

5.2.4 Финансы (экономические науки)

Научная статья

УДК 368:004.056

ФИНАНСОВЫЕ ИННОВАЦИИ В СТРАХОВАНИИ КИБЕРРИСКОВ: ПРОБЛЕМЫ ОЦЕНКИ И УПРАВЛЕНИЯ КАПИТАЛОМ

**Галиуллина Гыльфия Фагимовна, Доктор экономических наук, Доцент,
Казанский (Приволжский) федеральный университет,
Набережночелнинский институт, Россия, Набережные Челны,
gyliya.10@yandex.ru**

Аннотация. Статья посвящена развитию подходов к оценке и финансовому управлению киберрисками в страховании. В условиях ускоренной цифровизации экономики киберриски приобретают характеристики, затрудняющие их количественную оценку в страховании: быстрое изменение угроз, дефицит однородной статистики, высокая тяжесть отдельных убытков, зависимость страхователей от общей технологической инфраструктуры и возможность одновременного возникновения требований по значительному числу договоров. Цель исследования состоит в разработке концептуального подхода к стресс-тестированию портфеля страхования киберрисков и определении направлений использования его результатов в андеррайтинге, перестраховании и управлении капиталом страховой организации. Методологическую основу составили системный и сравнительный подходы, анализ современной актуарной литературы, документов страховых регуляторов и международных отраслевых исследований. Предложено разграничивать идиосинкратический, систематический и системный компоненты киберриска и строить стресс-сценарии прежде всего вокруг факторов накопления убытков: общих программных уязвимостей, сбоев облачной инфраструктуры, компрометации цепочек поставок и масштабных кампаний программ-вымогателей. Обосновано, что результаты стресс-тестирования должны использоваться не для механического увеличения технических резервов, а как

дополнительный источник информации при установлении лимитов андеррайтинга, покупке перестраховочной защиты, оценке концентрации портфеля и внутреннем планировании капитала. Рассмотрены финансовые инновации, расширяющие возможности передачи киберриска, включая параметрические решения и страховые ценные бумаги, связанные с киберриском. Сделан вывод о необходимости сочетания актуарных, сценарных и технологических методов оценки с регулярным обновлением информации о взаимозависимости страхователей.

Ключевые слова: киберриски; киберстрахование; страхование киберрисков; актуарная оценка; накопление риска; стресс-тестирование; страховой капитал; перестрахование; страховые ценные бумаги; финансовые инновации.

Original article

Financial Innovations in Cyber Risk Insurance: Challenges in Capital Valuation and Management

Galiullina Giliya Fagimovna, Doctor of Economics, Associate Professor, Kazan (Volga Region) Federal University, Naberezhnye Chelny Institute, Russia, Naberezhnye Chelny, gyliya.10@yandex.ru

Abstract. The article focuses on the development of approaches to cyber risk assessment and financial management in insurance. In an increasingly digital economy, cyber risks exhibit characteristics that complicate insurance quantification, including rapidly evolving threats, limited homogeneous loss data, high-severity events, common technological dependencies and the possibility of simultaneous claims across a large number of policies. The aim of the study is to develop a conceptual framework for stress testing cyber insurance portfolios and to determine how its results can be incorporated into underwriting, reinsurance and insurers' capital management. The

methodological framework combines systemic and comparative approaches with an analysis of recent actuarial research, insurance supervisory publications and international industry studies. The paper proposes distinguishing between idiosyncratic, systematic and systemic components of cyber risk and designing stress scenarios primarily around major accumulation drivers, including common software vulnerabilities, cloud infrastructure outages, supply-chain compromises and large-scale ransomware campaigns. The study argues that stress-test results should not mechanically increase technical provisions but should serve as an additional source of information for underwriting limits, reinsurance purchasing, portfolio concentration assessment and internal capital planning. Financial innovations expanding cyber risk transfer capacity, including parametric solutions and cyber insurance-linked securities, are also examined. It is concluded that sustainable cyber insurance requires a combination of actuarial, scenario-based and technology-oriented assessment methods together with regular updating of information on policyholder interdependencies.

