УДК 336.7

179. КИБЕРРИСКИ И ИХ ВЛИЯНИЕ НА ФИНАНСОВУЮ СТАБИЛЬНОСТЬ И СТОИМОСТЬ КОМПАНИЙ

Хорольский Н.В., студент гр. 477603
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лазаревич И. М. – канд. экон. наук, доц.

Аннотация. В современной глобальной экономике с тотальной цифровизацией бизнес-процессов вопрос обеспечения информационной безопасности трансформировался из технической задачи в фундаментальную проблему корпоративного управления и макроэкономической стабильности [1]. Актуальность исследования обусловлена тем, что информация стала ключевым активом, а способность компании защищать данные напрямую коррелирует с ее способностью генерировать прибыль и сохранять доверие инвесторов [2]. В экономическом контексте киберриски можно определить как форму финансовой угрозы, возникающую вследствие критической зависимости бизнеса от уязвимости информационных систем [3]. Особенность данных рисков заключается в их трансграничном характере и способности воздействовать на весь рынок, создавая предпосылки для системных кризисов [4].

Ключевые слова. Киберриски, финансовая стабильность, стоимость компании, кибербезопасность, рыночная капитализация, системный риск, цифровая экономика, утечка данных, киберустойчивость, количественная оценка рисков, метод дисконтированных денежных потоков, стоимость капитала, корпоративное управление, киберстрахование, финансовое хеджирование, волатильность акций, программы-вымогатели, атаки на цепочки поставок, инвестиционная привлекательность.

Для формирования целостного представления о проблеме необходимо определить место киберриска в системе экономических отношений. В научной литературе он рассматривается как подвид операционного риска, обладающий уникальными свойствами: транзитивностью (способностью передаваться между контрагентами), высокой скоростью реализации и асимметричностью информации [5].

С точки зрения теории информационной безопасности, сущность киберрисков раскрывается через триаду свойств информации, закрепленную в документах Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК) [6]:

1. Нарушение конфиденциальности: Несанкционированный доступ к чувствительной информации, что для публичной компании означает потерю интеллектуальной собственности и деловой репутации.
2. Нарушение целостности: Модификация финансовых реестров или данных, что подрывает доверие к достоверности отчетности.
3. Нарушение доступности: Блокировка доступа к сервисам, ведущая к остановке операционной деятельности.

Эволюция киберугроз обусловлена рядом фундаментальных факторов. Во-первых, это экспоненциальный рост цифровизации. Согласно отчету Всемирного экономического форума, киберпреступность институционализировалась и входит в пятерку главных глобальных рисков [7]. Во-вторых, наблюдается технологическое усложнение атак за счет использования искусственного интеллекта. Как отмечает Группа экспертов G7 по кибербезопасности, злоумышленники используют генеративные нейросети для автоматизации атак и создания гиперреалистичных фишинговых сообщений [8]. В-третьих, геополитическая напряженность трансформировала кибератаки в инструмент государственного воздействия, что подтверждается данными Международного валютного фонда [9].

На современном этапе выделяются три основных вида угроз, оказывающих наибольшее влияние на корпоративный сектор:

1. Программы-вымогатели: Использование вредоносного ПО для шифрования данных с целью получения выкупа. Тренд последних лет – рост атак на 75 % и развитие модели «вымогательство как услуга» [10].
2. Утечки данных: Хищение конфиденциальной информации, влекущее регуляторные штрафы и репутационный крах.
3. Атаки на цепочки поставок: Компрометация программного обеспечения поставщиков для скрытого доступа к целевым организациям.

Влияние киберрисков на экономику реализуется на двух уровнях: макроуровне (финансовая стабильность системы) и микроуровне (стоимость конкретной компании).

Высокая взаимосвязанность финансовых институтов создает каналы для «заражения». Атака на ключевой инфраструктурный узел способна вызвать каскадный эффект. Отчет Федеральной резервной системы США подчеркивает, что локальный сбой может привести к кризису ликвидности и панике на рынках [11]. Практика показывает, что киберриски способны наносить трансграничный ущерб.

Примером служит атака на Центральный банк Бангладеш через систему межбанковских сообщений SWIFT, доказавшая уязвимость глобальной финансовой инфраструктуры [12]. Другим примером является вирус-шифровальщик NotPetya, ущерб от которого превысил 10 миллиардов долларов по всему миру [13].

На корпоративном уровне киберриски трансформируются в финансовые потери через изменение фундаментальных показателей оценки бизнеса. Наиболее репрезентативной моделью для анализа является метод дисконтированных денежных потоков. Согласно классической финансовой теории, текущая стоимость бизнеса определяется как сумма ожидаемых в будущем свободных денежных потоков, приведенных к текущему моменту времени [14]. Негативное воздействие киберинцидентов на параметры данной модели осуществляется по нескольким ключевым направлениям.

