УДК 368.8

СИСТЕМНОСТЬ КИБЕРРИСКА ПРИ СТРАХОВАНИИ ИНФОРМАЦИОННЫХ РИСКОВ

Аванесов Аркадий Артемович, аспирант, Высшая школа управления, РУДН

Аннотация

В статье рассматривается влияние системности киберриска в страховании информационных рисков. В рамках исследования определена сущность киберриска, а также основные возможности страхового рынка в рамках управления риском с учетом характера системности киберриска в кибер страховании. Для достижения цели был проведен анализ исследований отечественных, зарубежных исследователей, а также отраслевые отчеты. Статья подготовлена в качестве доклада для секции «Образование для устойчивого развития территорий» IV ежегодной международной научно-практической конференции «Цифровая трансформация международной экономической системы» (2 октября 2025 г., МГИМО МИД России).

КЛЮЧЕВЫЕ СЛОВА: цифровизация экономики, киберриск, системность киберриска, страхование киберрисков, управление риском.

SYSTEMATIC CYBER-RISK IN INFORMATION RISK INSURANCE

Avanesov Arkady Artemovich, postgraduate student, Higher School of Management, RUDN University

Abstract

This article examines the impact of a systematic cyber risk on information risk insurance. The study defines the nature of cyber risk, as well as the insurance market's key risk management opportunities, taking into account the systemic nature of cyber risk in cyber insurance. To achieve this goal, a review of studies by domestic and international researchers, as well as industry reports, was conducted.
The article was prepared as a report for the section "Education for Sustainable Development of Territories" of the IV annual international scientific and practical conference "Digital Transformation of the International Economic System" (October 2, 2025, MGIMO University of the Ministry of Foreign Affairs of Russia).

KEYWORDS: digitalization of the economy, cyber-risk, systemic cyber risk, cyber risk insurance, risk management.

Цифровизация экономики является ведущим мировым трендом позволяя государству, потребителям и производителям услуг, товаров увеличивать эффективность своей деятельности, обслуживания граждан благодаря цифровизации процессов. Но данные преимущества имеют и обратную сторону, которые выражаются в постоянно растущим количестве киберинцидентов, при этом наличие постоянного геополитического аспекта только увеличивает вероятность киберинцидентов и расширяет зоны охвата среды риска. Учет данного фактора риска формирует негативный характер возможности его реализации, в том числе при поиске решений смягчения последствий путем использования механизма страхования киберрисков.

Цель исследования: определить влияние системности киберриска в рамках процесса страхования киберрисков».

Для достижения данной цели сформулированы задачи:

- определить сущность системности киберриска в рамках цифровизации экономики;
- определить основные возможности страхового рынка в рамках управления риском с учетом характера системности киберриска.

Материалы и методы исследования

В рамках данного исследования использованы теоретические методы исследования. Для решения задач были применены методы анализа, синтеза, индукции. Материалами исследования являются научные статьи отечественных, зарубежных авторов, а также отраслевые отчеты зарубежных компаний.

Для определения сущности системности киберриска был проведен анализ исследования Белозёрова С. А., Соколовской Е. В, и отраслевых отчетов зарубежных компаний путем сравнения различных концепций. Далее в рамках анализа зарубежных исследований путем синтеза, индукции и дедукции были определены основные подходы решения проблематики исследования.

Результаты и обсуждение

Белозёров С. А., Соколовская Е. В., в своем исследовании выделяют несколько ключевых факторов роста масштаба последствий реализации киберрисков приведем одни из наиболее критичных факторов: рост цифровизации финансового сектора, системный характер киберрисков, который имеет негативное фактор [1].

В этом же исследовании [Белозёров С. А., Соколовская Е.,2023] приходят к выводу о том, что «рост кибератак является одним из наиболее значимых современных вызовов для отрасли страхования, усугубляемым последствиями геополитической напряженности. Реализация киберрисков приобретает системный характер, а объем операционных убытков не подлежит страхованию в полном объеме» [1].