Keywords: cyber risk; cyber insurance; actuarial assessment; accumulation risk; stress testing; insurance capital; reinsurance; insurance-linked securities; financial innovation.

Введение. Цифровая трансформация экономической деятельности сопровождается ростом зависимости компаний от информационных систем, облачной инфраструктуры, программного обеспечения и цифровых цепочек поставок. Одновременно изменяется характер финансовых рисков: к традиционным операционным угрозам добавляются киберинциденты, способные приводить к прямым имущественным потерям, перерывам в деятельности, расходам на восстановление данных, ответственности перед третьими лицами и репутационным издержкам [1, 2, 13].

Российские исследования последних лет подтверждают системный характер цифровой трансформации страхового бизнеса. Д. И. Кулешова отмечает, что цифровизация повышает эффективность страховых процессов и

создаёт возможности для новых продуктов, но одновременно сопровождается увеличением киберрисков и требований к информационной безопасности [1]. В. И. Хабаров, М. С. Колбина и И. Ю. Кушелев связывают дальнейшую модернизацию страхового рынка с комплексным внедрением цифровых технологий и повышением качества управления инновациями [2].

Для страхования киберрисков цифровая взаимосвязанность имеет двойственное значение. С одной стороны, она формирует устойчивый спрос на страховую защиту. С другой стороны, общие программные продукты, облачные сервисы и технологические поставщики создают возможность одновременного возникновения убытков у большого числа страхователей. Именно это свойство отличает киберриск от значительной части традиционных рисков и затрудняет его диверсификацию внутри страхового портфеля [14, 15, 17].

Современная актуарная литература предлагает различать идиосинкратический, систематический и системный киберриск. Идиосинкратические события связаны с отдельным страхователем; систематические - с общим фактором или уязвимостью, воздействующей на несколько организаций; системные - с распространением риска по взаимосвязанной цифровой инфраструктуре [14]. Такой подход особенно важен для оценки накопления убытков, поскольку классическое предположение о независимости страховых событий для киберриска часто не выполняется.

Актуальность данной проблемы подтверждает и международная надзорная практика. IAIS рассматривает киберриски одновременно как собственный операционный риск страховщика и как риск, принимаемый посредством андеррайтинга, отмечая сохраняющиеся проблемы неоднозначности страхового покрытия, ценообразования и накопления убытков [20-22]. В декабре 2025 г. ЕЮРА отдельно выделило киберриск как потенциальный источник макрофинансовой нестабильности вследствие технологической взаимозависимости организаций и возможности значительных агрегированных убытков [19].

Обзор источников литературы. Научные исследования

киберстрахования развиваются по нескольким взаимосвязанным направлениям.

Первое направление посвящено цифровой трансформации страхового бизнеса. В работах российских авторов анализируются технологии искусственного интеллекта, больших данных, телематики, блокчейна, мобильных сервисов и автоматизации страховых процессов [1, 2]. Исследования показывают, что цифровизация одновременно повышает эффективность андеррайтинга и обслуживания клиентов и создаёт новые требования к управлению информационными и операционными рисками.

Второе направление непосредственно связано с экономической природой киберриска и возможностями его страхования. Российские публикации рассматривают проблемы формирования страховых продуктов, правового регулирования, информационной асимметрии и оценки ущерба [4, 6-12]. Вместе с тем значительная часть работ носит преимущественно описательный характер, тогда как для страховой организации принципиальное значение имеет не только идентификация угрозы, но и оценка её портфельной концентрации.

Третье направление образуют современные исследования моделирования и тарификации киберрисков. К. Awiszus и соавторы систематизируют идиосинкратические, систематические и системные киберриски и показывают, что классические актуарные модели остаются применимыми к отдельным типам риска, однако требуют усложнения при наличии взаимозависимости и сетевого распространения [14]. Исследование G. Zeller и M. Scherer показывает, что недоучёт структуры зависимости способен приводить к существенному искажению оценки накопленного портфельного риска [15].

