такие как Security Vision CRS, или страховые продукты, как правило, не обеспечивают оценку риска как управленческого процесса и не затрагивают его профилактическую составляющую.

С научной точки зрения важно отметить, что многие зарубежные решения находятся на стадии концептуальной проработки или препринтов, а потому требуют осторожного подхода к заимствованию. Однако даже в этом виде они демонстрируют направления, по которым может развиваться отечественная практика: упрощенные инструменты ранжирования угроз, количественные модели ущерба, адаптированные к масштабам и специфике МСП.

Таким образом, формирование доступных, экономически обоснованных и масштабируемых инструментов оценки киберрисков представляет собой не только научную, но и актуальную прикладную задачу. Разработка подобных решений позволит малому бизнесу перейти от реактивной модели ИБ к стратегическому управлению устойчивостью и цифровой безопасностью. Перспективными направлениями исследований являются интеграция методов оценки рисков в управленческий контур, разработка отраслевых шкал приоритетности и цифровых панелей самооценки с возможностью автоматической интерпретации результатов.

ЛИТЕРАТУРА

1. АНО «Агентство стратегических инициатив»; ООО «Третья сторона». Исследование защищённости от угроз информационной безопасности малого и среднего бизнеса. — 26.02.2024. — URL: https://asi.ru/library/main/198679/ (дата обращения: 15.05.2025). — Текст: электронный.
2. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Руководство по управлению рисками. — Введ. 2011-07-01. — М.: Стандартинформ, 2011. — 40 с.
3. Гришунин С.В., Пищалкина И.Ю., Сулоева С.Б. Оценка киберрисков в проектах интернета вещей // Научно-технические ведомости СПбГПУ. Экономические науки. — 2021. — Т. 14, № 6. — С. 102–116. — DOI: 10.18721/JE.14608.
4. Карпова Н.А. Страхование киберрисков — как способ защиты бизнеса от цифровых угроз // Consult-CCT. — 2020. — URL: https://consult-cct.ru/blogs/strahovanie-kiberriskov/ (дата обращения: 15.05.2025). — Текст: электронный.
5. Кузнецов Ф.А. Проблемы кибербезопасности, которые нельзя игнорировать в 2022 году // Russian Journal of Management. — 2022. — Т. 10, № 4. — С. 171–180. — DOI: 10.29039/2409-6024-2022-10-4-171-180.
6. Плетнёв Д.А., Викулин С.Н., Щелканогов П.Г., Плетнёв А.Д. Новые вызовы информационной безопасности малого и среднего бизнеса // Вестник Челябинского государственного университета. — 2022. — № 11 (469). — С. 177–181. — DOI: 10.47475/1994-2796-2022-11119.
7. Халин В.Г., Чернова Г.В. Цифровизация и киберриски // Управленческое консультирование. — 2023. — № 7. — С. 28–41.
8. Хамидуллин Р.Д. Методика оценки киберрисков корпоративного центра ИТ-мониторинга // Креативная экономика. — 2023. — Т. 17, № 12. — С. 4641–4660. — DOI: 10.18334/ce.17.12.120009.
9. Curtin M., Sheehan B., Gruben M., Kozma N., O'Carroll G., Murray H. Development of a cyber risk assessment tool for Irish small business owners / M. Curtin, B. Sheehan, M. Gruben [et al.]. — 2024. — URL: https://arxiv.org/abs/2408.16124 (date of access: 15.05.2025). — Text: electronic.
10. Franco M.F., Künzler F., von der Assen J., Feng C., Stiller B. RCVaR: an economic approach to estimate cyberattacks costs using data from industry reports / M.F. Franco, F. Künzler, J. von der Assen, C. Feng, B. Stiller. — 2023. — URL: https://arxiv.org/abs/2307.11140 (date of access: 15.05.2025). — Text: electronic.
11. Huertas-García Á., Muñoz J., De Miguel Ambite E., Avilés Camarmas M., Ovejero J.F. DETECTA 2.0: Research into non-intrusive methodologies supported by Industry 4.0 enabling technologies for predictive and cyber-secure maintenance in SMEs / Á. Huertas-García, J. Muñoz, E. De Miguel Ambite, M. Avilés Camarmas, J.F. Ovejero. — 2024. — URL: https://arxiv.org/abs/2405.15832 (date of access: 15.05.2025). — Text: electronic.
12. National Institute of Standards and Technology (NIST). Guide for Conducting Risk Assessments: Special Publication 800-30, Revision 1 / Joint Task Force Transformation Initiative. — Gaithersburg, MD: National Institute of Standards and Technology, 2012. — 95 p. — URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (date of access: 15.05.2025). — Text: electronic.
13. Sukumar A., Mahdiraji H.A., Jafari-Sadeghi V. Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors / A. Sukumar, H. A. Mahdiraji, V. Jafari-Sadeghi // Risk Analysis. — 2023. — Vol. 43, No. 10. — P. 2082–2098. — URL: https://onlinelibrary.wiley.com/doi/full/10.1111/risa.14092 (date of access: 15.05.2025). — Text: electronic.
14. World Economic Forum. Global Cybersecurity Outlook 2024. — January 2024. — URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (date of access: 15.05.2025). — Text: electronic.