УДК 336.77

СТРАХОВАНИЕ РИСКОВ В КРИПТОСФЕРЕ

Гылыджова Ш.М.

преподаватель

Туркменский государственный институт финансов,

Ашхабад, Туркменистан

Байрамгельдиева Т.

студент

Туркменский государственный институт финансов,

Ашхабад, Туркменистан

Аннотация

В статье рассматривается развитие криптострахования как инструмента управления рисками в сфере цифровых активов и блокчейн-технологий. Анализируются ключевые риски криптосферы, включая киберугрозы, регуляторную неопределённость и технологические сбои, а также существующие механизмы страховой защиты от потерь и убытков. Особое внимание уделено особенностям страхования киберрисков в странах СНГ, структуре договоров, тарифам и страховым событиям. Подчеркивается роль криптострахования в повышении доверия участников рынка, обеспечении компенсации потерь и стимулировании институционализации индустрии цифровых финансовых активов. Статья актуальна для специалистов финансового и страхового сектора, исследователей блокчейн-технологий и регуляторов.

Ключевые слова: Криптострахование, цифровые активы, блокчейн, киберриски, финансовые риски, регулирование, институционализация

RISK INSURANCE IN THE CRYPTO SPACE

Gylydzhova Sh.M.
Lecturer
Turkmen State Institute of Finance,
Ashgabat, Turkmenistan
Bayramgeldieva T.
Student
Turkmen State Institute of Finance,
Ashgabat, Turkmenistan

Annotation
The article examines the development of cryptoinsurance as a risk management tool in the digital assets and blockchain sector. It analyzes key risks in the crypto space, including cyber threats, regulatory uncertainty, and technological failures, as well as existing mechanisms for insurance protection against losses and damages. Special attention is given to the specifics of cyber risk insurance in the CIS countries, contract structures, premiums, and insured events. The role of cryptoinsurance in enhancing market participants' trust, ensuring loss compensation, and promoting the institutionalization of digital financial assets is emphasized. The study is relevant for financial and insurance professionals, blockchain researchers, and regulators.
Keywords: Cryptoinsurance, digital assets, blockchain, cyber risks, financial risks, regulation, institutionalization

Введение

В контексте динамичного развития сектора распределенных реестров (DLT) и криптовалют в мировой финансовой системе, проблема управления рисками приобретает критическое значение [1]. Институционализация и последующее масштабирование данной индустрии неразрывно связаны с разработкой эффективных механизмов трансферта риска [2]. В этой связи криптострахование выступает в качестве потенциально важного инструмента,

способствующего повышению доверия инвесторов и привлечению нового капитала за счет компенсации потерь, обусловленных специфическими рисками цифровых активов.

Это обусловлено чрезвычайно высоким уровнем риска, а также тем обстоятельством, что соответствующие вопросы находятся под контролем центральных банков стран СНГ, которые, с высокой вероятностью, не одобрят внедрение страховых программ в столь неопределённой и слабо урегулированной сфере [3, 4]. Ввиду отсутствия полноценной нормативно-правовой базы в данном направлении представляется целесообразным очертить возможные контуры формирования рынка страховых услуг в области криптовалют и связанных с ними финансовых инструментов.

В настоящее время в странах СНГ функционирует система общего страхования киберрисков, охватывающая, в том числе, участников финансового рынка. Так, для финансового сектора уже определены ключевые элементы договорных отношений в области киберстрахования: структура и состав договора, страховой тариф и страховая премия, категории участников страхового рынка, принципы андеррайтинга и инвестирования, а также перечень страховых событий [5, 6]. Кроме того, установлены отличительные особенности страхования киберрисков по сравнению с иными видами страхования и обозначены специфические страховые продукты, учитывающие особенности банкострахования [7]. Вероятно, по мере развития процессов обращения и хранения различных цифровых финансовых активов соответствующие процедуры будут адаптированы и актуализированы применительно к данному сегменту рынка.

Страховая защита от кибератак предусматривает возмещение ущерба, возникшего вследствие перерывов в деятельности организации, а также покрытие расходов, связанных с восстановлением функционирования информационных систем [8]. К числу таких расходов относятся затраты на восстановление и расшифровку данных, включая стоимость необходимого

программного обеспечения, а также расходы, направленные на минимизацию последствий инцидента и проведение расследования причин совершённого киберпреступления [9].

Однако страхование в криптосфере, также обозначаемое как криптострахование или страхование цифровых финансовых активов, представляет собой механизм защиты от потерь и рисков, непосредственно связанных с использованием криптовалют, функционированием блокчейн-технологий и обращением иных цифровых активов. Основная цель данного вида страхования заключается в минимизации финансовых рисков и обеспечении дополнительного уровня безопасности для держателей криптовалют и участников криптовалютных платформ.