Четвёртое направление связано с включением киберриска в модели капитала страховщика. J. Grewal и S. Cartagena подчёркивают необходимость учитывать динамичность угроз, внешние технологические факторы и зависимость отдельных киберэкспозиций при параметризации капитальных моделей [16]. Современные исследования страхового ценообразования также

показывают значимость тяжёлых хвостов распределения, корреляции и выбора адекватной поправки на риск [19].

Отдельным направлением становится альтернативная передача киберриска через рынки капитала. В условиях ограниченной ёмкости традиционного перестрахования рассматривается возможность использования ценных бумаг, связанных со страховыми рисками (ILS), и киберкатастрофических облигаций. The Geneva Association указывает, что развитие данных инструментов способно расширить доступную страховую ёмкость, однако требует повышения стандартизации договоров, качества моделей и прозрачности триггеров [17, 18].

В исследованиях 2026 г. всё больше внимания уделяется использованию искусственного интеллекта. Обзор А. Paragioudakis и соавторов показывает перспективность использования технической телеметрии, информации об уязвимостях и методов машинного обучения при страховой оценке риска [24].

Таким образом, в современной литературе всё больше внимания уделяется прикладной задаче измерения агрегированного воздействия киберриска на портфель и использования результатов такой оценки в андеррайтинге, перестраховании и внутреннем управлении капиталом.

Классические модели совокупного страхового убытка сохраняют значение при анализе киберрисков, однако их предпосылки требуют дополнительной проверки. Для части киберинцидентов может нарушаться предположение о независимости и одинаковом распределении страховых событий, поскольку несколько страхователей способны одновременно зависеть от одного программного продукта, облачного сервиса либо технологического поставщика [14, 15].

Кроме того, характер угроз является нестационарным: изменение используемых технологий и способов проведения атак способно достаточно быстро изменить как частоту событий, так и тяжесть убытков. Поэтому исторические страховые данные остаются важным информационным

источником, но не должны рассматриваться как единственная база прогнозирования будущих катастрофических потерь.

В этой связи наиболее обоснованным представляется комбинированный подход, включающий традиционный анализ частоты и тяжести убытков, выявление факторов общей технологической зависимости, сценарный анализ накопления и регулярное обновление исходных предположений [14-16, 19].

Материалы и методы исследования. Основу исследования составили аналитические отчеты международных перестраховочных компаний (Swiss Re Institute, Munich Re), данные регуляторов (Европейское управление пруденциального надзора - ЕВА, Национальная ассоциация страховых комиссаров США - NAIC), а также публикации в рецензируемых научных журналах по вопросам актуарной науки и управления финансовыми рисками.

Методологический аппарат включает системный анализ для декомпозиции факторов киберриска; метод экспертных оценок (метод Дельфи) для верификации и ранжирования стресс-сценариев; математическое и статистическое моделирование для построения распределений убытков; сравнительный анализ регуляторных подходов к оценке капитальных требований по киберрискам.

Для разработки методики стресс-тестирования был применен сценарно-параметрический подход. Вопросы формирования резервов исследованы через призму принципа осторожности с учетом требований современных стандартов платежеспособности (Solvency II, RBC). Особое внимание уделено синтезу традиционных актуарных методов с подходами, заимствованными из операционного риск-менеджмента в финансовом секторе.

Результаты исследования и их обсуждение. Предлагаемая методика основывается на сочетании детерминированных стресс-сценариев и вероятностного моделирования для оценки устойчивости капитала страховой организации. Ее цель заключается в оценке финансовых последствий реализации маловероятных, но правдоподобных событий.

Вместо общих сценариев (например, «крупная кибератака») формулируются конкретные, технологически детализированные сценарии, каждый из которых описывает определённый механизм накопления убытков. Примеры сценариев приведены в таблице 1.