Во-первых, происходит снижение денежных потоков. Это обусловлено прямыми потерями: расходами на расследование инцидента и восстановление систем, которые, по данным корпорации IBM, в среднем составляют 4,88 млн долларов на инцидент [15]. К этому добавляются юридические издержки и штрафы, которые в рамках Общего регламента по защите данных (GDPR) могут достигать 4 % от годового оборота [16]. Существенным фактором является потеря выручки от простоя бизнеса, как в случае с компанией Clorox, потерявшей значительную часть квартальной прибыли из-за кибератаки [17].

Во-вторых, наблюдается рост стоимости капитала. Ставка дисконтирования отражает рискованность вложений в актив. Инвесторы воспринимают киберуязвимость как дополнительный риск, что ведет к росту волатильности акций и увеличению премии за риск. Рейтинговые агентства включают киберустойчивость в кредитный рейтинг, снижение которого ведет к удорожанию заемного финансирования. Рост средневзвешенной стоимости капитала математически снижает справедливую стоимость акций.

В-третьих, происходит разрушение нематериальных активов. Для современных компаний деловая репутация (гудвилл) и бренд составляют основную часть стоимости. Утечка данных, как в случае с бюро кредитных историй Equifax (падение капитализации на 35 %), разрушает доверие клиентов, что ведет к долгосрочному снижению доли рынка [18]. Эмпирические исследования Национального бюро экономических исследований США подтверждают статистически значимую отрицательную реакцию фондового рынка на объявления об инцидентах [19].

Особую роль киберриски играют в сделках слияния и поглощения. Технологический аудит стал обязательным этапом сделок. Выявление скрытых уязвимостей ведет к дисконтированию (снижению) цены покупки, как это произошло в сделке телекоммуникационного холдинга Verizon и интернет-компании Yahoo, где цена была снижена на 350 млн долларов после раскрытия информации об утечках [20].

Для управления описанными угрозами необходим переход от качественных оценок к количественному моделированию. Передовым подходом является внедрение метрики Кибер-стоимость под риском (Cyber Value at Risk). Согласно исследовательской компании Gartner, данный метод позволяет рассчитать максимальный вероятный финансовый убыток на заданном горизонте с определенной доверительной вероятностью [21]. Это позволяет интегрировать киберриск в систему финансового планирования и обосновывать инвестиции в информационную безопасность.

В целях минимизации влияния киберрисков на стоимость бизнеса и обеспечения финансовой устойчивости для менеджмента компаний и корпоративного сектора предлагается комплекс стратегических мер:

1. Интеграция в корпоративное управление: Киберриск должен признаваться ключевым бизнес-риском. Необходим отказ от техноцентричного подхода в пользу риск-ориентированного управления на уровне Совета директоров.

2. Финансовое хеджирование: Использование киберстрахования позволяет трансформировать неопределенный риск катастрофических убытков в прогнозируемые операционные расходы, снижая волатильность денежных потоков [22].

3. Операционная устойчивость: Внедрение архитектуры «нулевого доверия» и создание изолированных контуров резервного копирования для минимизации последствий атак программ-вымогателей.

4. Коллективная безопасность: Участие в отраслевом обмене информацией об угрозах и взаимодействие с регуляторами для превентивного реагирования на системные угрозы.

Таким образом, результаты исследования свидетельствуют о фундаментальной трансформации киберрисков из технической категории в ключевой фактор экономической среды, определяющий финансовую устойчивость и инвестиционную привлекательность бизнеса. Выявленная взаимосвязь между уязвимостью информационных систем и рыночной капитализацией подтверждает, что игнорирование цифровых угроз ведет к неизбежной эрозии акционерной стоимости через механизмы снижения денежных потоков и роста стоимости капитала.

Преодоление данных вызовов требует перехода к комплексной стратегии управления, включающей интеграцию вопросов кибербезопасности в приоритеты Совета директоров, применение

методов количественного моделирования потерь и использование инструментов финансового хеджирования. Практическая реализация предложенного комплекса мер позволит минимизировать волатильность финансовых результатов, оптимизировать структуру капитала и обеспечить долгосрочную конкурентоспособность компании в условиях цифровой экономики.

Список использованных источников:

1. State of cybersecurity resilience 2023 : report / Accenture. – URL: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Of-Cybersecurity-2023.pdf (date of access: 13.03.2026).

2. Global cybersecurity outlook 2024 : insight report / World Economic Forum. – Geneva, 2024. – URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf (date of access: 13.03.2026).

3. Cyber risk : staff report / International Monetary Fund. – 2024. – URL: https://www.imf.org/en/Topics/cybersecurity (date of access: 13.03.2026).

