

Виды криптострахования

В зависимости от объекта, для которого могут реализоваться те или иные риски, в криптосфере выделяют несколько типов страхования, которые предназначены для обеспечения безопасности и защиты участников.

Каждый из этих видов страхования в криптосфере разрабатывается с учетом специфических рисков и потребностей участников. Они направлены на снижение финансовых рисков и обеспечение безопасности в криптосфере, способствуя повышению доверия и стимулированию дальнейшего развития данной области.

1. Страхование хранилища криптовалют предоставляет защиту от утраты или кражи цифровых активов, которые хранятся в цифровых кошельках или хранилищах. Это покрытие может включать кражу средств в результате хакерских атак, утрату личных ключей или ошибочные операции. Страховая компания возмещает финансовые потери, связанные с такими событиями.

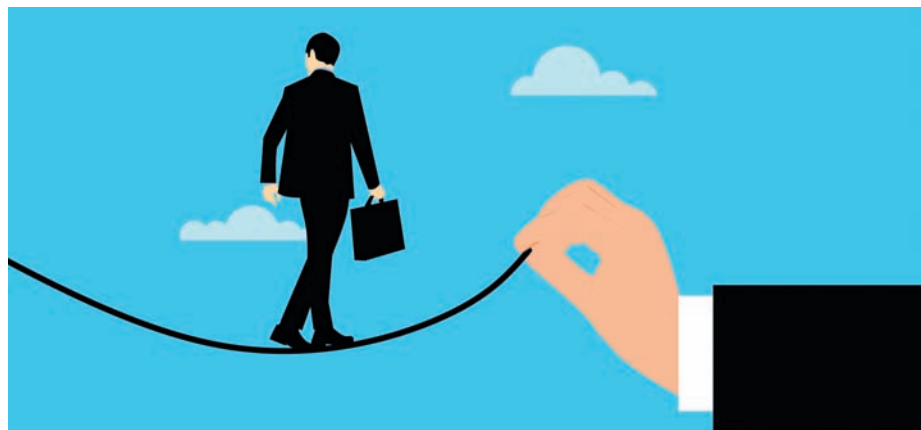
2. Страхование транзакций криптовалют предполагает защиту от потерь, связанных с неправильными или мошенническими транзакциями. В эти случаи включаются ошибочные переводы, фишинговые атаки или мошенничество при совершении сделок с цифровыми активами. Страхование транзакций помогает восстановить средства или компенсировать потери, понесенные в результате таких событий.

3. Страхование криптобирж предназначено для обеспечения защиты пользователей и криптобирж от таких угроз, как хакерские атаки, кражи средств, а также и от недобросовестного поведения со стороны самих бирж. К этому типу относится и защита средств клиентов, хранящихся на бирже, возможность компенсации потерь, понесенных пользователями в результате инцидентов, связанных с безопасностью.

3. Страхование смарт-контрактов предлагает защиту от возможных ошибок или уязвимостей в смарт-контрактах, которые могут привести к потере средств или неправильному исполнению условий контракта. Страхование смарт-контрактов может предоставить возможность компенсации потерь, возникших в результате ошибочных смарт-контрактов или взломов.

ГОСТ Р 59516–2021

Нельзя не упомянуть о действующем в России стандарте от 30.11.2021 г. ГОСТ Р 59516–2021¹ "Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности". Он был разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 27102:2019



"Менеджмент информационной безопасности. Рекомендации по страхованию киберрисков" (ISO/IEC 27102:2019 Information security management – Guidelines for cyberinsurance).

Стандарт предписывает в целях ослабления последствий, возникающих в результате инцидентов ИБ, в дополнение к принятым в соответствии с ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 27002 организационным и техническим мерам обеспечения ИБ, внедрять страхование рисков ИБ как один из инструментов управления киберрисками.

Страхование рисков ИБ не рассматривается как альтернатива эффективной системе менеджмента информационной безопасности (СМИБ) и не может исключить необходимость разработки планов реагирования на инциденты ИБ, создания системы обучения персонала и принятия других организационных и технических мер по защите информационных активов. Страхование рисков ИБ следует рассматривать как важный компонент СМИБ для противодействия угрозам ИБ и повышения устойчивости бизнеса.

Данный стандарт ссылается и на действующие версии ГОСТ Р ИСО/МЭК 27001 (требования к системам менеджмента ИБ), 27002 (нормы и правила менеджмента ИБ), 27003 (реализация системы менеджмента ИБ), 27004 (измерения при менеджменте ИБ), 27005 (менеджмент риска ИБ).

Вызовы криптострахования

Криптосфера относительно молода, и исторических данных о страховых случаях и рисках накоплено существенно меньше, чем в традиционном страховании. Конечно же, это создает дополнительные сложности для страховых компаний в оценке рисков и определении страховых премий.

К тому же криптовалюты характеризуются высокой волатильностью и неопределенностью, что, в свою очередь, еще больше усложняет прогнозирование рисков и оценку потенциальных убытков.

Как уже отмечалось, криптосфера весьма подвержена угрозам кибербезо-

пасности, включая хакерские атаки и последующие утечки данных. Поэтому успешное страхование криптосферы в дополнение к классическим методам защиты потребует разработки и внедрения специфических инструментов для мониторинга и реагирования, чтобы справиться с растущими киберугрозами.

В связи с уникальными особенностями блокчейн-технологии, страхование в области блокчейна может требовать дополнительной экспертизы и понимания технических аспектов для эффективной оценки рисков и разработки страховых продуктов. Страхование в области криптовалют также требует понимания криптографических принципов и методов хранения и передачи криптовалют.

И конечно же, сфера криптовалют сталкивается с разнообразными регуляторными и правовыми вопросами. Некоторые юрисдикции еще разрабатывают законы и политику, регулирующие криптовалюты и блокчейн. Необходимость соблюдения различных нормативных требований и соответствие законодательству может быть сложной задачей для страховых компаний.

Заключение

Роль страховых компаний в криптосфере состоит в обеспечении безопасности и защите участников от финансовых рисков, связанных с криптовалютами и блокчейном. Они играют важную роль в развитии и стабилизации данной отрасли, создавая доверие и обеспечивая компенсацию при возникновении нежелательных событий.

Криптострахование в России имеет потенциал для того, чтобы стать важным элементом криптосферы, обеспечивая безопасность, доверие и стабильность в этой инновационной области. Однако для его полного развития необходимо преодолеть первичную неопределенность.

Безусловно, самой действенной страховкой являются надежные системы защиты и сопутствующие превентивные меры, но иметь полис на всякий случай не помешает. ●

Ваше мнение и вопросы
присылайте по адресу
is@groteck.ru

¹ <https://docs.cntd.ru/document/1200179668>