Таблица 1 - Примеры стресс-сценариев для портфеля страхования киберрисков

Наименование сценария	Механизм реализации сценария	Охват портфеля	Временные параметры
Массовый криптографический сбой	Компрометация широко используемого алгоритма шифрования или протокола (TLS 1.3)	Все страхователи, использующие уязвимый протокол для передачи данных (оценка: 85% портфеля)	Волна убытков в течение 72 часов после публикации уязвимости
Атака на облачного провайдера	Распространение вредоносного ПО через инфраструктуру провайдера уровня AWS/Azure/GCP	Страхователи, чьи данные или приложения размещены у целевого провайдера (оценка: 25% портфеля)	Простой основных сервисов 24-96 часов
Координированная кибератака на критическую инфраструктуру	Координированные атаки на операторов энерго-, водо- и теплоснабжения в одном географическом регионе	Страхователи в целевых отраслях в регионе, а также их контрагенты (эффект второй волны)	Эскалация в течение 1 недели, восстановление – 2-4 недели

Источник: разработано авторами.

Для каждого сценария оценивается доля затронутых договоров (N) и строится функция распределения убытка (L) для каждого из них. Ввиду отсутствия достаточной статистики используется комбинация моделирования на основе экспертных оценок (экспертной группой определяются минимальный (L_{min}), наиболее вероятный (L_{mode}) и максимальный (L_{max}) убыток на один договор), Монте-Карло симуляции (на основе заданных параметров генерируется 100 000 итераций совокупного убытка по портфелю (AL) для сценария, где $AL = \sum L_i$. При этом учитывается положительная корреляция между индивидуальными убытками в рамках одного сценария, моделируемая с помощью копулярных функций (например, Гауссовой или t-копулы)).

Рассчитывается влияние совокупного убытка (AL) от каждого сценария на:

- коэффициент платежеспособности (SCR , на сколько процентных пунктов снизится SCR);
- чистые активы (абсолютное сокращение капитала);
- коэффициент убыточности ($Loss\ Ratio$) портфеля (рост на отчетную дату).

Результаты стресс-тестирования непосредственно используются в процессе резервирования и управления капиталом. Классический метод цепочки развития для формирования резервов по киберрискам неприменим в чистом виде из-за отсутствия сформированных треугольников убытков и длительного периода урегулирования, который для сложных инцидентов, связанных с судебными разбирательствами, может достигать 3-5 лет.

Предлагается динамический подход к формированию резервов, который включает два ключевых компонента:

1. Базовый резерв на основе вероятностной модели с учетом индекса урегулирования.

Резерв оценивается не только по известным и заявленным инцидентам ($IBNR$), но и включает компонент на потенциальные будущие инциденты по существующим договорам. Для его расчёта используются результаты моделирования методом Монте-Карло, в котором в качестве входных данных используются показатели частоты, скорректированные на индекс киберугроз (например, агрегированный индекс по данным компаний кибербезопасности). Формула (1) для оценки резерва на отчетную дату (t) может быть представлена как:

$$R_t = R_{IBNR}(t) + \sum (P_i * E[L_i] * K_{tail}) \quad (1)$$

где

$R_{IBNR}(t)$ - резерв по известным инцидентам (оценка методом Борнхюттера-Фергюсона);

P_i - вероятность киберинцидента для i -го договора в оставшийся срок действия;

$E[L_i]$ - математическое ожидание убытка при наступлении инцидента;

K_{tail} - коэффициент ($>>1$), калибруемый по результатам стресс-тестирования для учета системных и катастрофических событий.

2. Дополнительный буферный резерв, величина которого определяется, исходя из результатов стресс-тестирования. Целевой уровень буфера должен покрывать убыток, соответствующий 95-ому перцентилю распределения совокупного убытка по наиболее опасному из реалистичных сценариев, за вычетом перестраховочного покрытия.

Текущие стандарты Solvency II рассматривают киберриски в основном в рамках модулей страхового, операционного и рыночного рисков. Результаты исследования позволяют сформулировать конкретные предложения для регуляторов.

Сравнительный эффект от внедрения предложений по резервированию и капиталу отражен в таблице 2.

Таблица 2 - Сравнительный эффект от внедрения предложений по резервированию и капиталу (на примере портфеля с годовой премией 100 млн. руб.)