4. SRC statement on financial system cyber risk resilience / Systemic Risk Council. – 2020. – URL: https://www.systemicriskcouncil.org/2020/02/src-statement-on-financial-system-cyber-risk-resilience/ (date of access: 13.03.2026).

5. Cyber resilience : range of practices / Basel Committee on Banking Supervision. – Basel : BIS, 2018. – URL: https://www.bis.org/bcbs/publ/d454.pdf (date of access: 13.03.2026).

6. Information technology. Security techniques : ISO/IEC 27000:2018. – URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (date of access: 13.03.2026).

7. The global risks report 2024 / World Economic Forum. – Geneva, 2024. – URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (date of access: 13.03.2026).

8. G7 Cyber Expert Group statement on AI and cybersecurity / US Department of the Treasury. – 2024. – URL: https://home.treasury.gov/system/files/136/G7-CEG-Statement-AI-Cybersecurity.pdf (date of access: 13.03.2026).

9. Global financial stability report, April 2024 / International Monetary Fund. – Washington, 2024. – URL: https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024 (date of access: 13.03.2026).

10. 2024 global threat report / CrowdStrike. – 2024. – URL: https://go.crowdstrike.com/rs/281-OBQ-266/images/Global-Threat-Report-2024.pdf (date of access: 13.03.2026).

11. Cybersecurity and financial system resilience report / Federal Reserve. – Washington, 2024. – URL: https://www.federalreserve.gov/publications/files/cybersecurity-and-financial-system-resilience-report-202406.pdf (date of access: 13.03.2026).

12. Bangladesh Bank hackers stole $81m via SWIFT system // BBC News. – 2016. – URL: https://www.bbc.com/news/world-asia-35765646 (date of access: 13.03.2026).

13. The untold story of NotPetya, the most devastating cyberattack in history // Wired. – 2018. – URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (date of access: 13.03.2026).

14. Бригхэм, Ю. Финансовый менеджмент : полный курс : в 2 т. / Ю. Бригхэм, Л. Гапенски. – СПб. : Экономическая школа, 2021. – 497 с.

15. Cost of a data breach report 2024 : report / IBM Security. – 2024. – URL: https://www.ibm.com/downloads/cas/1ZMX7Z24 (date of access: 13.03.2026).

16. Regulation (EU) 2016/679 (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (date of access: 13.03.2026).

17. Clorox says cyberattack will weigh on earnings // The Wall Street Journal. – 2023. – URL: https://www.wsj.com/articles/clorox-cyberattack-earnings-impact-116666666 (date of access: 13.03.2026).

18. Equifax's market value falls 30% after data breach // Reuters. – 2017. – URL: https://www.reuters.com/article/us-equifax-breach-idUSKCN1BR2L4 (date of access: 13.03.2026).

19. The effect of data breaches on market value : working paper / National Bureau of Economic Research. – 2022. – URL: https://www.nber.org/system/files/working_papers/w29999/w29999.pdf (date of access: 13.03.2026).

20. Verizon, Yahoo agree to lowered $4.48 billion deal // Reuters. – 2017. – URL: https://www.reuters.com/article/us-yahoo-m-a-verizon-idUSKBN1601C0 (date of access: 13.03.2026).

21. The Gartner cyber risk quantification guide / Gartner. – 2023. – URL: https://www.gartner.com/en/audit-risk/trends/cyber-risk-quantification (date of access: 13.03.2026).

22. Allianz risk barometer 2024 / Allianz Global Corporate & Specialty. – Munich, 2024. – URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2024.pdf (date of access: 13.03.2026).

UDC 336.7

CYBER RISKS AND THEIR IMPACT ON FINANCIAL STABILITY AND COMPANY VALUE

Khorolski N.V., student gr. 477603
Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Lazarevich I. M. – Candidate of Economic Sciences, Associate Professor

Annotation. In the modern global economy, characterized by the total digitalization of business processes, the issue of ensuring information security has transformed from a technical task into a fundamental problem of corporate governance and macroeconomic stability [1]. The relevance of this research is due to the fact that information has become a key asset, and a company's ability to protect data directly correlates with its ability to generate profits and maintain investor confidence [2]. In an economic context, cyber risks can be defined as a form of financial threat arising from the critical dependence of business on the vulnerability of information systems [3]. A specific feature of these risks lies in their cross-border nature and their capacity to impact the entire market, creating prerequisites for systemic crises [4].

Keywords. Cyber risks, financial stability, company value, cybersecurity, market capitalization, systemic risk, digital economy, data breach, cyber resilience, quantitative risk assessment, discounted cash flow method, cost of capital, corporate governance, cyber insurance, financial hedging, stock volatility, ransomware, supply chain attacks, investment attractiveness.