5.2.4 Финансы (экономические науки)

Научная статья
УДК 336

ФИНАНСОВЫЕ ИННОВАЦИИ В СТРАХОВАНИИ КИБЕРРИСКОВ: ПРОБЛЕМЫ ОЦЕНКИ И КАПИТАЛИЗАЦИИ

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

Аннотация

Статья посвящена формированию методики стресс-тестирования страховых портфелей, подверженных киберрискам. В условиях стремительной цифровизации экономических процессов и сравнительно высокой зависимости общественного производства и государственного управления от информационно-коммуникационных технологий киберриски трансформировались из технической проблемы IT-отделов в комплексную угрозу финансовой стабильности хозяйствующих субъектов. Киберриски, проявляющиеся в виде целенаправленных атак, сбоев программного обеспечения или человеческих ошибок, приводят не только к прямым финансовым потерям, но и к существенным репутационным издержкам, судебным расходам и перерывам в бизнес-деятельности. Данная трансформация обусловила формирование спроса на адекватные страховые продукты, способные обеспечить перераспределение финансовых последствий киберинцидентов. Исследование финансовых инноваций в страховании киберрисков сфокусировано на разрешении противоречия между растущей потребностью рынка в защите от цифровых угроз и дефицитом надежных методов их квантификации. Изложение статьи будет посвящено последовательному анализу указанных проблем, обзору формирующихся рыночных решений и разработке практических предложений по

совершенствованию методологии оценки, стресс-тестирования и капитализации данного актуального класса рисков. Развитие страхования киберрисков находится на пересечении актуарной науки, риск-менеджмента и финансового инжиниринга. Его дальнейшая эволюция будет определяться способностью страхового сообщества разрабатывать и внедрять комплексные методологии оценки, соответствующие динамичной природе цифровых угроз, а также готовностью государственного сектора адаптировать пруденциальные требования к новой рискогенной реальности.

Ключевые слова: финансовые инновации; страхование киберрисков; финансовые последствия; проблемы оценки и капитализации; методика стресс-тестирования.

Original article

FINANCIAL INNOVATIONS IN CYBER RISK INSURANCE: PROBLEMS OF VALUATION AND CAPITALIZATION

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

Abstract

This article explores the development of a methodology for stress testing insurance portfolios exposed to cyber risks. With the rapid digitalization of economic processes and the relatively high dependence of public production and public administration on information and communications technology, cyber risks have transformed from a technical problem for IT departments into a complex threat to the financial stability of economic entities. Cyber risks, manifested in the form of targeted attacks, software failures, or human error, lead not only to direct financial losses but also to significant reputational costs, legal expenses, and business interruptions. This transformation has generated demand for adequate insurance products capable of

redistributing the financial consequences of cyber incidents. This study of financial innovations in cyber risk insurance focuses on resolving the contradiction between the growing market demand for protection against digital threats and the lack of reliable methods for quantifying them. This article will focus on a consistent analysis of these issues, a review of emerging market solutions, and the development of practical proposals for improving the assessment, stress testing, and capitalization methodologies for this relevant class of risks. The development of cyber risk insurance lies at the intersection of actuarial science, risk management, and financial engineering. Its future evolution will be determined by the insurance community's ability to develop and implement comprehensive assessment methodologies that align with the dynamic nature of digital threats, as well as the public sector's willingness to adapt prudential requirements to the new risk-generating reality.

Keywords: financial innovation; cyber risk insurance; financial consequences; valuation and capitalization issues; stress testing methodology.

Введение. Развитие страхования киберрисков сталкивается с комплексом методологических и практических проблем, обусловленных сущностью самого риска и ограничениями действующего на данный момент страхового механизма [1], [2].

Специфика киберрисков как объекта страхования заключается в их динамичной эволюции, определяющейся технологическими изменениями и адаптацией злоумышленников, в высокой коррелированности убытков ввиду общих уязвимостей, а также в существенной непрозрачности данных, необходимых для классической концепции актуарных расчётов. Эти факторы придают киберрискам выраженное значение, создавая потенциал для каскадных эффектов и кумулятивных убытков, способных влиять на платежеспособность страховых организаций [3]. Соответственно, ключевой проблемой становится разработка методологических основ для корректной оценки и капитализации данных рисков в рамках страховых портфелей.

