НАЦІОНАЛЬНА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ (НАК) · АНАЛІТИЧНИЙ ЦЕНТР

Коли система довіряє зловмиснику

Атака на Binance 29 жовтня 2026 року, компрометація машинних ідентичностей і нова архітектура кіберризиків

Research Report 02/2026 Ідентифікатор: **NCAU-RR-2026-02** 30.10.2026 Дані станом на **10:00 UTC 30.10.2026**

Українська / English

Підготовлено: Аналітичний центр Національної асоціації кібербезпеки на основі аналізу відкритих джерел, публічних повідомлень постраждалих організацій, технічних звітів дослідників і доступних блокчейн-даних. Після публікації технічного звіту Binance НАК оновить висновки і перевірить гіпотези.

Анотація

29 жовтня 2026 року з гаманців криптобіржі Binance було переміщено активи на суму, яку блокчейн-аналітики TRM Labs оцінили в 6,36 млрд доларів. За попередньою версією Binance, інцидент міг бути пов'язаний зі скомпрометованим робочим ноутбуком DevOps-інженера і подальшим доступом до внутрішнього сервісу, що формує заявки на виведення коштів. Компанія заявила, що не виявила доказів витоку приватних ключів.

Ця обставина ставить принципове питання: чи достатньо захищати криптографічні ключі, якщо зловмисник може отримати контроль над системою, яка має законне право ними користуватися? НАК розглядає інцидент у ширшому контексті атак на робочі станції інженерів, привілейовані облікові записи, постачальників і машинні ідентичності, порівнює його з 14 задокументованими випадками і пропонує три власні аналітичні інструменти: матрицю компрометації довіри, карту захисних бар'єрів і методику оцінки ризику однієї робочої станції.

Ключовий висновок: наявність легітимного цифрового підпису не завжди означає, що операцію санкціонував уповноважений власник активів. Безпека сучасної інфраструктури залежить не лише від захисту ключів і пристроїв, а й від незалежної перевірки повноважень, контексту і наслідків критичних дій.

1. Ключові висновки

1. **Масштаб.** Три незалежні аналітичні компанії оцінюють викрадене в 5,9–6,4 млрд доларів: TRM Labs 6,36 млрд [1], Elliptic 6,43 млрд [75], Chainalysis 5,912 млрд [10]. Це майже вчетверо більше за попередній рекорд, злам Bybit на близько 1,5 млрд у 2025 році [25], і більше, ніж було викрадено з криптосервісів за весь 2025 рік (понад 3,4 млрд за Chainalysis) [47]. C
2. **Механізм.** За заявою Binance, доказів витоку приватних ключів немає [2] B. За оцінкою TRM, атакуючий, імовірно, отримав контроль над інфраструктурою підпису гарячих гаманців у десяти мережах [1] C. Якщо це підтвердиться, йдеться про компрометацію рішення про підпис, а не самого ключа.
3. **Точка входу.** За попередньою версією Binance, ланцюжок почався зі скомпрометованого ноутбука DevOps-інженера і службового контейнера, який формує заявки на виведення [2] B. За поточною класифікацією НАК, включно з попередньою оцінкою Binance, у 9 із 15 інцидентів бази початковий доступ отримано через пристрій однієї людини, ще в одному частково (розділ 7). Це характеристика цільової вибірки НАК, а не оцінка поширеності методу серед усіх кібератак.

4. **Заморозка і залишок.** Протягом приблизно чотирьох годин емітенти стейблкоїнів і окремі мережі заморозили в блокчейні від 2,7 млрд (TRM, 00:30 UTC) до 2,84 млрд доларів (Elliptic, 08:00 UTC) [1] [75] A; за заявою Binance, близько 3 млрд [2]. На адресах, які аналітики пов'язують з атакуючим, залишалося від 2,4 млрд (TRM, лише ETH і BTC) до 3,3 млрд (Elliptic, усі незаморожувані активи) [1] [75] C.
5. **Розрив у виявленні.** Перше виведення відбулося о 20:05 UTC, перший публічний сигнал незалежного дослідника з'явився о 20:32 [86], емітенти почали заморожувати кошти о 20:57–21:01 UTC, а офіційна зупинка виведень Binance відбулася близько 22:15 UTC, приблизно через 2 години 10 хвилин після початку атаки [1][4][76]. Станом на 30.10 державної атрибуції немає [12]; блокчейн-аналітики приписують атаку північнокорейській групі TraderTraitor [1][11] C; Elliptic вважає це імовірним, але не певним [75].
6. **Розрив у стримуванні.** За даними Bitquery, делегування EIP-7702, через яке код атакуючого керував найактивнішим гарячим гаманцем Binance в Ethereum, діяло 3 години 50 хвилин і було скасоване о 00:10:35 UTC, більш ніж через 90 хвилин після зупинки виведень [76] A / C. Зупинка сервісу і відкликання вже виданих системою повноважень є різними операціями.

Межі дослідження

Це незалежний аналіз відкритих джерел (OSINT), а не експертиза пристроїв чи систем Binance. НАК не мала доступу до журналів, образів дисків чи внутрішньої інфраструктури компанії і не отримувала її коментарів. Технічний звіт Binance на момент публікації не вийшов. Факти, заяви сторін, оцінки аналітиків і гіпотези в тексті розмежовано за шкалою доказовості (розділ 2).

2. Методологія

2.1. Шкала доказовості НАК

Рівень	Що означає	Приклад у цьому дослідженні
A Спостережуваний факт	Дані, доступні для незалежної перевірки (транзакції в блокчейні, публічний документ)	Переказ 18 270 BTC о 20:20 UTC; заморозка USDT на адресі атакуючого
B Первинне свідчення	Заява організації з безпосереднім доступом до інформації: постраждалої сторони, емітента, органу влади	Попередня заява Binance про ноутбук DevOps-інженера; публікація ФБР
C Аналітична оцінка	Висновок зовнішніх фахівців на основі даних	Атрибуція TraderTraitor від TRM Labs; оцінка 5,912 млрд від Chainalysis
D Гіпотеза	Можливе пояснення без достатнього підтвердження	Конкретний спосіб зараження ноутбука

Рівень A не означає, що відомо, хто контролював адресу і з якою метою зроблено переказ: спостереження і його інтерпретація розділяються. On-chain величини наведено за реконструкцією TRM Labs і Blockaid; їх може перевірити будь-хто за адресами й хешами у відповідних звітах. Якщо заява організації відома лише через ЗМІ або допис у соцмережі, вона позначається B з посиланням на джерело, яке її зафіксувало. Рівень A стосується лише факту транзакції чи заморозки; належність адрес атакуючому і кримінальний характер операцій є аналітичною оцінкою, тому такі твердження позначено A/C.

2.2. Джерела і правила перевірки

Період збору даних: 29.10.2026, 20:00 UTC – 30.10.2026, 10:00 UTC. Використано 86 джерел: заяви компаній-учасниць; незалежну блокчейн-аналітику (TRM Labs, Elliptic, Bitquery, Chainalysis, Blockaid, Arkham, CryptoQuant); офіційні документи (ФБР, CISA, Генеральний інспектор МВС США, SEC, ЄС, CERT-UA); стандарти і специфікації (NIST, ISO, MITRE, C4, Ethereum). Ключова цифра вважається встановленою, якщо її підтверджує первинне джерело або дві незалежні аналітичні фірми. Розбіжності не усереднюються, а показуються окремо (розділ 5.4). Три незалежні блокчейн-реконструкції (TRM Labs, Elliptic, Bitquery) порівнюються в розділі 5.5. Окремої сторінки про інцидент на офіційних сайтах Binance НАК не знайшла; заяви компанії відтворено за ідентичними цитатами в кількох незалежних виданнях [2][19][79]. Сторінки TRM Labs, Elliptic і Bitquery НАК відкрила і звірила з ними ключові цифри 30.10.2026; допис Binance у X недоступний для автоматизованого перегляду. Твердження, які не вдалося підтвердити першоджерелом, до звіту не включено. Час подано в UTC (київський на дві години більший), суми в доларах США за цінами на момент переказу.