На основании проведенного анализа зарубежных источников можно выделить две концепции:

Концепция согласно исследованию Мирового валютного фонда.
В этом исследовании [Тамаш Г., Франк А., Морозова А., Уилсон К.,2019] авторами предложена концепция «системного киберриска», которая подразумевает возможность единичного события или развития события вызывать широкомасштабные сбои и негативные последствия, охватывающие множество организаций [2].

При этом, справедливо утверждение о том, взаимозависимости являются причиной возникновения характера системности киберриска и последующего возникновения

накопительного эффекта, что затрудняет его оценку и управлением им заинтересованными лицами.

Также, существует иная концепция страховой отрасли. В исследовании [С. Склафейн,2021] на базе Munich RE выявлены тенденции роста выдачи полисов страхования киберрисков, а также отображены результаты опроса страховщиков. Согласно результатами опроса «многие профессионалы отрасли считают киберриск системным, если он не подлежит страхованию исходя из масштаба потенциальных убытков, соотношения потерь между многими клиентами, секторами и регионами, а также сложности моделирования и хеджирования» [3]. Перечисление данных факторов подразумевает накопительный эффект системности киберрисков.

Согласно отчету, AIG от 2017 года, «системный киберриск» определяется как киберсобытие способное повлиять на множество компаний одновременно [4].

Стоит отметить, что на текущий момент несмотря на наличие различных концепций определения системного кибериска, единого понятия не существует.

В качестве яркого примера системного инцидента можно привести события 2017 года, когда хакеры, использовавшие шифровальщик WannaCry, эксплуатировали уязвимость в Windows. Это привело к тому, что в течение одного дня была нарушена безопасность более 230 000 компьютерных систем [5].

Программа NotPetya, которая притворялась шифровальщиком, использовала уязвимость в украинском программном обеспечении для подготовки налоговых деклараций. Это позволило ей осуществить атаку на международные корпорации, причиняя ущерб, оцениваемый примерно в 10 миллиардов долларов [6].

Учитывая критичность накопления кибериска в результате событий, которые могут привести к системным последствиям убытков в результате перерыва производственной деятельности, хищения данных, ответственность перед третьими лицами для страховщиков является негативным эффектом, так как окончательный размер ущерба и потенциальных потерь может превысить прогнозируемые потери страховщика.

Тем не менее, в исследовании [Д. Форси, Д. Бейтмана, 2022] авторы рассматривают возможность разработки механизма компенсации ущерба при возникновении реализации киберриска в рамках государственного партнерства. Суть данного механизма заключается в передачи определенной части элементов системных киберрисков от страховщика к государству по итогу достижения определенного уровня размера убытка, согласно мнению авторов, данный механизм позволит привлечь больше частного капитала на рынок и более

упорядочить порядок возмещения выплат [7]. Аналогичный механизм успешно применяется в наиболее сложных сферах страхования, таких как экстремальные погодные условия, ядерная энергетика, торговые кредиты. При этом применение данного механизма позволит расширить покрытие страхования и увеличить предложение на рынке страхования.

Аналогично Европейское управление по страхованию в своем исследовании «Стратегии Киберандеррайтинга» приходит к заключению, что вероятность возникновения системных рисков при реализации киберинцидентов, может требовать государственного реагирования с целью поддержки страхового рынка и устойчивости экономики [8].

Несмотря на критичность накопления взаимосвязанных рисков при страховании информационных рисков, проблема оценки риска страховщиком является одновременно и стимулом поиска решений в рамках принятия решений об отказе, передачи, принятии риска.