Страховые компании, специализирующиеся на криптостраховании, формируют страховые полисы и условия их предоставления с учётом специфики цифровых активов и особенностей функционирования блокчейн-индустрии [10]. В рамках своей деятельности они осуществляют комплексный анализ рисков, оценку уровня защищённости криптовалютных платформ, а также внедряют современные технологические решения, включая механизмы мультиподписи и системы холодного хранения (cold storage), направленные на обеспечение сохранности и безопасности застрахованных активов [11].

В сфере блокчейн-технологий страхование может быть ориентировано на обеспечение защиты процессов и элементов, непосредственно связанных с функционированием самой технологии. К ним относятся смарт-контракты, цифровые идентификаторы, децентрализованные приложения, а также иные инновационные решения, основанные на распределённых реестрах. В то же время страхование в области криптовалют сосредоточено преимущественно на вопросах обеспечения безопасности и управления рисками, возникающими при хранении, передаче и использовании криптовалютных активов.

Основные риски в криптосфере

Криптовалюты и технологии блокчейн представляют собой инновационное направление, открывающее значительные возможности и предлагающее новые подходы к финансовым и технологическим процессам. Вместе с тем данная сфера характеризуется рядом специфических рисков, которые необходимо учитывать при работе с цифровыми активами и блокчейн-решениями [12]. Ниже приведён обзор ключевых рисков, присущих криптосфере [13, 14].

Кибербезопасность

Подобно любой ИТ-инфраструктуре, криптосфера подвержена разнообразным угрозам кибербезопасности, включая целенаправленные атаки, фишинг, мошеннические схемы и кражи цифровых активов. Злоумышленники могут нацеливаться на цифровые кошельки, централизованные криптобиржи или смарт-контракты с целью получения несанкционированного доступа к активам. Недостатки в программном обеспечении и слабые меры защиты могут привести к утрате средств и компрометации конфиденциальной информации пользователей.

Регуляторные риски

Криптовалюты и технологии блокчейн подвержены регуляторным рискам, обусловленным потенциальными изменениями законодательства, политическими решениями и действиями государственных органов регулирования. Трансформации в правовом поле могут оказывать влияние на легальность и способы использования криптовалют, а также на требования к деятельности криптобирж и иных участников криптосферы.

Кроме того, в настоящее время отсутствует единая международная или национальная система регулирования криптосферы, что создаёт значительную правовую неопределённость для её участников. Неопределённость правового статуса цифровых активов и ограниченная защита прав потребителей повышают потенциальные риски, включая возможность мошенничества и проявления неэтичного поведения в рамках криптовалютного рынка [15].

Технические риски

Сбои или ошибки в работе блокчейн-сетей и смарт-контрактов могут приводить к утрате цифровых активов либо нарушению целостности данных. Недостатки в коде, ошибки при разработке программного обеспечения и техническая несовершенность систем создают уязвимости, которые могут быть использованы злоумышленниками для вмешательства в функционирование платформ и компрометации безопасности цифровых активов.

Виды криптострахования

В зависимости от объекта страховой защиты и характера потенциальных рисков в криптосфере выделяются различные типы страхования, направленные на обеспечение безопасности и защиту участников рынка цифровых активов. Каждый из этих видов страхования адаптирован под специфические потребности и угрозы, присущие работе с криптовалютами, блокчейнами и связанными с ними технологиями.

Каждый из видов страхования в криптосфере формируется с учётом специфических рисков и потребностей участников рынка цифровых активов. Их основная цель заключается в снижении финансовых рисков и обеспечении безопасности операций в криптосфере, что способствует укреплению доверия участников и созданию предпосылок для дальнейшего развития данной отрасли.

Страхование хранилища криптовалют

Страхование хранилища криптовалют обеспечивает защиту от утраты или кражи цифровых активов, находящихся в цифровых кошельках или специализированных хранилищах. Данное покрытие может включать риски, связанные с хакерскими атаками, потерей личных ключей или ошибочными операциями. В случае наступления страхового события страховая компания компенсирует финансовые потери, понесённые владельцем активов.

Страхование транзакций криптовалют

Страхование транзакций криптовалют обеспечивает защиту от финансовых потерь, возникающих в результате неправильных или

мошеннических операций. К таким случаям относятся ошибочные переводы, фишинговые атаки и мошенничество при проведении сделок с цифровыми активами. Данный вид страхования позволяет восстановить утраченные средства или компенсировать понесённые убытки, обеспечивая дополнительный уровень безопасности для участников криптосферы.