2.3. Визначення

- **Машинна ідентичність:** облікові дані сервісів, контейнерів, скриптів і ботів (токени, ключі API, сертифікати), за якими системи довіряють одна одній без участі людини.
- **Інфраструктура підпису:** сукупність систем, що формують, погоджують і підписують транзакції, включно з апаратними модулями зберігання ключів і політиками підпису.
- **Вхід через пристрій однієї людини:** початковий доступ отримано через компрометацію (шкідливе ПЗ, викрадені облікові дані або сесія) пристрою чи особистого акаунта, яким користується конкретна особа. Не належать сюди обман людини без компрометації пристрою, інсайдерські дії, найм підставної особи і вразливості периметра.

3. Хронологія

Кошти почали виводити о 20:05 UTC у мережі XRP Ledger, а не в Ethereum, за якою стежить більшість систем моніторингу. Arkham називає пізніший час, 20:30 UTC [8]; дослідження спирається на детальнішу реконструкцію TRM.

Час (UTC)	Подія	Рівень	Джерело
28.10, 05:55–07:00	Планове обслуговування гаманців Binance у мережі Ethereum з призупиненням депозитів і виведень, оголошене 27.10; зв'язок з атакою не встановлено	B	[83]
28.10, ранок	Адреса, яку TRM пов'язує з оператором атаки, отримує три виведення з міксера Tornado Cash для оплати комісій (Bitquery фіксує поповнення близько 1 ETH о 14:54 29.10)	A / C	[1][76]
29.10, день	За TRM, код тестують на двох гаманцях, репетирують на третьому; приблизно за чотири години до атаки його встановлено на гарячий гаманець Binance	C	[1]
20:05–20:09	П'ять гаманців Binance у XRP Ledger відправляють 233,46 млн XRP	A	[1]
після 20:10	Спорожнюються гаманці в Solana та Optimism	A	[1]
20:20	18 270 BTC одним переказом; транзакція з 50 авторизаціями EIP-7702 в Ethereum (20:20:59); за дві хвилини 612,7 млн USDT і 46,4 млн TRX у Tron	A	[1][5]
20:24:23	Гарячий гаманець Ethereum спорожнено: 167 464 ETH, 1,615 млрд USDT і близько 60 інших токенів	A	[1][5]
20:57	World Liberty Financial заморожує WLFI на головній адресі-отримувачі: перша заморозка	A	[76]
20:32	Незалежний дослідник Spreek публічно повідомляє в X про можливий злам: перший публічний сигнал	B	[86]

Час (UTC)	Подія	Рівень	Джерело
20:41 / 20:59	Через виклики з Binance 14 зі смарт-акаунта Hot Wallet 34, власником якого був Binance 14, виведено 780 млн, а потім ще 43 млн USDC (разом 823 млн)	A	[5][84] [85]
21:01–21:04	Tether заморожує 971,1 млн USDT, Circle заморожує 823 млн USDC	A	[1]
21:15	Чанпен Чжао (CZ): «User funds are safe! It does look like a hack on Binance»	B	[3]
21:16–21:29	Binance двічі редагує першу заяву: прибирає фразу про відсутність впливу на кошти, додає «User funds are completely safe»	B	[3]
21:44	Повторне «дочищення» Binance 14 уже після першої заяви Binance: близько 200 млн USDT і 370 ETH надходять на вже заморожену адресу	A	[84]
22:01–22:10	Ripple заморожує 40,5 млн RLUSD, World Liberty Financial 27,8 млн USD1	A	[1]
близько 22:15	Binance офіційно зупиняє виведення (TechCrunch фіксує підтвердження о 22:27)	B	[4][9]
23:05–23:56	Друга хвиля: гаманці в Avalanche і Polygon; останнє «дочищення» о 23:56	A	[1]
30.10, 00:08	Arbitrum Security Council блокує близько 30 млн (8 426 ETH і 74,6 млн ARB)	A	[1]
00:10:35	Binance скасовує делегування EIP-7702; до цього код атакуючого керував гаманцем 3 год 50 хв і був викликаний сім разів	A / C	[76]
00:36	Співзасновниця Binance I Xe: «Binance will cover all hacking losses»	B	[7]
близько 02:25	Попередня заява Binance: ноутбук DevOps-інженера, службовий контейнер, несанкціоновані виведення; близько 6,3 млрд зачеплено, близько 3 млрд заморожено; доказів витоку ключів немає (інші джерела фіксують 02:21–02:36)	B	[2][5]
04:17	I Xe: виведення планують відновити протягом 48 годин; сервіс виведення і контроль адрес перебудовують	B	[6]
близько 08:37	Binance повідомляє про виявлення «додаткових точок проникнення» понад ноутбук інженера; відновлення виведень очікується приблизно через 45 годин	B	[77][78]
близько 09:00	Виведення досі зупинені, депозити працюють	B	[20]

Від першого анонімного фінансування з Tornado Cash до першого виведення минуло близько півтори доби (розрахунок НАК за даними TRM). Це вказує на сплановану операцію з тестуванням, а не на спонтанне використання випадкового доступу.

4. Технічна реконструкція

4.1. Ланцюжок атаки

Ланка	Що відомо	Рівень	Джерело
Робочий ноутбук DevOps-інженера	Точка входу за попередньою версією Binance; спосіб зараження не розкрито; згодом Binance повідомила про додаткові точки проникнення	B	[2][77]
Службовий контейнер	Внутрішній сервіс, що формує заявки на виведення; через нього надіслано несанкціоновані заявки	B	[2]
Інфраструктура підпису	Окрім Ethereum, гаманці спорожнено ще в дев'яти мережах звичайними коректно підписаними переказами; TRM робить висновок, що інфраструктуру підпису, імовірно, скомпрометовано; Blockaid фіксує одночасний підпис 11 ключами гарячих гаманців; за Elliptic, другий гарячий гаманець в Ethereum напряму підписав атакуючому дев'ять переказів на 174 млн	C	[1][5][75]

Ланка	Що відомо	Рівень	Джерело
Десять мереж	XRP Ledger, Solana, Optimism, Bitcoin, Tron, Ethereum, Arbitrum, Base, Avalanche, Polygon	A	[1]