Существующие актуарные модели, основанные на анализе ретроспективных статистических данных для оценки частоты и тяжести убытков, отражают ограниченность применительно к киберрискам. Исторические данные являются недостаточными, нерепрезентативными, а сущность риска не соответствует предпосылкам многих вероятностных моделей, таким как независимость и стационарность событий. Это создает значительные трудности в достоверном расчете страховой премии и формировании технических резервов, что, в свою очередь, способствует неоптимальному ценообразованию, недострахованию или отказу от принятия риска [4].

Ответом на данные вызовы становится активное развитие финансовых инноваций, включающих как новые страховые продукты с адаптивными условиями и лимитами ответственности, так и альтернативные механизмы трансфера риска. К последним относятся специализированные решения по хеджированию, секьюритизация киберрисков через облигации и создание синтетических финансовых инструментов. Эффективность данных механизмов зависит от качества лежащих в их основе моделей оценки, что актуализирует задачу разработки концепции стресс-тестирования страховых портфелей, подверженных киберрискам. Методология должна выходить за рамки исторических сценариев и включать в себя комплексные сценарии, моделирующие кибератаки на инфраструктуру или массовые эксплуатации уязвимостей, с учетом корреляций с другими категориями риска в балансе страховщика.

Наконец, неразрывно связанной с вопросами оценки является проблема формирования достаточных страховых резервов и регулирования требований к платежеспособности (эквиваленты). Текущие нормативные подходы могут не в полной мере отражать специфику киберрисков, что создает необходимость в научно обоснованных совершенствованиях [5]. Формирование резервов по страхованию киберрисков должно учитывать потенциально катастрофические убытки, а также операционные риски, связанные со сложностью оценки и

урегулирования убытков.

Обзор источников литературы. Киберриски характеризуются неопределенностью параметров распределения убытков. Их частота и тяжесть нестатичны во времени, будучи обусловленными антропогенными факторами: быстро меняющимися тактиками злоумышленников, скоростью внедрения новых технологий и эффективностью мер. Это нарушает ключевое условие классического страхования – наличие устойчивых закономерностей [6].

Одна уязвимость в широко используемом программном обеспечении или атака на крупного провайдера облачных услуг может одновременно затронуть значительное число организаций в разных отраслях и государствах, вызывая кумулятивные убытки, угрожающие платежеспособности страховщика [7]. Данное свойство приближает киберриски к катастрофическим, но с более высокой частотой триггерных событий.

Существует асимметрия информации и проблема морального риска. Страхователь лучше осведомлен о состоянии своих киберзащитных систем, а наличие страхового покрытия может снижать его стимулы к инвестициям в безопасность. Кроме того, масштаб убытка часто зависит от действий страхователя уже после инцидента (качество цифровой криминалистики, публичное раскрытие информации) [8].

Трансграничный характер киберинцидентов и отсутствие унифицированного законодательства осложняют урегулирование убытков, создавая юридическую неопределенность в вопросах применимости права и объемов компенсации.

Значение киберрисков обусловливается их способностью провоцировать каскадные эффекты в глубоко интегрированной цифровой экономике. Убыток для одного предприятия может вызвать операционные сбои по всей цепочке создания стоимости, привести к масштабным утечкам персональных данных с последующими регуляторными штрафами и коллективными судебными исками, сократить степень доверия к финансовым институтам или системам критической

инфраструктуры. Таким образом, киберриски трансформируются из операционных рисков компаний в фактор финансовой стабильности, что требует грамотного отражения в риск-менеджменте страховых организаций и нормативно-правовом регулировании.

Традиционные актуарные методы, основанные на анализе исторических данных по частоте и тяжести инцидентов для построения распределений убытков (например, с использованием пуассоновского распределения для частоты и логнормального – для тяжести), обладают определенными ограничениями.

Рынок страхования киберрисков относительно молодой сегмент, а информация об убытках фрагментирована, зачастую конфиденциальна и плохо структурирована. Доступные временные ряды слишком короткие для надежных статистических выводов. Кроме того, быстрое технологическое развитие делает исторические данные малорелевантными для оценки будущих угроз [9].