Страхование криптобирж

Страхование криптобирж направлено на защиту как самих платформ, так и их пользователей от угроз, включая хакерские атаки, кражу средств и недобросовестные действия со стороны операторов бирж. Данный вид страхования охватывает, в частности, защиту средств клиентов, хранящихся на бирже, а также предоставляет возможность возмещения убытков, понесённых пользователями в результате инцидентов, связанных с нарушением безопасности.

Страхование смарт-контрактов

Страхование смарт-контрактов обеспечивает защиту от потенциальных ошибок или уязвимостей в их коде, которые могут привести к утрате средств или некорректному исполнению условий контракта. Данный вид страхования позволяет компенсировать финансовые потери, возникшие вследствие ошибок в смарт-контрактах или их эксплуатации злоумышленниками.

ГОСТ Р 59516–2021

Важным элементом нормативной базы в России является стандарт ГОСТ Р 59516–2021 от 30.11.2021 «Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности». Данный стандарт разработан с учётом положений международного стандарта ISO/IEC 27102:2019 «Information security management – Guidelines for cyberinsurance» («Менеджмент информационной безопасности. Рекомендации по страхованию киберрисков») и устанавливает требования к организации и проведению страхования рисков в области информационной безопасности.

Стандарт предписывает, что с целью смягчения последствий инцидентов информационной безопасности, помимо организационных и технических мер, реализуемых в соответствии с ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 27002, следует внедрять страхование рисков информационной безопасности как один из инструментов комплексного управления киберрисками [16, 17].

Страхование рисков информационной безопасности не должно рассматриваться как замена эффективной системы менеджмента информационной безопасности (СМИБ) и не освобождает от необходимости разрабатывать планы реагирования на инциденты, организовывать обучение персонала и внедрять другие организационные и технические меры по защите информационных активов. Вместо этого страхование рисков ИБ следует рассматривать как важный элемент СМИБ, направленный на противодействие угрозам информационной безопасности и повышение устойчивости бизнеса.

Данный стандарт также опирается на действующие версии международных и национальных стандартов серии ГОСТ Р ИСО/МЭК 27000, включая:

ГОСТ Р ИСО/МЭК 27001 – требования к системам менеджмента информационной безопасности;

ГОСТ Р ИСО/МЭК 27002 – нормы и правила менеджмента информационной безопасности;

ГОСТ Р ИСО/МЭК 27003 – руководство по реализации системы менеджмента информационной безопасности;

ГОСТ Р ИСО/МЭК 27004 – показатели и измерения в менеджменте информационной безопасности;

ГОСТ Р ИСО/МЭК 27005 – управление рисками информационной безопасности.

Вызовы криптострахования

Криптосфера является относительно молодой отраслью, и объём исторических данных о страховых случаях и рисках существенно меньше, чем в

традиционном страховании. Это создает значительные сложности для страховых компаний при оценке рисков, разработке страховых продуктов и определении адекватного уровня страховых премий.

Кроме того, криптовалюты обладают высокой волатильностью и значительной степенью неопределённости, что дополнительно усложняет процесс прогнозирования рисков и оценку потенциальных финансовых потерь для страховых компаний.

Как уже отмечалось, криптосфера отличается высокой подверженностью угрозам кибербезопасности, включая хакерские атаки и утечки данных. В связи с этим эффективное страхование цифровых активов, помимо традиционных мер защиты, требует разработки и внедрения специализированных инструментов для мониторинга и оперативного реагирования, позволяющих противодействовать постоянно растущим киберугрозам.

С учётом уникальных особенностей блокчейн-технологий страхование в этой сфере может требовать специализированной экспертизы и глубокого понимания технических аспектов для корректной оценки рисков и разработки страховых продуктов. Аналогично, страхование криптовалют предполагает знание криптографических принципов, а также методов безопасного хранения и передачи цифровых активов.

Кроме того, сфера криптовалют сталкивается с широким спектром регуляторных и правовых вопросов. Во многих юрисдикциях законодательство и нормативные акты, регулирующие криптовалюты и технологии блокчейн, находятся в стадии разработки. Для страховых компаний соблюдение различных нормативных требований и обеспечение соответствия действующему законодательству представляют собой серьёзную и сложную задачу.

Заключение

Страховые компании в криптосфере выполняют ключевую функцию по обеспечению безопасности и защите участников от финансовых рисков, связанных с криптовалютами и технологиями блокчейн. Их деятельность

способствует развитию и стабилизации отрасли, укрепляет доверие участников и обеспечивает возможность компенсации убытков при наступлении нежелательных событий, создавая тем самым основу для устойчивого функционирования рынка цифровых активов.

Криптострахование в странах СНГ обладает потенциалом стать значимым элементом экосистемы цифровых активов, обеспечивая безопасность, укрепляя доверие участников и способствуя стабильности в данной инновационной сфере. Вместе с тем, для полноценного развития этого направления необходимо преодолеть существующую первичную неопределённость и сформировать соответствующую нормативно-правовую и технологическую базу.