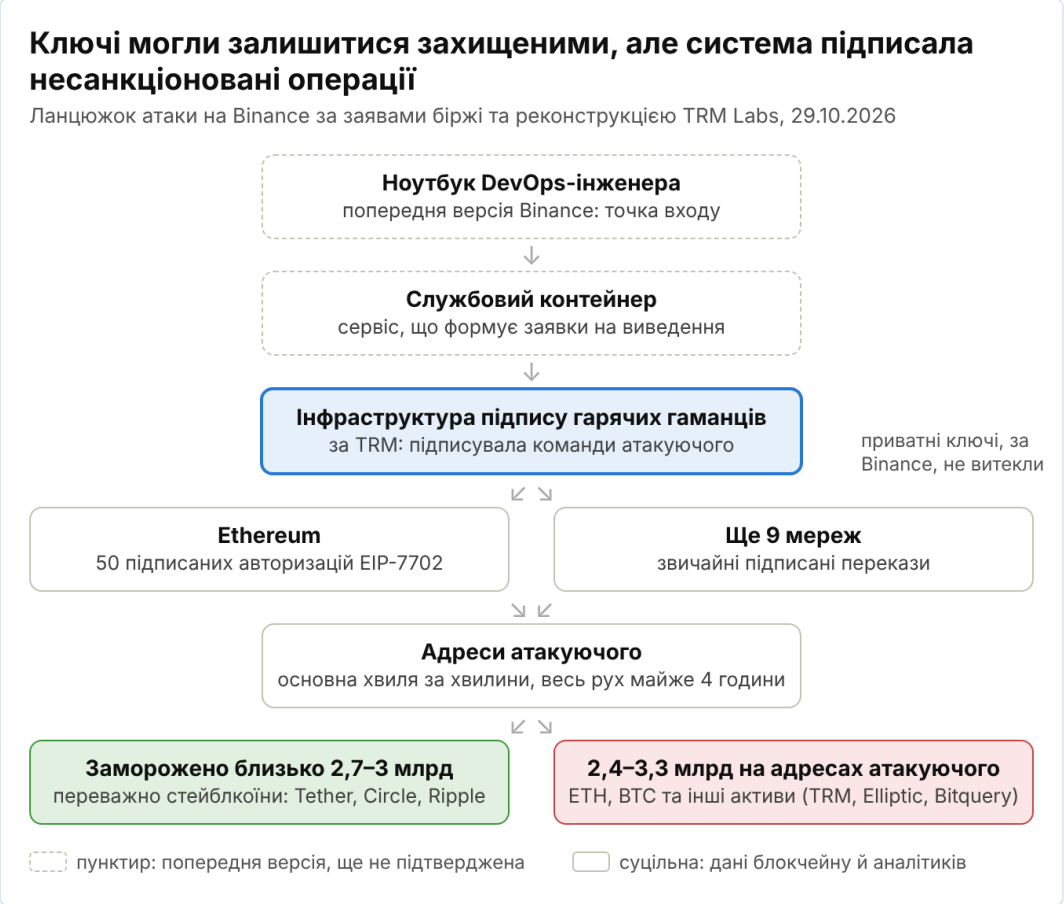


Рисунок 1. Ланцюжок атаки на Binance за заявами біржі та реконструкцією TRM Labs. Пунктир: попередня версія Binance; суцільна лінія: дані блокчейну й аналітиків.

Генеральний директор Binance Річард Тенг заявив, що атака «не була одним кліком» і не спиралася на дозволи одного інженера [5] B. Ноутбук був входом, але масштаб збитку визначила внутрішня архітектура довіри.

4.2. Ключ і право ним користуватися

Імовірний сценарій полягає в тому, що компрометація сервісу ініціювання транзакцій дозволила зловмиснику впливати на процес підпису D. Які саме внутрішні перевірки були обійдені, наразі публічно не встановлено. Перші заходи Binance після атаки, відкликання авторизацій скомпрометованих адрес і перебудова сервісу виведення та контролю адрес [2][6], узгоджуються з цим сценарієм, але не доводять його. Дев'ять переказів, підписаних другим гарячим гаманцем напряму, Elliptic трактує як ознаку того, що атакуючий міг безпосередньо давати команди інфраструктурі підпису [75] C.

Ієрархія між гаманцями. Binance 14 був власником смарт-акаунта Hot Wallet 34, тому після перехоплення керування Binance 14 атакуючий через його виклики вивів із Hot Wallet 34 ще 823 млн USDC [84][85] A / C. Ієрархія власності між гарячими гаманцями перетворює компрометацію одного гаманця на компрометацію кількох.

Незалежно від деталей цього інциденту, сценарій ілюструє загальну проблему машинних ідентичностей: службові облікові записи, контейнери і роботи часто мають ширші права, ніж люди, а перевіряються слабше. Людину автентифікують паролем, другим фактором і пристроєм; сервісу

нерідко довіряють за замовчуванням. Висновок НАК: захист ключа без захисту рішення про підпис не гарантує захисту активів. Політика підпису має перевіряти суть транзакції (адресу, суму, частоту, нову чи відому адресу) незалежно від того, хто її ініціював.

4.3. Прийом із 50 авторизаціями EIP-7702

Оновлення Ethereum Pectra (7 травня 2025 року) запровадило механізм EIP-7702: звичайний гаманець може підписати авторизацію, яка делегує його поведінку смарт-контракту [68]. Авторизація дійсна лише з поточним порядковим номером транзакції (nonce). Активний гарячий гаманець біржі постійно змінює nonce, тому атакуючий подав одну транзакцію з 50 заздалегідь підписаними авторизаціями для 50 послідовних nonce (18 914 775–18 914 824) [5][13] A. Одна з них збіглася, і через 3 хвилини 24 секунди гаманець було спорожнено [1]. За Bitquery, делегування діяло 3 години 50 хвилин, код атакуючого викликали сім разів, а скасовано делегування о 00:10:35 UTC, більш ніж через 90 хвилин після зупинки виведень [76].

Специфікація прямо попереджає, що погано спроєктований делегат може отримати майже повний контроль над гаманцем [68]. TRM припускає, що пачка з 50 підписів свідчить про обмежений у часі доступ атакуючого або про те, що підписи отримано від самої системи біржі [1] C. Зловживання EIP-7702 не нове: у 2025 році Wintermute повідомляла, що понад 80% делегувань EIP-7702 вказували на однаковий контракт-«пилосос» зловмисників [69].

4.4. Відображення на MITRE ATT&CK

Етап	Що відомо	Рівень	Техніки ATT&CK v20
Підготовка	Фінансування через Tornado Cash, тести і репетиція на сторонніх гаманцях [1]	C	Не відображається в Enterprise
Початковий доступ	Ноутбук DevOps-інженера [2]. Спосіб невідомий; можливий сценарій: фейкова співбесіда або «тестове завдання», як у кампанії Contagious Interview, атаки якої Binance відбивала за два дні до інциденту [18]	D	T1566.003 Spearphishing via Service; T1204.002 Malicious File; T1195.001 Compromise Software Dependencies and Development Tools
Облікові дані	Не розкрито. За аналогією з UNC4899 [55], CircleCI [36] і Bybit/Safe [26]: викрадення сесій і токенів	D	T1539 Steal Web Session Cookie; T1550.004 Web Session Cookie; T1552.001 Credentials In Files
Рух усередині	Доступ до службового контейнера заявок на виведення [2]; конкретні техніки не розкрито	B / D	T1078.004 Cloud Accounts; T1609 Container Administration Command; T1552.007 Container API
Зловживання підписом	Підписані перекази в 10 мережах; 50 авторизацій EIP-7702 [1][5]	A	Відповідної техніки немає
Наслідок	Виведення 6,36 млрд [1]	A	T1657 Financial Theft
Відмивання	Обміни на DEX, Aave, JustLend, THORChain [1][17][75]	A / C	Поза межами ATT&CK

MITRE описує Contagious Interview як групу G1052 і пов'язує з нею T1566.003, T1204 і T1195.001 [58]. Окремої сторінки для TraderTraitor (UNC4899, Jade Sleet, Slow Pisces) у MITRE немає; її діяльність задокументовано CISA, Google Cloud і Palo Alto Unit 42 [51][55][56].

