Секция «Риски и методы воздействия на риск в условиях цифровизации»

Оценка влияния киберрисков на предприятиях розничной торговли

Научный руководитель – Гришунин Сергей Вадимович

Егорова Александра Алексеевна
Выпускник (магистр)
Московский государственный университет имени М.В.Ломоносова, Экономический факультет, Кафедра математических методов анализа экономики, Москва, Россия
E-mail: alxegorova@gmail.com

Доклад посвящен представлению разработанного механизма управления рисками информационной безопасности (киберрисков) и модели оценки влияния таких рисков на предприятия сектора розничной торговли. Актуальность темы объясняется высокой подверженностью розничных компаний кибератакам и значительными финансовыми потерями предприятий от реализации киберрисков. По результатам исследований[1] на долю розничной торговли в 2018 году пришлось около 40% инцидентов кибератак, а финансовые убытки от киберрисков составили 50.6 млрд. долларов[2]. Убытки складываются как из прямых потерь (из-за недоступности информационных активов, искажения данных о ценах и запасах товаров, вывода денежных средств), так из-за косвенных потерь (оттока покупателей и поставщиков, потери репутации). Однако, существующие механизмы и методы оценки киберрисков обладают недостатками, не позволяющими использовать их в условиях, растущих информационных угроз. Обзор литературы показал: существующие модели CRAMM, FAIR, OCTAVE, TARA, COBIT for Risk, позволяют оценивать риски только на основании экспертных суждений относительно ущерба и вероятности киберриска с использованием балльных шкал. Такие подходы не позволяют (1) производить оценку рисков в денежном выражении; (2) оценивать их влияние на ключевые показатели эффективности бизнеса; (3) корректно учитывать корреляцию между рисками, и (5) «отслеживать» влияние киберугроз от источников возникновения до ключевых показателей эффективности компании (включая финансовые показатели). Существующие механизмы не позволяют обеспечить как координацию и интеграцию действий по управлению рисками, так и обеспечить возможность предоставления объективной количественной оценки влияния киберрисков.

Целью исследования являлась разработка механизма управления киберрисками и количественной модели оценки рисков информационной безопасности в розничной торговле. По результатам исследования выполнены следующие задачи: (1) предложены новые подходы к классификации, идентификации, оценке и управлению киберрисками; (2) разработана структурно-логической схема механизма управления киберрисками (включая детальное описание его отдельных блоков и моделей); (3) разработана и протестирована на реальных данных модель количественной оценки влияния киберрисков на ключевые показатели эффективности и финансово-экономические метрики предприятий розничной торговли; и (4) предложена модель оценки эффективности мероприятий по управлению киберрисками. Теоретической и методологической базой исследования послужили труды зарубежных и российских исследователей в области корпоративных финансов, управления рисками и кибербезопасности. Были использованы работы: Д. Хуббарда, А. Рефсдала, Ф. Фанстона и С. Вагнера, Д. Антонуцци И. Котенко, Ю. Черданцевой, И. Ивашковской и др. Учтены рекомендации стандартов информационной безопасности, таких как ИСО 27005, а также стандартов риск-менеджмента (COSO, ISO 31000) [18]. В ходе исследования были использованы такие методы, как системный подход к изучению проблемы исследования,

фундаментальные теоретические положения, изложенные в источниках. Применен следующий инструментарий: (1) диаграмма «галстук-бабочка» для идентификации рисков; (2) методы статистического анализа данных; (3) имитационное моделирование с помощью метода Монте-Карло; и (4) метод «микроморт» для оценки параметров распределения вероятностей.

Представленный механизм управления киберрисками и модель оценки рисков информационной безопасности устраняют методологические и функциональные изъяны в части управления киберрисками, выделенные в литературе. Механизм обеспечивает интеграцию и координацию действий по управлению рисками между менеджментом и службой информационной безопасности, а разработанная модель оценки рисков информационной безопасности позволяет рассчитывать доверительные интервалы значений финансовых показателей розничной компании с учетом влияния киберрисков, выделять и приоритезировать степень влияния основных источников угроз, что в результате дает полную и объективную оценку киберрисков. Научную новизну представляет и расширенный функционал модели оценки киберрисков, который позволяет (1) анализировать вклад отдельных рисков и, при необходимости, добавлять или исключать риски из анализа; (2) учитывать корреляцию между рисками; (3) задавать четкий период прогнозирования; (4) рассчитывать, ожидаемый, неожиданный и критический уровень потерь в денежном выражении и (5) позволяет строить прогнозы даже в условиях ограниченной информации о киберугрозах. Наконец, модель позволяет «прослеживать» киберриски от источников их возникновения до финансовых показателей компании, что с высокой точностью позволяет выявить источники прогнозируемого ущерба на самой ранней стадии.

