Блокчейн под атакой: $3,4 млрд потерь за 2025 год и что это значит для CISO

Ольга Ринглер
Руководитель проектов консалтинга, Positive Technologies

Ольга Ринглер

Экспертиза:

- Комплексная оценка уровня защищенности ключевых инфраструктур, задействованных в реализации государственных функций:
- Объекты критической информационной инфраструктуры
- Государственные информационные системы
- Облачные экосистемы
- Комплаенс: от разработки до реализации нормативных требований (требования по технической защите информации, экспериментальные правовые режимы)

О чем поговорим

Узбекистан активно строит блокчейн-инфраструктуру — и одновременно становится частью глобального ландшафта угроз

1

Главная угроза в 2026 году

Не смарт-контракты, а люди и ключи

2

Карта векторов атак

Какие атаки наиболее актуальны

3

Как защититься

Меры безопасности без ограничения роста

$3,4 млрд –украдено из блокчейн-систем в 2025-26 годах

BYBIT: $1,5 млрд

- Не через уязвимость кода
- Компрометация стороннего вендора
- Подмена UI подписания

Оценка защищенности подрядчика – уже must have

Grinex: $1 млрд

- Нет технического отчёта
- Наиболее вероятные версии – компрометация внутренней инфраструктуры и человеческий фактор

Не CVE в коде, а процессы, люди и архитектура изоляции

Q1 2026: $482 млн

- Фишинг и компрометация приватных ключей обогнали атаки на смарт-контракты

Вектор атак смещается от кода к людям и инфраструктуре

Инциденты и способы взлома

Grinex: $1 млрд
взлом внутренней инфраструктуры

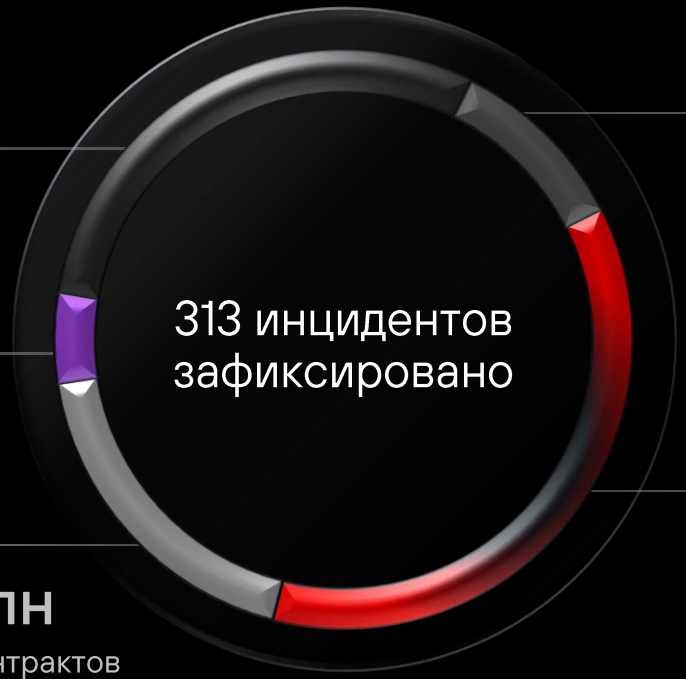
ByBit: $1,5 млрд
атака на цепочку поставок

Cetus: $200 млн
уязвимость кода протокола

YieldBox: $10 млн
уязвимость через манипуляцию ценой актива

CrossCurve: $3 млн
подделка сообщений из-за слабого ACL

Типы атак в 2025 году



$1 млрд
Прочее

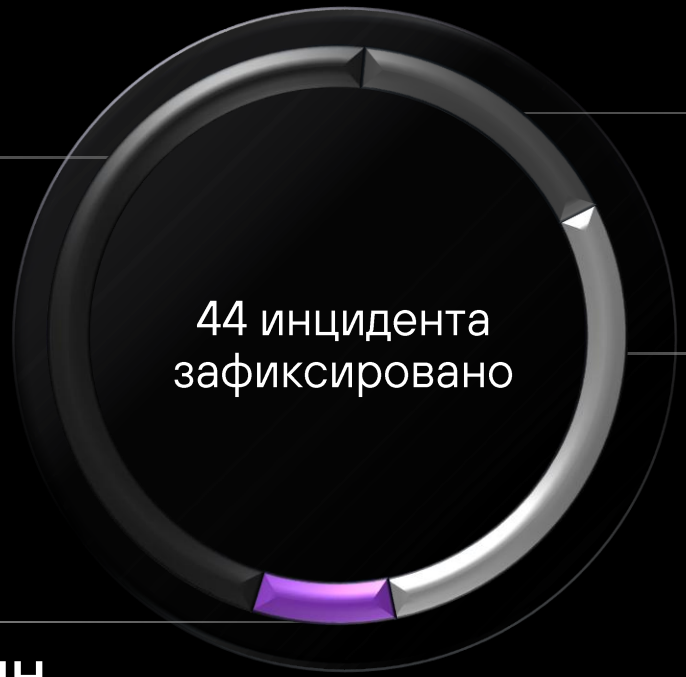
$177 млн
Фишинг и соц.инженерия

$525 млн
Уязвимости контрактов

$180 млн
Утечки ключей

$1,4 млрд
Цепочки поставок/инфраструктура

Типы атак в 2026 году



$326 млн
Уязвимости контрактов

$71,9 млн
Утечки ключей

$306 млн
Фишинг и соц.инженерия

$18,5 млн
Прочее

Ландшафт угроз

2025

- Манипуляция ценами и данными
- Опережение транзакций и извлечение прибыли из порядка исполнения
- Атаки на мосты и межсетевое взаимодействие
- Атаки на кастоди

2026

- Взлом кода приложения и эксплуатация уязвимостей
- Компрометация чувствительной информации
- Компрометация CI / CD библиотек

Zero-click атаки и последствия

Тип риска	Проект	Последствия	Ущерб
Ошибка в обновлении	Compound	Нарушение логики распределения ЦА, пользователи получили избыточные токены	280k COMP ($80 млн.)
Ошибка по внешних данных	Synthetix	Некорректный курс актива – сделки с аномальной прибылью – остановка системы и ручное восстановление	До 1 млрд $ «бумажной» прибыли, прямые выплат $45 тыс.
Перегрузка сети	MakerDAO	Аномальные комиссии и сбой аукционов – ликвидации по нулевой стоимости и как следствие потеря залога и недообеспечение системы	$4,5 млн. необеспеченого DAI, 8 $млн. потерь золота.
Кроссчейн ошибка в коде	Nomad	Ошибка в коде моста – прием системой поддельных сообщений – массовый вывод средств	$186-190 млн.

Что делать CISO

Три приоритета: непрерывный аудит, контроль устранения, культура ИБ на всех уровнях

Смарт-контракты

- Статический и динамический анализ кода
- Фаззинг
- Верификация критичных функций
- Анализ бизнес-логики и экономики протокола
- Проверка proxy-паттернов

Кастоди-решения

Анализ архитектуры управления ключами, операционных процедур подписания и политик авторизаци.

Распределенные реестры

- Тестирование на проникновение сетевого и P2P-слоя
- Анализ устойчивости консесусного механизма
- Проверка настроек конфигурации и изоляции узлов

habrahabr.ru/company/pt

secserv@ptsecurity.com

ptsecurity.com

Спасибо!