5. Фінансова картина

5.1. Скільки вкрали: чому оцінок кілька

Оцінка	Хто	База оцінки	Рівень
6,36 млрд	TRM Labs [1]	Ціни на момент переказів	C
6,23 млрд	TRM Labs [1]	Поточні ціни після падіння ринку	C
близько 6,3 млрд	Binance [2]	«Зачеплені активи»	B
6,43 млрд	Elliptic [75]	На момент крадіжки	C
5,912 млрд; згодом 6,4 млрд	Chainalysis [10][81]	На момент крадіжки; оновлена оцінка CEO	C
понад 5,7 млрд (пік)	Arkham [8]	Баланс гаманців атакуючого	C



Рисунок 2. Виведені кошти за мережами, млн доларів США (TRM Labs, 00:30 UTC 30.10.2026) [1].

5.2. Заморожено і не заморожено

Хто заморозив	Актив	Сума	Джерело
Tether	USDT	близько 1,77 млрд у блокчейні (TRM); 1,567 млрд за заявою CEO Tether	[1][21]
Circle	USDC	близько 825 млн (TRM); «понад 800 млн у координації з правоохоронцями» за заявою CEO Circle	[1][22]
Ripple	RLUSD	40,5 млн підтверджено в блокчейні; заява I Xe про близько 200 млн не підтверджена	[1]
Arbitrum Security Council	ETH, ARB	близько 30 млн	[1]
World Liberty Financial	USD1	27,8 млн	[1]
Разом		**близько 2,7 млрд (TRM, 00:30 UTC; Bitquery); 2,84 млрд (Elliptic, 08:00 UTC); близько 3 млрд (Binance)**	[1][2][75] [76]

За Bitquery, шість з 11 заморозок Tether припали на вже порожні гаманці, а близько 729 млн USDT встигли обміняти на ETH і TRX до заморозки [76]; за Elliptic, Tether заморозив головний гаманець атакуючого в Ethereum через 37 хвилин, заблокувавши 1,18 млрд USDT [75].

Атакуючий швидко переводив стейблкоїни в незаморожувані активи: близько 325 млн USDT обміняно на децентралізованих біржах на 122 300 ETH більш ніж на 10% нижче ринку; 60 млн USDT внесено в Aave як заставу під позику близько 19 760 ETH; 300 млн USDT переведено в протокол JustLend у мережі Tron; із 88,5 млн RLUSD продано близько 48 млн до заморозки [1] A / C. Elliptic оцінює обміни ширше:

434 млн USDT на 160 451 ETH зі збитком 12–26% до ринку; Aave заморозив відповідні ринки після позики [75]. Залишок на адресах атакуючого оцінюють у близько 2,4 млрд (TRM, 00:30 UTC, ETH і BTC), 3,2 млрд (Bitquery, 06:43 UTC) і 3,33 млрд (Elliptic, близько 07:00 UTC, 43 адреси) [1][75][76].

Заморожене не означає повернене. Повернення потребує окремих правових процедур: Bybit через півтора року після зламу 2025 року добилася в американському суді попередньої заборони на розпорядження активами, повернувши близько 48,4 млн і заморозивши понад 30,5 млн [27].

5.3. Вплив на ринок

За вечір 29.10 біткоїн знизився на 4,8% нижче 77 тис. доларів, ефір на 5,7%, BNB на 8%, токен Aave на 11% [8]. За одну годину ліквідовано позиції з кредитним плечем на 629 млн доларів, з них 607 млн довгих [14]; за добу близько 1,54 млрд, 84% довгих позицій, близько 239 тисяч трейдерів [15]. Ринок почав знижуватися ще до перших сигналів про злам, тому весь обвал не можна приписувати інциденту [14]. До інциденту на Binance зберігалося близько 144 млрд доларів активів за даними DefiLlama, тобто втрата становить близько 4% [8]; страховий фонд SAFU оцінюється приблизно в 1 млрд доларів у біткоїнах [8]. Аналітики Fundstrat не вважають інцидент подією платоспроможності [16].

5.4. Розбіжності в даних

Показник	Розбіжність	Як трактує НАК
Початок атаки	20:05 UTC (TRM) проти 20:30 UTC (Arkham)	20:05: TRM фіксує XRP Ledger, Arkham рахує від руху в Ethereum
USDC	780 млн (Blockaid) проти 823 млн (TRM)	Два перекази з Hot Wallet 34: 780 млн о 20:41 і 43 млн о 20:59; разом 823 млн [84]
Гаманець BTC	«Гарячий» (TRM) проти «холодного» (CryptoQuant)	Не встановлено до технічного звіту Binance D
Загальна заморозка	2,54 млрд (рання заява Binance), 2,7 млрд (TRM), близько 3 млрд (пізніша заява Binance)	Цифри зростали протягом ночі; 2,7 млрд підтверджено в блокчейні
Bitget	350–388 млн у різних джерелах	Близько 387,5 млн за уточненою оцінкою компанії [45]
Фінансування з Tornado Cash	Три виведення вранці 28.10 (TRM) проти близько 1 ETH о 14:54 29.10 (Bitquery)	Можливо, різні адреси або етапи; не встановлено D
Кількість мереж	10 (TRM), 11 (Elliptic), 9 (Bitquery)	Різний облік другорядних мереж і токенів
Обмін USDT на ETH	325 млн зі знижкою понад 10% (TRM) проти 434 млн зі збитком 12–26% (Elliptic)	Різний час зрізу і перелік обмінів
Мости і міксери	Об'єднання коштів з Bitget через THORChain (ZachXBT); близько 1,9 млн TRX через THORChain (Elliptic); не виявлено до 06:43 UTC (Bitquery)	Рух через мости на ранок 30.10 мінімальний

5.5. Три незалежні реконструкції

НАК не обирає зручну цифру, а зіставляє три публічні блокчейн-реконструкції. Різниця пояснюється часом зрізу, переліком мереж і методикою оцінки.

Показник	TRM Labs [1]	Elliptic [75]	Bitquery [76]
Час зрізу даних	00:30 UTC	близько 08:00 UTC	06:43 UTC
Загальна сума	6,36 млрд	6,43 млрд	близько 6,3 млрд
Мережі	10	11	9 (17 гарячих гаманців)

Показник	TRM Labs [1]	Elliptic [75]	Bitquery [76]
Заморожено	близько 2,7 млрд	2,84 млрд (44%)	близько 2,7 млрд
На адресах атакуючого	близько 2,4 млрд (ETH і BTC)	близько 3,33 млрд (43 адреси)	близько 3,2 млрд
Біржі, міксери, мости	Далі очікуються мости і OTC-брокери	Майже нічого, крім близько 1,9 млн TRX через THORChain	Не виявлено
Атрибуція	TraderTraitor, висока впевненість	КНДР імовірно, із застереженнями	Власної не робить

6. Атрибуція

TRM Labs з високою впевненістю приписує атаку північнокорейській групі TraderTraitor [1]; генеральний директор Chainalysis Джонатан Левін назвав ту саму групу [11] C. Binance виконавця не називає. Державної атрибуції станом на 30.10 немає: Мін'юст і ФБР США на запити не відповіли [12]; речник Binance заявив, що компанія працює з правоохоронними органами, щоб встановити особи злочинців [11]. Аналітична атрибуція не є остаточним встановленням осіб злочинців.

Elliptic також вважає причетність КНДР імовірною, але не певною, і наводить застереження: спільна з Bitget адреса отримала лише близько 39 тис. доларів коштів Binance і може свідчити про спільного «відмивача», а не про того самого виконавця; стейблкоїни утримувалися 37–46 хвилин, що нетипово для КНДР; методи відмивання (маркетмейкери, DeFi-кредитування) відрізняються від схеми після зламу Bybit [75] C.