Так, например, в исследовании [М. Халили, М. Лю, А. Романовски,2019] авторы описывают, как зависимость от киберрисков может быть учтена при заключении полисов киберстрахования [9]. В рамках своего исследования авторы выявляют основную причину системного риска, проявляющийся в взаимозависимости бизнеса между организациями в результате аутсорсинга или отношений в цепочке поставок. В этих случаях состояние безопасности одной фирмы зависит не только от ее собственных усилий, но и от усилий других фирм. При этом, несмотря на отказ страховщиков страховать зависимые риски, существует нереализованный стимул страховщика страховать данные риски. Основной смысл возможности страхования зависимости риска сети страхователей заключается в совместной разработке политики, которая стимулирует страхователей коллективно прилагать больше усилий в плане повышения уровня безопасности, что одновременно может привести к повышению уровня безопасности для всех зависимых рисков, по сравнению с страхованием независимых рисков страхователей и увеличения прибыли.

Согласно предложенному подходу справедливо утверждение о том, что страховая компания может получать более высокую прибыль, страхуя всех агентов (поставщиков услуг и их клиентов), при условии, что она должным образом мотивирует поставщиков услуг повышать уровень безопасности. Это связано с тем, что снижение рисков для поставщиков услуг приводит к снижению рисков для их клиентов, то есть выгода имеет мультипликативный эффект. В конечном счёте это не только позволяет страховой компании брать на себя риски всех агентов без ущерба для своей прибыли, но и способствует повышению общественного благосостояния.

Заключение

В рамках проведенного исследования получены следующие выводы:

- Цифровизация экономики и геополитическая ситуация является причиной роста системного характера киберрисков;
- Единого определения системности взаимозависимости киберрисков на текущий момент не сформировано, но при этом в рамках изученного и проанализированного материала можно, утверждать, что все концепции определений переплетаются между собой;
- Несмотря на взаимозависимость киберрисков, как фактора отказа от принятия риска на страхование, возможности рынка страхования в расширении зоны охвата рынка заключаются в формировании программ поддержки на государственном уровне;
- Возможность повышения уровня коллективной безопасности взаимозависимых страхователей в рамках принятия решения о страховании может сподвигнуть страховщиков к развитию стратегии и политики страхования информационных рисков с целью увеличения прибыли и зоны охвата рынка.

Литература

1. Белозёров С. А., Соколовская Е. В // Киберриски в условиях геополитических конфликтов: вызовы и возможности для страхования // Роль управления рисками и страхования в обеспечении устойчивости общества и экономики. Сборник трудов XXIV Международной научно-практической конференции. Отв. редакторы Е.В. Злобин, И.Б. Котлобовский. Москва, 2023. С. 190-194.
2. Надзор за рисками кибербезопасности / Кристофер Уилсон, Тамаш Гайдош, Фрэнк Адельманн и Анастасия Морозова // Международный валютный фонд, 2019.
3. Сюзанна Склафейн / Создание киберпространства - ключ к выживанию, считает исполнительный директор Munich Re // Управление перевозчиками 2021.
4. Является ли киберриск системным? / Американская международная группа (AIG), 2017[Электронный ресурс]. URL-адрес: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2017/cs2017_0167.pdf (Дата обращения: 31.08.2025)
5. Чарльз Купер / WannaCry: уроки, извлеченные 1 год спустя // Symantec, 15 мая 2018 г.
6. Ионут Аргире / NotPetya—Разрушительный очиститель, замаскированный под вредоносное ПО // Неделя безопасности, 29 июня 2017 г.

7. Дэвид Форси, Джон Бейтман, Ник Бикрофт и Бо Вудс. Системный киберриск: учебник, 2022.
8. Стратегия кибер-андеррайтинга / Европейское управление по страхованию и профессиональным пенсиям, 2022. [Электронный ресурс]. URL-адрес: https://www.eiopa.europa.eu/document-library/strategy/cyber-underwriting-strategy. (Дата обращения: 31.08.2025)
9. Мохаммад Махди Халили, Мингьян Лю, Саша Романоски / Учет и контроль зависимости от рисков при составлении полисов киберстрахования // Журнал кибербезопасности, Том 5, выпуск 1, 2019.