Разработанная модель построена и протестирована на основании статистических данных об уязвимостях и инцидентах информационной безопасности в российских розничных компаниях. Прогнозы, выполненные по модели, являются статистически обоснованными и помогут повысить эффективность бизнеса за счет детальной оценки киберугроз и разработки эффективных мероприятий по управлению ими. Апробация механизма модели в крупной российской розничной сети по продаже техники для дома показала возможность сокращения ущерба от операционных рисков (включая кибератаки) до 30%. Это подтверждает высокую практическую применимость разработанных инструментов.

Доклад состоит из введения, трех основных разделов и заключения. В введении осуществлена постановка проблемы, обоснована актуальность темы, представлены выводы по обзору литературы, объяснен выбор методологии и инструментария, описаны статистические данные. В первом разделе приведена детализация разработки и результаты тестирования модели, описаны ее основные достоинства и недостатки. Во-втором разделе, во-первых, предложена блок схема механизма управления киберрисками и модель оценки киберрисков с описанием порядка использования и интеграции в практику управления рисками. Во-вторых, предложен подход к анализу эффективности мероприятий по управлению киберрисками, позволяющий выбирать оптимальные меры по снижению последствий киберрисков до допустимого уровня. В третьем разделе представлены результаты апробации модели на практике и подтверждена возможность ее практического применения. В *заключительном слове* нами представлены выводы по исследованию, а также направления дальнейших исследований авторов по развитию механизма управления и модели оценки рисков информационной безопасности.

[1] См, например, аналитический отчет консультационной компании Akmai Technologies за 2018 год, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-executive-summary-2019.pdf

[2] См, исследование Национальной Федерации розничной торговли совместно с Флоридским университетом https://nrf.com/sites/default/files/2019-06/NRSS%202019.pdf

Источники и литература

1) Antonucci, D.: The cyber risk handbook: creating and measuring effective cyber-security capabilities. Wiley Finance, NJ (2017).

2) Gusmao, A., Poleto, T., Silva, M., Silva, L.: Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management 43(6), 248-260 (2018).

3) Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology (2018).

4) Grichounine, S.: Developing the mechanism of qualitative risk assessment in strategic controlling. SPbSPU Journal. Economics 10(2), 64-74 (2017).

5) Ivashkovskaya, I., Stepanova, A.: Does strategic corporate performance depend on corporate financial architecture? Empirical study of European, Russian and other emerging market's firms. Journal of Management and Governance, 15(4), 603-616

6) ISO/IEC 27005:2013. Information technology - security techniques - information secu-rity risk management. International Organization for Standardization, (2005).

7) Grishunin, S., Suloeva S., Nekrasova, T., Egorova, A.: Development of the Mechanism of Assessing Cyber Risks in the Internet of Things Projects. In: Galinina, O., Andreev, S., Koucheryavy Y. (eds) NEW2AN ruSMART 2019, LNCS, vol. 11660, pp. 481-494. Springer, Heidelberg (2019).

8) Grishunin, S., Mukhanova, N., Suloeva, S.: Development of concept of risk controlling for industrial enterprise. Organizer of Production 26(1), 45-46 (2018).

9) Filko, S., Filko I.: Risk controlling of information security. Accounting, analysis and audit: theoretical and practical problems, SSAU 16, 123-127 (2016).

10) Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K.: A review of cyber security risk assessment methods for SCADA systems. Computers & Security 56, 1-27 (2016).

11) Kotenko, I., Chechulin, A.: A cyber attack modeling and impact assessment frame-work. In: 5th International Conference on Cyber Conflict Proceedings, pp. 1-24. IEEE, Tallinn (2013).