Контекст. За даними Chainalysis, у 2025 році з криптосервісів викрадено понад 3,4 млрд доларів, з них щонайменше 2,02 млрд (близько 59%) припадає на КНДР [47]. У 2026 році до зламу Bitget було викрадено 1,73 млрд у 333 інцидентах [48]; за даними DefiLlama, до 26 жовтня втрати від зламів у 2026 році становили 2,369 млрд у 312 інцидентах, тобто один інцидент Binance приблизно в 2,7 раза більший за всі втрати від зламів у 2026 році до нього [80]. За даними TRM, сукупні крадіжки КНДР до квітня 2026 року перевищили 6 млрд доларів [49]; якщо атрибуцію буде підтверджено, один інцидент 29 жовтня приблизно подвоїть цей показник. Багатонаціональна група моніторингу санкцій (MSMT) оцінювала крадіжки КНДР у щонайменше 2,84 млрд за січень 2024 – вересень 2025 року [50].

Методи. Уряд США ще у 2022 році описав TraderTraitor як кампанію проти системних адміністраторів та інженерів DevOps криптокомпаній через «рекрутингові» листи і троянізовані застосунки [51]. ФБР у 2024 році попереджало про «тестові завдання» на співбесідах, які запускають шкідливі пакети [52]. Google Cloud у 2025 році описав атаки UNC4899, у яких жертви запускали шкідливі Docker-контейнери на робочих машинах після звернень у LinkedIn і Telegram, а атакуючі використовували викрадені сесійні cookie в AWS [55]. Це найближчий публічний прецедент до ланцюжка, описаного Binance.

7. Порівняльний аналіз

НАК зібрала 15 публічно задокументованих інцидентів, включно з Binance, у яких вирішальну роль відіграла одна людина, один пристрій або один людський процес. Критерій «вхід через пристрій однієї людини» визначено в розділі 2.3 і показано окремою колонкою, щоб класифікацію можна було перевірити.

Таблиця 7a. Втрати й атрибуція

Інцидент	Дата	Втрати	Атрибуція	Тип атрибуції	Джерело
Binance	10.2026	6,36 млрд (TRM)	TraderTraitor (КНДР)	Аналітична	[1][11]

Інцидент	Дата	Втрати	Атрибуція	Тип атрибуції	Джерело
Bitget	09.2026	близько 387,5 млн	КНДР	Аналітична, заява CEO	[45][46]
Bybit (через Safe)	02.2025	близько 1,5 млрд	TraderTraitor	Державна (ФБР)	[25][26]
Radiant Capital	10.2024	близько 50 млн	UNC4736 / AppleJeus	Аналітична (Mandiant)	[28]
DMM Bitcoin (через Ginco)	05.2024	4 502,9 BTC, 308 млн	TraderTraitor	Державна (ФБР, поліція Японії)	[29][30]
Okta	10.2023	файли 134 клієнтів	не оприлюднено		[43]
MGM Resorts	09.2023	близько 100 млн (EBITDAR)	Scattered Spider / ALPHV	Заяви атакуючих	[40]
CircleCI	12.2022	секрети і токени клієнтів	не оприлюднено		[36]
LastPass	2022	резервні копії сховищ клієнтів	не оприлюднено		[34][35]
Uber	09.2022	доступ до внутрішніх систем	Lapsus$	Заява компанії	[44]
Ronin / Axie Infinity	03.2022	близько 620 млн	Lazarus	Державна (ФБР)	[31][33]
Arup	01.2024	25,6 млн	не встановлено		[38][39]
KnowBe4	07.2024	втрат даних немає	КНДР	Заява компанії	[42]
Coinbase	05.2025	витрати 180–400 млн (оцінка)	не оприлюднено		[41]
USGS (США)	2018	не оцінено	не застосовно		[37]

Таблиця 7б. Точка входу і класифікація

Інцидент	Точка входу	Приманка або метод	Вхід через пристрій однієї людини
Binance	Ноутбук DevOps-інженера (попередньо)	Не розкрито	так (попередньо)
Bitget	Zero-day у двох сторонніх засобах безпеки, далі сервер гаманців	Технічна вразливість	ні
Bybit (через Safe)	MacBook розробника Safe{Wallet}	Docker-проєкт «симулятор інвестицій»; викрадені сесії AWS	так
Radiant Capital	Пристрій розробника, далі кілька пристроїв	ZIP із «PDF-звітом» у Telegram від «колишнього підрядника»	частково
DMM Bitcoin (через Ginco)	Комп'ютер співробітника постачальника	«Тестове завдання» від «рекрутера» в LinkedIn; сесійні cookie	так
Okta	Особистий профіль Google на робочому ноутбуці	Збережені облікові дані сервісного акаунта	так
MGM Resorts	Служба підтримки	Дзвінок від імені співробітника (деталі зі слів атакуючих)	ні

Інцидент	Точка входу	Приманка або метод	Вхід через пристрій однієї людини
CircleCI	Ноутбук інженера	Шкідливе ПЗ, не виявлене антивірусом; викрадена сесія SSO з 2FA	так
LastPass	Домашній комп'ютер DevOps-інженера	Вразливе стороннє медіа-ПЗ, кейлогер	так
Uber	Особистий пристрій підрядника	Шкідливе ПЗ, викрадений пароль, «втома від MFA»	так
Ronin / Axie Infinity	Співробітник Sky Mavis	Фейкова вакансія, офер у PDF (за джерелами The Block [32])	так
Arup	Фінансовий співробітник	Відеодзвінок із дипфейками «колег»; 15 переказів	ні
KnowBe4	Найнятий «працівник»	Північнокорейський IT-працівник з викраденою особою	ні
Coinbase	Кілька працівників підтримки	Підкуп, далі вимога викупу 20 млн	ні
USGS (США)	Службовий ноутбук	Понад 9 000 сторінок для дорослих, зокрема через російські сайти зі шкідливим ПЗ	так

Що показує база

- За поточною класифікацією НАК, включно з попередньою оцінкою Binance, у 9 із 15 випадків початковий доступ отримано через пристрій однієї людини, ще в одному (Radiant) частково. У двох (Arup, MGM) людину обманули без компрометації пристрою, у двох (KnowBe4, Coinbase) загроза була всередині компанії, в одному (Bitget) вирішальною стала технічна вразливість периметра. Ці співвідношення описують цільову вибірку НАК, сформовану з інцидентів, де роль людини або пристрою вже була відома, і не є оцінкою поширеності методу серед усіх кібератак.
- У п'яти випадках (Bybit, DMM, Okta, LastPass, Uber) компрометація сталася в постачальника, на особистому пристрої або через особистий акаунт, тобто за межами формального периметра жертви.
- Сім із 15 інцидентів пов'язують із КНДР: три на рівні державної атрибуції (Bybit, DMM, Ronin), три на рівні аналітичної (Binance, Bitget, Radiant), один за заявою постраждалої організації (KnowBe4). Щонайменше у трьох із них (DMM, Ronin, KnowBe4) вхід пов'язаний з наймом: вакансія, тестове завдання або фіктивний працівник.
- У жодному випадку не зламано криптографію. Двофакторна автентифікація не зупинила атаки, у яких викрадали вже активну сесію (CircleCI, Bybit/Safe, DMM).

8. Матриця компрометації довіри

Перший аналітичний інструмент НАК показує, які саме повноваження отримував атакуючий у семи найкраще задокументованих інцидентах. Він допомагає зрозуміти, що втрата пристрою небезпечна не сама по собі, а тим, яку довіру система до нього має.