Как отмечено выше, киберинциденты - одинаково распределенные события, что нарушает базовые предпосылки многих актуарных моделей. Корреляция убытков делает опасным использование закона больших чисел в его классической форме [10].

Значительная часть риска определяется качеством кибергигиены, человеческим фактором и эффективностью мер безопасности, что слабо поддается квантификации в рамках актуарного подхода [11], [12].

Вследствие этих ограничений для оценки киберрисков необходим синтетический подход, комбинирующий:

1) Сценарный анализ и стресс-тестирование, основанные на экспертных суждениях о потенциальных векторах атак и уязвимостях.

2) Структурные (детерминистические) модели, симулирующие распространение кибератаки по сетям и оценивающие прямые и косвенные убытки.

3) Использование альтернативных данных, таких как данные тестов на

проникновение, информация об уязвимостях из открытых источников (CVSS), активность в Интернет-сети.

Таким образом, развитие страхования киберрисков движется по пути создания гибридных финансово-технологических решений. Они сочетают элементы традиционного страхования, параметрических продуктов, сервисной модели и альтернативного трансфера риска на рынки капитала. Научная новизна заключается в разработке интегральных моделей оценки, которые согласуют параметры этих новых инструментов с динамической природой самого риска, обеспечивая финансовую устойчивость страхового сектора в условиях цифровых угроз.

Материалы и методы исследования. Основу исследования составили аналитические отчеты международных перестраховочных компаний (Swiss Re Institute, Munich Re), данные регуляторов (Европейское управление пруденциального надзора - EBA, 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 капиталоемкости киберрисков.

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 принципе комбинации 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 ориентирован на определенный канал возникновения кумулятивных убытков. Примеры сценариев приведены в таблице 1.

Таблица 1 - Примеры стресс-сценариев для портфеля страхования киберрисков

Наименование сценария	Целевой вектор	Охват портфеля	Временные параметры
Массовый крипто-графический 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
Целенаправленная информационная	Координи-рованные атаки на	Страхователи в целевых	Эскалация в течение 1

война против критической инфраструктуры	операторов энерго-, водо- и теплоснабжения в одном географическом регионе	отраслях в регионе, а также их контрагенты (эффект второй волны)	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 ($Lmin$), наиболее вероятный ($Lmode$) и максимальный ($Lmax$) 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 отчётную дату).

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

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 расчета используются результаты симуляций Монте-Карло, где в качестве входных данных применяются 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 в размере 95-й перцентили распределения совокупного убытка по наиболее опасному из реалистичных сценариев (первому, второму, третьему) за вычетом покрытия перестрахования.

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.

Таким образом, интеграция результатов продвинутого стресс-тестирования в процессы резервирования и управления капиталом позволяет преодолеть ключевой парадокс страхования киберрисков: необходимость

оперировать в условиях неопределенности, сохраняя при этом платежеспособность и выполняя обязательства перед страхователями. Предлагаемые меры носят превентивный характер и направлены на укрепление устойчивости страхового сектора.

Выводы. Специфика киберрисков как объекта страхования состоит в их динамичности, высокой потенциальной коррелированности убытков, значительной неопределенности параметров распределения и трансграничном характере. Эти свойства придают киберрискам системное значение, трансформируя их из операционного риска отдельных компаний в фактор, способный оказывать влияние на финансовую устойчивость страхового сектора и стабильность смежных отраслей экономики. Данная трансформация формирует объективную потребность в грамотных решениях, способных обеспечить перераспределение финансовых последствий киберинцидентов.

Традиционные актуарные модели, основанные на анализе ретроспективных статистических данных о частоте и тяжести убытков, отражают ограниченность в применении к киберрискам. Недостаточность информации, её нерепрезентативность в условиях быстрых технологических изменений, а также нарушение базовых предпосылок моделей о независимости и стационарности событий делают невозможной достоверную оценку тарифов и резервов исключительно классическими методами. Это обусловливает необходимость разработки синтетических подходов к оценке, интегрирующих сценарный анализ, структурное моделирование и методы из области кибербезопасности.