Безусловно, наиболее эффективной защитой остаются надёжные системы безопасности и комплекс превентивных мер, однако наличие страхового полиса в качестве дополнительного инструмента защиты будет целесообразным и оправданным шагом.

Библиографический список

1. Цифровые активы: правовое регулирование и оценка рисков // Киберленинка. — 2021. — URL: https://cyberleninka.ru/article/n/tsifrovye-aktivy-pravovoe-regulirovanie-i-otsenka-riskov (дата обращения: 01.11.2025).

2. Риски цифровых финансовых активов // Вестник Алтайской академии экономики и права. — 2023. — URL: https://vaael.ru/article/view?id=3540 (дата обращения: 01.11.2025).

3. Юридические аспекты криптовалют в СНГ: Полное руководство по регулированию в России, Беларуси и Казахстане // vc.ru. — URL: https://vc.ru/crypto/2249830-yuridicheskie-aspekty-kriptovalyut-v-sng (дата обращения: 01.11.2025).

4. Подобных А. Страхование рисков в криптосфере: защита цифровых активов и обеспечение безопасности // Информационная безопасность. — 2022.

— URL: https://www.itsec.ru/articles/strahovanie-riskov-v-kriptosfere-zashchita-cifrovyh-aktivov-i-obespechenie-bezopasnosti (дата обращения: 01.11.2025).

5. Проблемы при страховании киберрисков // Коммерсантъ. — 2024. 08.11. — URL: https://www.kommersant.ru/doc/7284519 (дата обращения: 01.11.2025).

6. Киберстрахование // TA Dviser. — 2024. — URL: https://www.tadviser.ru/index.php/Статья:Киберстрахование (дата обращения: 01.11.2025).

7. Страхование киберрисков. Как извлечь пользу и выбрать подходящие условия // HighTech+. — 2023. 14.02. — URL: https://hightech.plus/2023/02/14/strahovanie-kiberriskov-kak-izvlech-polzu-i-vibrat-podhodyashie-usloviya (дата обращения: 01.11.2025).

8. «Страхование киберрисков не панацея, но элемент комплексной защиты» / Виткова Л. // РБК+. 27 ноя. 2024. URL: https://spb.plus.rbc.ru/news/6746eed97a8aa9efdb85f79e (дата обращения: 01.11.2025).

9. «Страхование киберрисков: между необходимостью и неопределённостью» // РБК+. 04 дек. 2024. URL: https://spb.plus.rbc.ru/news/675015be7a8aa938f421952d (дата обращения: 01.11.2025).

10. Цифровая ответственность. Как устроено страхование криптовалюты / РБК.Крипто // РБК. – 2023. – 23 марта. – URL: https://www.rbc.ru/crypto/news/641c2d409a79476a94b94651 (дата обращения: 01.11.2025).

11. Криптострахование: виды, когда оно необходимо и как его оформить // vc.ru. – 2024. – URL: https://vc.ru/crypto/2179893-kriptostrahovanie-vidy-neobhodimost-i-oformlenie (дата обращения: 01.11.2025).

12. Асташкина И. Д. Риски инвестирования в криптовалюты на примере падения рынка NFT // Актуальные исследования. 2023. № 43(173).

URL: https://apni.ru/article/7251-riski-investirovaniya-v-kriptovalyuti (дата обращения: 01.11.2025).

13. Проблемы и риски криптовалют // Хабр. 2023. URL: https://habr.com/ru/companies/kaspersky/articles/341552/ (дата обращения: 01.11.2025).

14. Капустина Н. В., Мамедова Д. Р. Минимизация рисков использования криптовалюты в незаконной деятельности // Управление рисками: проблемы и решения (РИСК'Э–2022): материалы науч.-практ. конференции с зарубежным участием, 10–11 ноября 2022 г. — Санкт -Петербу
— Электронная публикация. — DOI:10.18720/SPBPU/2/id22 -335.

15. Криптовалюты: тренды, риски, меры // Банк России (Consultation paper). 2022. № MP Review 15. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 01.11.2025).

16. Волошина К. А. Влияние криптовалюты на развитие российской экономики: угрозы и экономические возможности // Государственное и муниципальное управление. Ученые записки. — 2024. — № 1. — С. 97–103.

17. Михайлов А. А. О легальном закреплении понятия криптовалюты в законодательстве Российской Федерации // Международный журнал гуманитарных и естественных наук. — 2023. — Вып. -8 С. (63-64. — DOI:10.24412/2500 -1000- 2023- 8- 1- 60- 64.

Оригинальность 75%