Інцидент	Людські облікові дані або сесія	Доступ через постачальника	Машинна ідентичність	Право ініціювати або підписувати транзакції	Обман процедури перевірки
Binance	○	·	●	●	○
Bybit / Safe	●	●	·	·	●
DMM / Ginco	●	●	·	●	●
Radiant Capital	●	·	·	●	●
CircleCI	●	·	●	·	·
LastPass	●	·	●	·	·
KnowBe4	·	·	·	·	●

Критерії колонок. Людські облікові дані або сесія: атакуючий використав пароль, cookie чи токен конкретної людини або шкідливе ПЗ на її пристрої. Доступ через постачальника: компрометація сталася в організації, що надає послугу жертві. Машинна ідентичність: атакуючий використав облікові дані сервісу, контейнера або інтеграції. Право ініціювати або підписувати транзакції: атакуючий отримав змогу створити або підписати фінансову транзакцію системою жертви. Обман процедури перевірки: людина або процес схвалили дію через підміну інформації чи особи.

● підтверджено первинним джерелом або аналітикою; ○ імовірно, рівень D; · не застосовно або не встановлено. Binance: підтверджено лише доступ до службового контейнера і надсилання несанкціонованих заявок на виведення за заявою компанії [2]; контроль над механізмом підпису залишається аналітичною оцінкою [1][75]. Bybit/Safe: викрадені сесії AWS, Safe як постачальник Bybit, шкідливий JavaScript показував підписантам легітимні транзакції [25][26]. DMM/Ginco: сесійні cookie, постачальник Ginco, підміна легітимного запиту на транзакцію [29][30]. Radiant: шкідливе ПЗ на пристроях підписантів, які бачили легітимні транзакції [28]. CircleCI: сесія SSO, викрадені токени і секрети клієнтів [36]; постраждалою організацією була сама CircleCI, тому колонку постачальника не позначено. LastPass: майстер-пароль через кейлогер, ключі доступу до резервних копій [34][35]. KnowBe4: обман процедури найму [42].

Висновок. У чотирьох із семи випадків (Bybit, DMM, Radiant, KnowBe4) атакуючий обманював процедуру перевірки, а не зламував її технічно, ще в одному (Binance) це імовірно; у трьох (Binance, CircleCI, LastPass) отримав машинні облікові дані. Найбільші втрати (Binance, Bybit, DMM) пов'язані з тим, що атакуючий впливав на саму транзакцію: ініціював її, підписував або підміняв те, що бачили підписанти.

9. Карта захисних бар'єрів

Другий інструмент НАК розділяє три різні завдання, які часто змішують: запобігти атаці, обмежити збиток і прискорити виявлення.

Інцидент	Запобігти	Обмежити збиток	Прискорити виявлення
Binance	Окремі робочі станції для привілейованого доступу; чужий код лише в одноразових ВМ; короткі сесії, прив'язані до пристрою	Незалежна політика підпису; ліміти гарячих гаманців у кожній мережі; затримка великих виведень на нові адреси; відкликання делегувань EIP-7702 одночасно із зупинкою виведень; без ієрархії власності між гарячими гаманцями	Моніторинг усіх мереж у реальному часі, зокрема XRP Ledger; сигнал на пакетні авторизації EIP-7702

Інцидент	Запобігти	Обмежити збиток	Прискорити виявлення
Bybit / Safe	Ізольовані середовища розробки без доступу до бойової хмари; короткі сесії AWS, прив'язані до пристрою	Незалежна перевірка хешу транзакції підписантами на апаратному пристрої	Контроль цілісності клієнтського коду (JavaScript) на сервері
DMM / Ginco	Тестові завдання лише в одноразових ВМ; вимоги безпеки в договорі з постачальником	Політика транзакцій: білі списки адрес і ліміти	Аномалії використання сесій постачальника
Radiant	Заборона відкривати архіви з месенджерів на пристроях підписантів	Підписанти на окремих чистих пристроях; незалежна симуляція транзакцій; апаратні гаманці з читабельним екраном	Моніторинг змін власників і порогів мультипідпису
CircleCI	EDR понад антивірус; прив'язка сесій до пристрою	Короткоживучі токени замість довгострокових секретів	Аномалії сесій за місцем і часом
LastPass	Заборона привілейованого доступу з особистих пристроїв; контроль стороннього ПЗ	Бойові ключі не в особистих сховищах паролів; окремі ключі резервних копій	Сигнали на масовий доступ до резервних копій
KnowBe4	Перевірка особи кандидата	Поступова видача доступів (спрацювало: даних не втрачено)	EDR на нових пристроях (спрацювало: близько 25 хвилин до ізоляції)

Запобіжні заходи для Binance є висновком НАК за аналогією з іншими інцидентами; фактичний спосіб проникнення не розкрито. Час реакції KnowBe4 розраховано НАК за часовими мітками компанії [42].

10. Методика оцінки ризику однієї робочої станції

Третій інструмент НАК відповідає на питання, яке варто поставити на раді директорів будь-якої компанії: що саме зможе зробити атакуючий, якщо завтра скомпрометують ноутбук конкретного інженера або керівника? Методика не дає числового рейтингу: вона відтворювана і дає якісний профіль ризику за шістьма вимірами.

Вимір	Ключові питання	Ознаки високого ризику	Приклад
1. Досяжність	Які системи доступні з цієї станції без додаткової автентифікації: бойова хмара, CI/CD, підпис, платежі?	Прямий доступ до бойових систем або до сервісів, що ініціюють транзакції	Binance, Bybit/Safe
2. Постійність повноважень	Повноваження постійні чи видаються на час задачі? Скільки живуть сесії і токени? Чи є секрети у файлах?	Постійні права адміністратора; довгі сесії; ключі API на диску	CircleCI, LastPass
3. Незалежне підтвердження	Які критичні дії вимагають підтвердження іншою людиною на іншому пристрої або незалежною політикою?	Одна людина або один сервіс може завершити критичну дію	Radiant, Arup
4. Гігієна середовища	Чи запускається сторонній код? Чи є особисті профілі, пошта, браузинг, права адміністратора?	Тестові завдання, особисті акаунти й робочий доступ на одному пристрої	DMM, Okta
5. Виявлення	Чи є EDR і телеметрія? Чи є сигнали на аномальні сесії? Скільки часу до виявлення?	Лише антивірус; немає сигналів на нові місця входу	CircleCI, KnowBe4

Вимір	Ключові питання	Ознаки високого ризику	Приклад
6. Відкликання і стримування	Як швидко можна відкликати сесії, токени і ключі та ізолювати пристрій? Які ліміти обмежують збиток за цей час?	Відкликання займає години; немає лімітів на суму чи частоту	Binance (делегування діяло 90+ хв після зупинки), KnowBe4

Порядок застосування. (1) Скласти перелік станцій з привілейованим доступом. (2) Для кожної відповісти на питання шести вимірів і позначити кожен як низький, середній або високий ризик. (3) Описати найгірший сценарій у вікні до відкликання доступу: які дії можливі і який збиток вони дають. (4) Для кожного високого виміру призначити контроль із розділу 11 і відповідального. (5) Повторювати оцінку після змін у ролях, системах чи постачальниках.

11. Контролі та зіставлення з рамками

Таблиця пов'язує контролі з етапами атаки і з вимогами визнаних рамок. Це аналітичне зіставлення НАК для полегшення впровадження, а не офіційна оцінка відповідності чи сертифікація. Номери контролів ISO/IEC 27001:2022 наведено за відповідністю з ISO/IEC 27002:2022 [62]; для формальних посилань варто звірятися з текстом стандарту.