Показатель	Традиционный подход (цепочка развития)	Предлагаемый динамический подход	Эффект для финансовой устойчивости
Базовый резерв	45 млн. руб. (только IBNR)	60 млн. руб. (IBNR + прогнозный компонент)	+15 млн. руб.
			Более консервативное отражение обязательств
Буферный резерв	0 (не формируется)	20 млн. руб. (размер на основе 95-го перцентиля второго сценария)	+20 млн. руб.
			Прямое покрытие потенциального системного шока
Требуемый капитал (SCR) под киберриск	25 млн. руб.	35 млн. руб. (с учётом стресс-теста)	+10 млн. руб.
			Капитал лучше соотносится с истинным профилем риска
Общий финансовый буфер против кибершока	25 млн. руб. (только SCR)	50 млн. руб. (SCR + буферный резерв)	Удвоение емкости для поглощения экстремальных убытков

Источник: разработано авторами.

Развитие киберстрахования сопровождается расширением набора инструментов передачи и управления риском. Их значение особенно возрастает применительно к систематическим и системным событиям, которые трудно полностью диверсифицировать внутри страхового портфеля.

Перестрахование остаётся базовым механизмом ограничения крупных и агрегированных убытков. Однако его способность поглощать экстремальный киберриск зависит от готовности перестраховщиков принимать риски, характеризующиеся высокой неопределённостью и корреляцией [17, 21, 22].

Параметрические элементы покрытия потенциально позволяют ускорить выплату при наступлении заранее определённого и объективно фиксируемого события, например при недоступности конкретного цифрового сервиса в течение установленного периода. Их преимуществом является упрощение урегулирования, а ограничением - базисный риск, то есть возможное несовпадение параметрического триггера с фактическими финансовыми потерями страхователя.

ILS и облигации киберкатастрофы создают возможность передачи части экстремального риска инвесторам рынка капитала. The Geneva Association отмечает рост интереса к подобным инструментам, однако их дальнейшее развитие требует большей стандартизации условий страхового покрытия, устойчивых моделей накопления и прозрачных условий срабатывания триггеров [18].

Андеррайтинг, основанный на данных, представляет собой ещё одно направление финансово-технологических инноваций. Интеграция данных об уязвимостях, технической телеметрии и актуальной информации об угрозах позволяет постепенно переходить от статического андеррайтинга, основанного на анкетах страхователя, к более динамической оценке риска [24].

При обсуждении европейской системы платежеспособности необходимо различать Solvency Capital Requirement (SCR) и коэффициент платежеспособности. SCR представляет собой величину требуемого капитала,

тогда как показатель платежеспособности отражает соотношение допустимых собственных средств и соответствующего капитального требования.

Поэтому результат стресс-теста корректно выражать, например, через:

- изменение чистого убытка;
- изменение собственных средств;
- возможное изменение внутренней оценки требуемого капитала;
- изменение коэффициента платежеспособности;
- изменение концентрации и перестраховочного покрытия.

Современные актуарные исследования подчёркивают, что при включении киберриска в капитальную модель особенно важно корректно отражать зависимости между страхователями, параметры экстремальных событий и взаимосвязь модели с общей системой управления рисками [16].

Таким образом, использование результатов комплексного стресс-тестирования в процессах резервирования и управления капиталом позволяет решать одну из ключевых задач страхования киберрисков - обеспечивать платежеспособность и выполнение обязательств перед страхователями в условиях высокой неопределённости.

Выводы. Проведённое исследование подтверждает, что страхование киберрисков формируется как самостоятельное и методологически сложное направление страховой деятельности. Специфика киберриска определяется его быстро меняющимся характером, ограниченностью сопоставимой статистики убытков, технологической взаимозависимостью страхователей и возможностью возникновения значительных накопленных потерь вследствие одного общего события.

Современные актуарные исследования показывают, что классические методы страхового моделирования сохраняют ценность применительно к части киберрисков, однако требуют дополнения моделями зависимости, сценарным анализом и инструментами оценки накопления [14-16, 19]. Поэтому противопоставление «традиционных» и «новых» методов представляется менее

продуктивным, чем их последовательная интеграция.

Устойчивость портфеля киберстрахования зависит не только от адекватности индивидуальной страховой премии, но и от способности страховщика выявлять общие технологические зависимости между объектами страхования. Именно накопление нескольких требований вследствие одной уязвимости или зависимости от общего поставщика способно превращать относительно управляемый индивидуальный риск в существенную нагрузку на страховой портфель.

