БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Экономический факультет

ЭКОНОМИКА, ФИНАНСЫ И АУДИТ: ПРОБЛЕМЫ, ПРИОРИТЕТЫ И ПЕРСПЕКТИВЫ

Материалы
I Международной научно-практической конференции

Минск, 24 октября 2025 г.

Научное электронное издание

Минск, БГУ, 2026

ISBN 978-985-881-937-8

УДК 338.2(06)+336(06)
ББК 65.05я431+65.26я431

Экономика, финансы и аудит: проблемы, приоритеты и перспективы : материалы I Междунар. науч.-практ. конф., Минск, 24 окт. 2025 г. / Бел. гос. ун-т ; редкол.: А. А. Королёва (гл. ред.) [и др.]. – Минск : БГУ, 2026. – 1 электрон. опт. диск (CD-ROM). – Текст : электронный. – ISBN 978-985-881-937-8.

Представлены исследования отечественных и зарубежных авторов по актуальным вопросам современного состояния мировой и национальной экономики. Рассмотрены механизмы обеспечения финансовой устойчивости хозяйствующих субъектов, а также современные тренды в области аудита и финансового контроля. Особое внимание уделено цифровой трансформации экономических процессов, внедрению инновационных методов управления и поиску путей адаптации бизнеса к меняющейся информационной системе.

Минимальные системные требования:
PC, Pentium 4 или выше; RAM 1 Гб; Windows XP/7/10; Adobe Acrobat.

Оригинал-макет подготовлен в программе Microsoft Word

На русском и английском языках

В авторской редакции

Ответственный за выпуск *О. В. Машевская*
Компьютерная верстка *А. Н. Багрецовой*

Подписано к использованию 13.03.2026. Объем 4,8 МБ.

Белорусский государственный университет.
Управление редакционно-издательской работы.
Пр. Независимости, 4, 220030, Минск.
Телефон: (017) 259-72-40
e-mail: urir@bsu.by
http://elib.bsu.by

УДК 368.8

КИБЕРСТРАХОВАНИЕ КАК МЕХАНИЗМ УПРАВЛЕНИЯ ОСТАТОЧНЫМ РИСКОМ

А. А. Аванесов

аспирант, Российский университет дружбы народов имени Патриса Лумумбы, г. Москва, Россия, Arkady.avanesov@bk.ru

Статья посвящена исследованию возможности применения киберстрахования в качестве меры управления риском, в рамках исследования были проанализированы отраслевые отчеты, мировые стандарты, а также научные исследования зарубежных авторов. Выявлена возможность использования механизма в управлении остаточным риском, а также определены некоторые аспекты процесса киберстрахования: стимулирование общего уровня безопасности, вероятность возникновения морального риска, асимметрия информации.

Ключевые слова: киберстрахование; киберриск; цифровая экономика; управление риском; информационная безопасность.

CYBER INSURANCE AS A RESIDUAL RISK MANAGEMENT MECHANISM

A. A. Avanesov

postgraduate student, Patrice Lumumba Russian University of Friendship of Peoples, Moscow, Russia, Arkady.avanesov@bk.ru

The article is devoted to the study of the possibility of using cyber insurance as a risk management measure. The study analyzed industry reports, global standards, and scientific research by foreign authors. The possibility of using the mechanism in residual risk management was identified, and some aspects of the cyber insurance process were determined: the promotion of the overall level of security, the likelihood of moral risk, and information asymmetry.

Keywords: cyber insurance; cyber risk; digital economy; risk management; information security.

Растущая значимость управления киберрисками обусловлена цифровизацией экономики и ростом геополитического аспекта. Для достижения устойчивости цифровой экономики и ее развития, требуется развитие системы управления рисками, ведь последствия от этих рисков могут иметь системный и точечный характер, направленный на прерывание производственной деятельности, вплоть до потери прибыли, уничтожении имущества, а также возникновения ответственности перед третьими лицами.

Согласно опубликованному Барометру рисков 2025 от Allianz результат опросов респондентов отображает восприятие значимости киберисков в мировой экономике 38 % опрошенных поставили киберриски на первом место в рейтинги [1].

В другом исследовании Munich RE глобальных кибер рисков был проведен опрос по всему меру, в результате которого выяснилось, что 72 % респондентов крайне серьезно и серьезно оценивают последствия кибер рисков [2].

В глобальном исследовании «Risk in focus 2026» был проведен опрос более 800 внутренних аудиторов государственного и частного сектора, согласно опросу, наиболее высокий приоритет присвоен рискам кибербезопасности и защите данных, большинство специалистов отметили, что большую часть времени составляет именно аудит кибербезопасности [3].

В статистическим данным исследования «РТК-Солар» в 2024 году количество кибератак в РФ достигло 31 тыс., при этом наблюдается тренд на рост числа кибератак в каждом квартале 2024 г. Большинство кибератак направлены на государственный сектор, а также финансовую и транспортную отрасль [4].