Контроль	Етап	NIST CSF 2.0	ISO/IEC 27001:2022	Інші рамки
Окремі «стерильні» робочі станції для привілейованого доступу	Початковий доступ	PR.AA, PR.PS	8.1, 8.2, 8.18	Microsoft PAW [70]
Тестові завдання і чужий код лише в одноразових ВМ	Початковий доступ	PR.AT, PR.PS	6.3, 8.7	ФБР [52], Microsoft [54]
Короткі сесії, прив'язані до пристрою; повторна автентифікація для бойових систем	Облікові дані	PR.AA	8.5	NIST SP 800-207 [61]
Найменші привілеї для сервісних облікових записів і контейнерів; сегментація	Рух усередині	PR.AA, PR.PS	5.15, 5.18, 8.22	Zero Trust [61]
Незалежна політика підпису: адреса, сума, частота, нові адреси	Підпис	PR.PS, DE.AE	8.24, 8.32	CCSS 1.05.8.1, 1.05.2.2 [63]
Кілька підписантів на окремих пристроях у різних операторів	Підпис	PR.AA	8.2	CCSS 1.02.1.1, 1.02.4.1, 1.05.9.1 [63]
Ліміти гарячих гаманців; затримка великих виведень на нові адреси	Наслідок	GV.RM, PR.PS	8.32	Timelock-механізми
Моніторинг блокчейну в реальному часі з автоматичною зупинкою	Наслідок	DE.CM, DE.AE	8.15, 8.16	CCSS 2.02.3, 2.02.4.1 [63]
Управління ризиками постачальників і підрядників	Усі етапи	GV.SC	5.19, 5.20, 5.21	CCSS 2.03 [63]; DORA [66]
План реагування з контактами емітентів і правоохоронців, заготовлені заяви	Реагування	RS.MA, RS.CO	5.24–5.27	DORA: 4/24 год, 72 год, 1 міс. [67]

12. Регуляторний вимір

Європейський Союз. Регламент MiCA (2023/1114) з 30 грудня 2024 року вимагає від постачальників послуг з криптоактивами стійких IT-систем відповідно до DORA (стаття 68) і робить їх відповідальними за втрату активів клієнтів унаслідок інциденту, що їм приписується, у межах ринкової вартості на момент втрати (стаття 75(8)) [64][65]. Перехідний період для наявних операторів завершився 1 липня 2026 року [65]. DORA (2022/2554) застосовується з 17 січня 2025 року [66]; для великих ІКТ-інцидентів первинне повідомлення подається протягом 4 годин після класифікації і не пізніше 24 годин після виявлення, проміжне протягом 72 годин, фінальне через місяць [67]. Застосовність цих норм до конкретної юридичної особи залежить від її ліцензії і юрисдикції; НАК не аналізувала статус окремих компаній групи Binance. Рекомендації нижче є загальними для ринку.

Групові структури. Binance.US, окрема компанія, заявила, що інцидент її не зачепив [82]. Для регуляторів це аргумент оцінювати не лише юридичну, а й операційну відокремленість місцевих ліцензіатів міжнародних груп: чи мають вони власні ключі, інфраструктуру підпису і гарячі гаманці, чи користуються спільними з групою.

Україна. Закон «Про віртуальні активи» № 2074-IX ухвалено у 2022 році, але він не набрав чинності. Законопроєкт № 10225-д прийнято в першому читанні 3 вересня 2025 року [74]; 31 липня 2026 року друге читання відклали на осінь через відсутність погодження між відомствами щодо розподілу повноважень НБУ і НКЦПФР [71]. Даних про голосування до 30.10.2026 НАК не знайшла. Українські IT-фахівці вже є ціллю фейкових рекрутерів: у серпні 2026 року CERT-UA попередив про кампанію UAC-0145 (підкластер Sandworm), яка під виглядом вакансій поширювала троянізований VPN-клієнт [72][73].

13. Рекомендації НАК

13.1. Біржам, кастодіанам і фінтеху

1. Розділити право ініціювати виведення і право його підписувати: система підпису має застосовувати власну політику, а не довіряти сервісу-ініціатору.
2. Тримати в гарячих гаманцях мінімально необхідні суми; запровадити ліміти на транзакцію і на період, затримки для великих виведень на нові адреси.
3. Не робити один гарячий гаманець власником інших: ієрархія власності між гаманцями поширює компрометацію з одного гаманця на кілька [84][85].
4. Моніторити всі мережі, а не лише Ethereum: у цьому інциденті атака почалася в XRP Ledger.
5. Заздалегідь погодити з емітентами стейблкоїнів і операторами мереж протокол екстреної заморозки з цілодобовими контактами.
6. Провести ревізію використання EIP-7702 і заборонити підпис авторизацій делегування поза контрольованим процесом.
7. Включити в план реагування відкликання вже виданих повноважень (делегувань, дозволів, сесій), а не лише зупинку сервісу: у цьому інциденті делегування EIP-7702 діяло понад 90 хвилин після зупинки виведень [76].
8. Пройти незалежну оцінку за CCSS v9 і оприлюднити її рівень.

13.2. Будь-якому бізнесу і державним організаціям

1. Застосувати методику з розділу 10 до станцій усіх, хто має привілейований доступ, починаючи з IT-директора і фінансового директора.
2. Виділити окремі пристрої для привілейованого доступу; заборонити на них особисті профілі і сторонній код.

3. Перевіряти платежі й скидання доступів через незалежний канал, незалежно від того, хто з'являється у відеодзвінку.
4. Включити вимоги безпеки до договорів з підрядниками і поширити на них моніторинг доступу.
5. Запровадити правило «повідом за п'ять хвилин без покарання» і перевіряти його на навчаннях.

13.3. Регуляторам, зокрема в Україні

1. Передбачити в законодавстві про віртуальні активи обов'язкове повідомлення про великі інциденти в строки, співставні з DORA.
2. Закріпити відповідальність кастодіана за втрату активів клієнтів і вимоги до сегрегації за зразком статті 75 MiCA.
3. Посилатися на визнані стандарти (ISO/IEC 27001, CCSS) як на мінімальні вимоги до ліцензіатів.
4. Вимагати від ліцензіатів, що входять до міжнародних груп, розкривати, чи спільні з групою ключі, інфраструктура підпису і гарячі гаманці, і демонструвати здатність стримати інцидент на рівні групи.
5. Створити механізм швидкої взаємодії з емітентами стейблкоїнів і міжнародними правоохоронними органами для заморозки активів.

13.4. IT-фахівцям і розробникам

1. Не запускати тестові завдання, архіви і репозиторії від рекрутерів на робочому пристрої; використовувати одноразову віртуальну машину.
2. Насторожуватися, якщо співбесіда швидко переходить у Telegram або вимагає встановити застосунок, VPN чи пакет.
3. Повідомляти службу безпеки про підозрілі звернення: інформація про одну кампанію захищає всю галузь.

13.5. Громадянам та інвесторам

1. Баланс на біржі є зобов'язанням біржі, а не монетами у вашому розпорядженні: довгострокові заощадження варто зберігати в апаратному гаманці.
2. Кредитне плече перетворює чужий інцидент на ваш збиток: у перші години ліквідовано позиції на сотні мільйонів доларів.
3. Після гучних зламів зростає шахрайство: жодна біржа не просить «підтвердити акаунт» за посиланням або переказати кошти на «безпечну адресу».
4. Стейблкоїни може заморозити емітент, і це стосується не лише злодіїв.