Основным элементом предлагаемой методики является сценарная модель стресс-тестирования, объединяющая выявление технологической концентрации, формирование правдоподобного сценария, оценку возможных финансовых последствий и выбор управленческих мер. Основными областями применения результатов являются андеррайтинговые лимиты, тарификация, перестрахование, риск-аппетит и внутреннее управление капиталом.

При этом результаты стресс-тестирования не должны приводить к созданию произвольных технических резервов или признанию дополнительных резервов собственным капиталом. Технические обязательства, перестрахование и капитал представляют различные уровни финансовой защиты и должны оцениваться в соответствии с их экономическим и нормативным назначением.

Перспективным направлением развития рынка являются финансовые инновации, позволяющие увеличивать доступную ёмкость страхования. Наряду с традиционным перестрахованием к ним относятся параметрические элементы покрытия, *insurance-linked securities* и киберкатастрофические облигации [17, 18, 23]. Их дальнейшее распространение будет зависеть от качества моделей накопления, стандартизации условий покрытия и доверия инвесторов к механизму триггера.

Развитие искусственного интеллекта и андеррайтинга, основанного на данных, создаёт дополнительные возможности для более динамичной оценки киберрисков посредством использования технической телеметрии и внешних

данных об угрозах [24]. Вместе с тем применение таких моделей связано с рисками, обусловленными качеством данных, ограниченной интерпретируемостью и недостаточной устойчивостью моделей, что требует сохранения экспертного контроля.

Практическое значение предложенного подхода заключается в возможности его использования страховыми организациями при формировании внутренних стресс-сценариев и лимитов киберэкспозиций. Перспективным направлением дальнейших исследований является эмпирическая апробация модели на реальном портфеле с описанием методики учёта зависимостей, построения распределений убытков и оценки эффекта перестрахования.

Список литературы

1. Кулешова Д. И. Развитие инноваций страхового бизнеса в условиях цифровой экономики // Дискуссия. – 2025. – №. 3 (136). – С. 180-189.
2. Хабаров В. И., Колбина М. С., Кушелев И. Ю. Внедрение цифровых инноваций как фактор развития и модернизации страхового рынка // Экономика и управление. – 2023. – Т. 29. – №. 1. – С. 33-44.
3. Кравченко Е. В., Суховеева А. А. Технологические тренды развития страховой отрасли // Финансовая экономика. – 2021. – №. 6. – С. 201-204.
4. Аванесов А. А. Проблемы страхования киберрисков // Экономическое развитие России. – 2025. – Т. 32. – №. 6. – С. 260-263.
5. Сипратов Р. О. Страхование киберрисков в условиях функционирования банковских экосистем // Финансовая экономика. – 2022. – Т. 8. – С. 134-139.
6. Жмурова С. С., Джафаров Д. И. Правовое регулирование страхования киберрисков в России: опыт зарубежных стран и перспективы развития // Право и государство: теория и практика. – 2025. – №. 4. – С. 334-337.
7. Воеводин В. А. Об оценивании устойчивости функционирования объектов микропараметрического страхования киберрисков // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51. – №. 4. – С. 40-49.

