Страхование рисков в криптосфере: защита цифровых активов и обеспечение безопасности

Александр Подобных, *руководитель Санкт-Петербургского РО АРСИБ, руководитель Комитета по безопасности цифровых активов и противодействию мошенничеству, судебный эксперт*

Страхование в криптосфере должно быть важным инструментом для повышения доверия и привлечения новых участников в индустрию блокчейна и криптовалют. Однако стоит отметить, что во всем мире криптострахование все еще находится в стадии развития и покрытие и условия могут различаться в зависимости от страховой компании и регулирования в конкретной юрисдикции. В российской криптосфере такая практика практически отсутствует. Это связано с очень высоким уровнем риска и тем, что эти вопросы контролирует ЦБ России, который вряд ли пропустит программу страхования в столь неопределенной области, ведь полноценного регулирования в данном направлении еще нет. Попробуем определить контуры возможного рынка страховых услуг в криптосфере.

Пока в России есть общее страхование киберрисков, в том числе и для участников финансового рынка. Например, для финансового сектора сегодня определены договор киберстрахования и его составляющие, страховой тариф и премия страхователя, участники страхового рынка, андеррайтинг и инвестирование, страховые события, отличие страхования киберрисков от иного, страховые продукты рынка, учет особенностей банкострахования. Вероятно, с развитием обращения и хранения различных цифровых финансовых активов процедуры будут спроецированы и актуализированы под этот сегмент.

Страховая защита от кибератак покрывает ущерб от перерывов в деятельности, расходы на восстановление системы, расходы на восстановление и дешифровку данных (включая стоимость необходимого ПО), расходы на минимизацию последствий и расследование причин киберпреступления.

Но страхование в криптосфере, известное также как криптострахование или страхование цифровых активов, представляет собой процесс обеспечения защиты от потерь и рисков, связанных именно с криптовалютами, блокчейнами и другими ЦФА. Его цель – снижение финансовых рисков и обеспечение безопасности для держателей криптовалюты и участников криптовалютных платформ.

Страховые компании, специализирующиеся на криптостраховании, разрабатывают полисы и условия страхования, учитывая особенности цифровых активов и индустрии блокчейна. Они проводят анализ рисков, оценку безопасности платформ и используют технологии, такие как мультиподпись и холодное хранение (Cold Storage), для обеспечения безопасности активов.

В области блокчейна страхование может быть направлено на аспекты, связанные с самой технологией, – смарт-контракты, цифровые идентификаторы, децентрализованные приложения и другие инновационные решения. Страхование в области криптовалют, с другой стороны, фокусируется на безопасности и управлении рисками, связанными с хранением, передачей и использованием криптовалютных активов.

Основные риски в криптосфере

Криптовалюты и технология блокчейн, несомненно, являются технологически инновационным направлением и предоставляют множество потенциальных преимуществ и инноваций. Однако есть и специфичные риски, которые необходимо учитывать при работе именно в криптосфере. Рассмотрим основные риски, связанные с этой областью.

Кибербезопасность

Как и любая ИТ-инфраструктура, криптосфера подвержена угрозам кибербезопасности, таким как целевые атаки, фишинг, мошенничество и кражи. Злоумышленники могут нацелиться на цифровые кошельки, централизованные криптобиржи или смарт-контракты, чтобы получить несанкционированный доступ к цифровым активам. Уязвимости в программном обеспечении и слабые меры безопасности могут стать причиной утраты средств или компрометации конфиденциальных данных.

Регуляторные риски

Криптовалюты и блокчейн подвержены регуляторным рискам, связанным с возможными изменениями законодательства, политическими решениями и государственными регуляторными действиями. Изменения в правовом регулировании могут повлиять на легальность и использование криптовалют, а также на требования к деятельности криптобирж и других участников криптосферы.

К тому же отсутствует единое международное или национальное регулирование криптосферы. Это создает неопределенность и риски для участников, так как их правовой статус может оказаться неопределенным, а защита прав потребителей может быть недостаточной. Отсутствие достаточных регуляторных механизмов может способствовать возникновению мошенничества и неэтичного поведения в криптосфере.

Технические риски

Технические сбои или ошибки в блокчейне или смарт-контрактах могут привести к потере средств или нарушению целостности данных. Несовершенство кода и недостатки в разработке программного обеспечения могут привести к уязвимостям и возможности злоумышленников вмешаться в работу системы.