Целью данного исследования является рассмотрение механизма киберстрахования, как меры управления остаточным риском. Для достижения данной цели был проведен качественный анализ научных исследований, международных отраслевых отчетов.

Управление киберриском или риском информационной безопасности в мире, как правило регламентируются стандартами ISO серии 27000. Но, компания «Bi.zone» предлагает использовать комбинированный подход с использованием также стандарта серии ISO 31000.

Суть данного подхода заключается в расширении охвата зоны риска, для определения конечного ущерба для бизнес-процесса. Данный подход позволяет провести отбор наиболее важных и опасных для бизнеса реализуемых сценариев убытка. Учитывая характер киберриска и быструю его обучаемость несмотря на применение технических и организационных мер по управление киберрисками, риск наступления события все же остается, в том числе в отношении рисков, которые могли быть оценены, как менее приоритетные. Тем самым, оставшийся остаточный риск по итогу принятых технических мер требует дополнительных мер [5].

Учитывая данную потребность, страховщиками был разработан механизм страхования информационных рисков или киберрисков. В покрытии киберстрахования наиболее часто встречается: ответственность перед третьими лицами, ущерб в результате перерыва производственной деятельности, возмещение расходов. Исходя из вышеперечисленного покрытия, можно сделать вывод о том, что страхование может служить мерой управления остаточным риском и инструментом повышения общего уровня системы управления рисками, но несмотря на это без применения базовых эффективных технических мер по защите системы и организационных мер по контролю первичного риска механизм страхования остаточного риска не имеет смысла.

В исследовании Халили М, М. Лю М., Романоски С., посвященном оценки киберриска в киберстраховании, авторы приходят к выводу о том, что киберстрахование несет в себе моральный риск [6]. Под моральным риском подразумевается возможное поведение страхователя после заключения договора страхования, выражающегося в снижении заинтересованности поддержания уровня безопасности ИТ-систем, а также прекращении планирования по улучшению уровня безопасности страхователем. В связи с этим, в рамках процесса страхования страховщику целесообразно применять стимулирующие меры по повышению общего уровня безопасности страхователя. В данном случае стимулом для страхователя может быть снижение цены договора страхования в обмен на выполнение компенсирующих технических мер по безопасности. Снижение цены договора страхования и выполнение компенсирующих мер при наличии договора страхования может быть весьма эффективным дополнением общей системы управления рисками компании.

Несмотря на преимущества и возможности использования киберстрахования в качестве меры управления риском, возникают некоторые вопросы требующие решения. К примеру, асимметрия информации между страхователем и страховщиком, при которой стороны не всегда готовы достоверно и открыто делиться необходимой информацией для полноценной оценки риска и более справедливого определения условий страхования [7]. При этом страхователь не всегда понимает в каких случаях точно будет произведена выплата, а в каких случаях нет. Данные проблемы являются следствием незрелости рынка страхования киберрисков, учитывая, что данный вид киберстрахования является совсем новым в большинстве стран мира.

По итогу проведенного исследования, можно выделить следующие выводы:

- процесс цифровизации экономика является причиной поиска мер управления киберрисками;

- механизм киберстрахования может быть использован, как мера управления остаточным риском, но не первичным;

- процесс страхования киберрисков влечет к моральному риску, что является стимулом страховщика в стимулировании страхователя к увеличению техническим мер безопасности ИТ-систем;

- асимметрия информация, отсутствие понимания покрытия страхования является признаком незрелости рынка киберстрахования.

Библиографические ссылки

1. Отчет «Барометр рисков Allianz, определяющий основные бизнес-риски на 2025 год» // URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf.

2. Отчет «Глобальное исследование киберрисков и страхования в 2024 году» / URL: https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html.

3. Отчет, «Risk in Focus 2026» URL: https://www.eciia.eu/2025/09/risk-in-focus-2026-hot-topics-for-internal-auditors/.

4. Отчет РТК-Солар, «Кибератаки на российские компании в 2024 году». 2025. URL: https://rt-solar.ru/analytics/reports/5320/.

5. Эл. Ресурс / Bi.zone. Управление киберрисками. Как определить главные угрозы для компании. URL: https://bi.zone/expertise/business-continuity-management/cyber-risk-management/.

6. *Khalili M. M., Liu M.* Embracing and controlling risk dependency in cyber-insurance policy underwriting // Journal of Cybersecurity. 2020. URL: https://www.researchgate.net/publication/336677735_ Embracing_and_controlling_risk_dependency_in_cyber-insurance_policy_underwriting.

7. *Shettya S., McShanea M., Zhangb L., Kesanb J. P., Kamhouac C. A., Kwiatc K., Njillac L. L.* Reducing Informational Disadvantages to Improve Cyber Risk Management // The Geneva Papers. 2018. URL: https://www.researchgate.net/publication/322962330_Reducing_Informational_Disadvantages_to_Improve_Cyber_Risk_Management.