8. Саченко Л. А., Деревянкин А. А., Берберова М. А., Деревянкин Г. А. Страхование кибер-рисков АЭС–вопросы согласования условий и подходов к оценке рисков // Информационное общество. – 2024. – №. 2. – С. 112-122.
9. Левин Ю. А., Сапелин В. В. Страхование киберрисков: вопросы формирования безопасной информационной инфраструктуры бизнеса // Финансовый бизнес. – 2022. – №. 9. – С. 231.
10. Клишина Ю. Е., Углицких О. Н., Серафимова В. А. Страхование юридических лиц от киберрисков: проблемы и перспективы развития // Финансы и учетная политика. – 2023. – №. 2 (30). – С. 11-14.
11. Аванесов А. А. Роль страхования информационных рисков // Экономика, предпринимательство и право. – 2023. – Т. 13. – №. 11. – С. 4879-4890.
12. Мурадова А. О., Худайбердиева Н. А., Хаклиев Р. Г. Страхование кибербезопасности: вызовы и перспективы в современной экономике // Вестник науки. – 2024. – Т. 3. – №. 3 (72). – С. 97-100.
13. Мадатова О. В. Управление финансовыми рисками, связанными с интеллектуальной собственностью, в условиях цифровой трансформации и глобальной конкуренции // Финансы и управление. – 2025. – № 3. – С. 139–167. DOI: 10.25136/2409-7802.2025.3.75786.
14. Awiszus K., Knispel T., Penner I. et al. Modeling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks // European Actuarial Journal. – 2023. – Vol. 13. – P. 1–53. DOI: 10.1007/s13385-023-00341-9.
15. Zeller G., Scherer M. Is accumulation risk in cyber methodically underestimated? // European Actuarial Journal. – 2024. – Vol. 14. – P. 711–748. DOI: 10.1007/s13385-024-00381-9.
16. Grewal J., Cartagena S. Cyber risk within capital models // British Actuarial Journal. – 2024. – Vol. 29. – Article e16. DOI: 10.1017/S1357321724000114.
17. The Geneva Association. Cyber Risk Accumulation: Fully Tackling the Insurability Challenge. – Zurich: The Geneva Association, 2023.
18. The Geneva Association. Catalysing Cyber Risk Transfer to Capital Markets:

- Catastrophe Bonds and Beyond. – Zurich: The Geneva Association, 2024.
19. Bardopoulos J. Cyber-insurance pricing models // British Actuarial Journal. – 2025. – Vol. 30. – Article e6. DOI: 10.1017/S1357321724000205.
20. European Insurance and Occupational Pensions Authority. Financial Stability Report, December 2025. – Frankfurt am Main: EIOPA, 2025.
21. International Association of Insurance Supervisors. Global Insurance Market Report 2025. – Basel: IAIS, 2025. – 77 p.
22. Currat A., Perry J., Yong J. Cyber Insurance Unpacked: The Corporate Digital Safety Net // FSI Insights. – 2026. – No. 75. – Basel: Bank for International Settlements, 2026. – 44 p.
23. Pain D., Romanosky S. Strengthening Cyber Resilience Through Insurance. – Zurich: The Geneva Association, 2026.
24. Paragioudakis A., Komninos N., Smyrlis M. et al. Risk management for cyber insurance: a survey for data-driven approaches with the use of AI // International Journal of Information Security. – 2026. – Vol. 25. – Article 112. DOI: 10.1007/s10207-026-01275-5.

References

1. Kuleshova D. I. Razvitie innovatsii strakhovogo biznesa v usloviyakh tsifrovoi ekonomiki // Diskussiya. – 2025. – №. 3 (136). – S. 180-189.
2. Khabarov V. I., Kolbina M. S., Kushelev I. Yu. Vnedrenie tsifrovyykh innovatsii kak faktor razvitiya i modernizatsii strakhovogo rynka // Ekonomika i upravlenie. – 2023. – T. 29. – №. 1. – S. 33-44.
3. Kravchenko E. V., Sukhovееva A. A. Tekhnologicheskie trendy razvitiya strakhovoi otrasli // Finansovaya ekonomika. – 2021. – №. 6. – S. 201-204.
4. Avanesov A. A. Problemy strakhovaniya kiberriskov // Ekonomicheskoe razvitie Rossii. – 2025. – T. 32. – №. 6. – S. 260-263.
5. Sipratov R. O. Strakhovanie kiberriskov v usloviyakh funktsionirovaniya bankovskikh ekosistem // Finansovaya ekonomika. – 2022. – T. 8. – S. 134-139.
6. Zhmurova S. S., Dzhaфарov D. I. Pravovoe regulirovanie strakhovaniya kiberriskov

v Rossii: opyt zarubezhnykh stran i perspektivy razvitiya // *Pravo i gosudarstvo: teoriya i praktika*. – 2025. – №. 4. – S. 334-337.

7. Voevodin V. A. Ob otsenivanii ustoichivosti funktsionirovaniya ob"ektov mikroparametricheskogo strakhovaniya kiberriskov // *Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki*. – 2024. – T. 51. – №. 4. – S. 40-49.