Ответом на методологические вызовы стало развитие комплекса финансовых инноваций. К ним относятся новые страховые продукты, такие как параметрические полисы и комбинированные покрытия, снижающие асимметрию данных и базисный риск. Для управления катастрофической составляющей и корреляцией убытков формируются специализированные механизмы перестрахования, включая перестраховочные пулы, а также

инструменты секьюритизации, в частности катастрофические облигации с кибертриггерами. Эффективность данных механизмов непосредственно зависит от качества лежащих в их основе моделей оценки.

В качестве методологического ядра для управления портфельным киберриском предложена методика стресс-тестирования, основанная на применении детерминированных сценариев. Ее отличительной чертой является фокус на технологически конкретных и правдоподобных событиях, способных вызвать кумуляцию убытков. Использование экспертных оценок для параметризации сценариев в сочетании с методами стохастического моделирования, учитывающими корреляцию, позволяет количественно оценить потенциальное воздействие форс-мажорных обстоятельств на капитал и платежеспособность страховщика.

Формирование страховых резервов по киберрискам требует пересмотра традиционных методов, исходя из принципа осторожности. Предлагаемый динамический подход предполагает расчет резерва не только по произошедшим, но и по прогнозируемым инцидентам, с включением катастрофической компоненты, размер которой калибруется по результатам стресс-тестирования. Образование подобного буферного резерва повышает способность страховой организации поглощать крупномасштабные неожиданные убытки.

Для повышения устойчивости страхового сектора целесообразно рассмотреть возможность введения отдельного корректирующего коэффициента или математического модуля в расчет норматива платежеспособности (SCR), который бы учитывал результаты стресс-тестирования. Кроме того, признание дополнительных буферных резервов в качестве элементов капитала второго уровня и дифференциация требований к перестраховочному покрытию в зависимости от его способности снижать риск могут создать новые стимулы для формирования страховщиками внутренних финансовых буферов против киберугроз.

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 инфраструкутры 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.

References

1. Kuleshova D. I. Development of innovations in the insurance business in the context of the digital economy // Discussion. - 2025. - No. 3 (136). - P. 180-189.
2. Khabarov V. I., Kolbina M. S., Kushelev I. Yu. Implementation of digital innovations as a factor in the development and modernization of the insurance market // Economy and Management. - 2023. - Vol. 29. - No. 1. - P. 33-44.
3. Kravchenko E. V., Sukhoveeva A. A. Technological trends in the development of the insurance industry // Financial Economics. - 2021. - No. 6. - P. 201-204.
4. Avanesov A. A. Problems of cyber risk insurance // Economic development of Russia. – 2025. – Vol. 32. – No. 6. – P. 260-263.
5. Sipratov R. O. Cyber Risk Insurance in the Context of Functioning Banking Ecosystems // Financial Economics. – 2022. – Vol. 8. – P. 134-139.
6. Zhmurova S. S., Dzhafarov D. I. Legal Regulation of Cyber Risk Insurance in Russia: Experience of Foreign Countries and Development Prospects // Law and State: Theory and Practice. – 2025. – No. 4. – P. 334-337.
7. Voevodin V. A. On Assessing the Stability of Functioning of Objects of Microparametric Cyber Risk Insurance // Bulletin of the Dagestan State Technical University. Technical Sciences. – 2024. – Vol. 51. – No. 4. – P. 40-49.
8. Sachenko L. A., Derevyankin A. A., Berberova M. A., Derevyankin G. A. Insurance of NPP cyber risks – issues of coordinating conditions and approaches to risk assessment // Information society. - 2024. - No. 2. - P. 112-122.
9. Levin Yu. A., Sapelin V. V. Cyber risk insurance: issues of forming a secure information infrastructure of business // Financial business. - 2022. - No. 9. - P. 231.
10. Klishina Yu. E., Uglitskikh O. N., Serafimova V. A. Insurance of legal entities against cyber risks: problems and development prospects // Finance and accounting

policy. - 2023. - No. 2 (30). - P. 11-14.

11. Avanesov A. A. The Role of Information Risk Insurance // Economy, Entrepreneurship and Law. - 2023. - Vol. 13. - No. 11. - P. 4879-4890.

12. Muradova A. O., Khudaiberdieva N. A., Khakliev R. G. Cybersecurity Insurance: Challenges and Prospects in the Modern Economy // Science Bulletin. - 2024. - Vol. 3. - No. 3 (72). - P. 97-100.

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.