8. Sachenko L. A., Derevyankin A. A., Berberova M. A., Derevyankin G. A. Strakhovanie kiber-riskov AES–voprosy soglasovaniya uslovii i podkhodov k otsenke riskov // *Informatsionnoe obshchestvo*. – 2024. – №. 2. – S. 112-122.

9. Levin Yu. A., Sapelin V. V. Strakhovanie kiberriskov: voprosy formirovaniya bezopasnoi informatsionnoi infrastruktury biznesa // *Finansovyi biznes*. – 2022. – №. 9. – S. 231.

10. Klishina Yu. E., Uglitskikh O. N., Serafimova V. A. Strakhovanie yuridicheskikh lits ot kiberriskov: problemy i perspektivy razvitiya // *Finansy i uchelnaya politika*. – 2023. – №. 2 (30). – S. 11-14.

11. Avanesov A. A. Rol' strakhovaniya informatsionnykh riskov // *Ekonomika, predprinimatel'stvo i pravo*. – 2023. – T. 13. – №. 11. – S. 4879-4890.

12. Muradova A. O., Khudaiberdieva N. A., Khakliev R. G. Strakhovanie kiberbezopasnosti: vyzovy i perspektivy v sovremennoi ekonomike // *Vestnik nauki*. – 2024. – T. 3. – №. 3 (72). – S. 97-100.

13. Madatova O. V. Upravlenie finansovymi riskami, svyazannymi s intellektual'noi sobstvennost'yu, v usloviyakh tsifrovoi transformatsii i global'noi konkurentsii // *Finansy i upravlenie*. – 2025. – №. 3. – S. 139–167. DOI: 10.25136/2409-7802.2025.3.75786.

14. Awiszus K., Knispel T., Penner I. et al. Modeling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks // *European Actuarial Journal*. – 2023. – Vol. 13. – P. 1–53. DOI: 10.1007/s13385-023-00341-9.

15. Zeller G., Scherer M. Is accumulation risk in cyber methodically underestimated? // *European Actuarial Journal*. – 2024. – Vol. 14. – P. 711–748. DOI: 10.1007/s13385-

024-00381-9.

16. Grewal J., Cartagena S. Cyber risk within capital models // *British Actuarial Journal*. – 2024. – Vol. 29. – Article e16. DOI: 10.1017/S1357321724000114.
17. The Geneva Association. Cyber Risk Accumulation: Fully Tackling the Insurability Challenge. – Zurich: The Geneva Association, 2023.
18. The Geneva Association. Catalysing Cyber Risk Transfer to Capital Markets: Catastrophe Bonds and Beyond. – Zurich: The Geneva Association, 2024.
19. Bardopoulos J. Cyber-insurance pricing models // *British Actuarial Journal*. – 2025. – Vol. 30. – Article e6. DOI: 10.1017/S1357321724000205.
20. European Insurance and Occupational Pensions Authority. Financial Stability Report, December 2025. – Frankfurt am Main: EIOPA, 2025.
21. International Association of Insurance Supervisors. Global Insurance Market Report 2025. – Basel: IAIS, 2025. – 77 p.
22. Currat A., Perry J., Yong J. Cyber Insurance Unpacked: The Corporate Digital Safety Net // *FSI Insights*. – 2026. – No. 75. – Basel: Bank for International Settlements, 2026. – 44 p.
23. Pain D., Romanosky S. Strengthening Cyber Resilience Through Insurance. – Zurich: The Geneva Association, 2026.
24. Paragioudakis A., Komninos N., Smyrlis M. et al. Risk management for cyber insurance: a survey for data-driven approaches with the use of AI // *International Journal of Information Security*. – 2026. – Vol. 25. – Article 112. DOI: 10.1007/s10207-026-01275-5.

Статья поступила в редакцию 09.01.2026; одобрена после рецензирования 27.02.2026; принята к публикации 30.03.2026.

The article was submitted 09.01.2026; approved after reviewing 27.02.2026; accepted for publication 30.03.2026.