14. Відкриті питання та індикатори

Індикатор	Чому важливо	Очікуваний строк
Відновлення виведень на Binance	Головний індикатор ліквідності і довіри	за останньою оцінкою Binance, близько 05:47 UTC 01.11.2026 [78]
Технічний звіт Binance і оновлений Proof of Reserves	Підтвердить або спростує гіпотези про точку входу, спосіб зараження і роль інфраструктури підпису	Обіцяно, строк не названо [2]
Деталі «додаткових точок проникнення»	Покаже, чи був ноутбук єдиним входом, і змінить оцінку моделі «один пристрій»	Невідомо [77]
Державна атрибуція	Переводить атрибуцію з рівня C на рівень B	Невідомо
Рух 2,4 млрд в ETH і BTC	Мости, сервіси обміну і позабіржові брокери як точки можливого перехоплення	Постійно

Індикатор	Чому важливо	Очікуваний строк
Зв'язок із зламом Bitget	Якщо підтвердиться, йдеться про серію атак на біржі	Невідомо [17]
Повернення замороженого	Покаже реальну ефективність заморозки як інструменту захисту	Місяці
Реакція регуляторів ЄС і України	Перевірка норм MiCA і DORA; доля законопроєкту № 10225-д	2026–2027

Питання до архітекторів безпеки біржі. Чому одна службова роль могла ініціювати виведення в десяти мережах одночасно? Що саме означає «немає доказів витоку ключів», якщо підпис виконувався за командами скомпрометованого сервісу? Чи були сигнали в журналах доступу за 28–29 жовтня? Як заражено ноутбук і чи пов'язано це з кампанією фейкових співбесід? Чи пов'язане планове обслуговування гаманців Ethereum 28 жовтня з підготовкою атаки?

15. Обмеження та застереження

- Дослідження підготовлено протягом 14 годин після початку інциденту; частина даних попередня і може змінитися.
- Заяви Binance, керівників Tether, Circle та інших компаній зафіксовано за дописами в соцмережах і публікаціями медіа; НАК не відкривала дописи безпосередньо, текст заяви Binance відтворено за ідентичними цитатами в кількох незалежних виданнях [2][19][79].
- Блокчейн-дані подано станом на 00:30 UTC (TRM Labs), 06:43 UTC (Bitquery) і близько 08:00 UTC (Elliptic) 30.10.2026.
- Атрибуцію КНДР надали приватні аналітичні компанії; державної атрибуції немає. Згадка компанії чи особи не є звинуваченням.
- Дослідження не є інвестиційною чи юридичною порадою.

Як цитувати

Аналітичний центр НАК. Коли система довіряє зловмиснику: атака на Binance 29 жовтня 2026 року, компрометація машинних ідентичностей і нова архітектура кіберризиків. Research Report 02/2026 (NCAU-RR-2026-02). Національна асоціація кібербезпеки, 30.10.2026. ncaua.vercel.app/uk/research/binance-hack-machine-identity-trust-2026

Виправлення та коментарі: через контактну форму на сайті НАК.

Джерела

Інцидент Binance

1. TRM Labs. North Korea steals $6.36 billion from Binance in the largest hack in history. 29.10.2026. https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history
2. Binance. Попередня заява про інцидент безпеки, 30.10.2026 (X); переказ: PANews. https://x.com/binance/status/2115993361517891592 · https://panews.io/articles/01a18aa0-7624-71d3-95c4-901bde2cba87
3. FinanceFeeds. Binance edited hack statement twice. 30.10.2026. https://financefeeds.com/binance-hack-statement-edited-user-funds-safe/
4. FinanceFeeds. Binance halts withdrawals. 29.10.2026. https://financefeeds.com/binance-halts-withdrawals-suspected-hack/
5. FinanceFeeds. Eleven keys signed, no leak (дані Blockaid, заява P. Тенга). 30.10.2026. https://financefeeds.com/binance-hack-eleven-keys-signed-no-leak/
6. FinanceFeeds. Binance withdrawals to resume within 48 hours. 30.10.2026. https://financefeeds.com/binance-withdrawals-resume-48-hours/

7. CoinDesk. Live updates. 29–30.10.2026. https://www.coindesk.com/business/2026/10/29/live-updates-bitcoin-clings-to-usd80-000-as-strategy-s-cushion-thins-before-earnings
8. CoinDesk. Potential multi-billion Binance hack hitting crypto markets. 29.10.2026. https://www.coindesk.com/business/2026/10/29/potential-multi-billion-binance-hack-hitting-crypto-markets
9. TechCrunch. Binance pauses withdrawals. 29.10.2026. https://techcrunch.com/2026/10/29/binance-pauses-withdrawals-as-hackers-suspected-of-stealing-billions-in-crypto/
10. investingLive. Chainalysis estimates $5.9B stolen. 30.10.2026. https://investinglive.com/cryptocurrency/chainalysis-estimates-5-9b-stolen-in-suspected-binance-hack-nearly-4-times-bybit/
11. Associated Press (WFSB). North Korea-linked $6.3 billion hack, blockchain intelligence firms say. 30.10.2026. https://www.wfsb.com/2026/10/30/north-korea-linked-63-billion-hack-binance-blockchain-intelligence-firms-say/
12. Euronews / AFP. Binance confirms major hack. 30.10.2026. https://euronews.com/2026/10/30/crypto-platform-binance-confirms-major-hack-with-more-than-25bn-frozen
13. crypto.news. Binance hack: EIP-7702 wallet attack. 30.10.2026. https://crypto.news/binance-hack-eip-7702-wallet-attack/
14. PANews (дані CoinGlass). Ліквідації за годину. 29.10.2026. https://panews.io/articles/01a18974-b901-703b-9d7e-a863192210e2
15. crypto.news (дані CoinGlass). Bitcoin price falls, liquidations. 30.10.2026. https://crypto.news/bitcoin-price-falls-binance-hack-liquidations/
16. Yahoo Finance. Bitcoin drops to $76,000 as Binance hack spooks investors (коментар Fundstrat). 30.10.2026. https://finance.yahoo.com/markets/article/bitcoin-drops-to-76000-as-binance-hack-spooks-investors-tether-circle-freeze-assets-083406383.html
17. PANews. ZachXBT: кошти Binance і Bitget об'єднано через THORChain. 30.10.2026. https://panews.io/articles/01a18b2f-d427-707d-a6ae-55777882372c
18. TokenPost. Binance blocked North Korea-linked attacks (Contagious Interview). 27.10.2026. https://www.tokenpost.com/news/technology/41876
19. The Hacker News. Binance suffers security breach. 30.10.2026. https://thehackernews.com/2026/10/binance-suffers-security-breach.html
20. The Cryptonomist. Binance hacking update: withdrawals. 30.10.2026. https://en.cryptonomist.ch/2026/10/30/binance-hacking-update-withdrawal/
21. Паоло Ардоїно (Tether), допис про заморозку USDT. 29.10.2026. https://x.com/paoloardoino/status/2115918000373346709
22. Джеремі Аллер (Circle), допис про заморозку USDC. 29.10.2026. https://x.com/jerallaire/status/2115916207463481846
23. ChainCatcher. Bybit: системи працюють нормально. 29.10.2026. https://www.chaincatcher.com/en/article/2300138
24. Forbes. Binance's $6.3 billion hack started with one engineer's laptop. 30.10.2026. https://www.forbes.com/sites/digital-assets/2026/10/30/binances-63-billion-hack-started-with-one-engineers-laptop/

Порівняльні інциденти

25. FBI. PSA I-022625-PSA: North Korea responsible for $1.5 billion Bybit hack. 26.02.2025. https://ic3.gov/psa/2025/psa250226
26. The Hacker News. Safe{Wallet} confirms North Korean TraderTraitor hackers (дані Mandiant). 07.03.2025. https://thehackernews.com/2025/03/safewallet-confirms-north-korean.html
27. NK News. Crypto exchange sues North Korean government over $1.5B heist. 08.2026. https://www.nknews.org/2026/08/crypto-exchange-sues-north-korean-government-and-hackers-over-1-5b-heist/
28. Radiant Capital. Incident Update. 06.12.2024. https://medium.com/@RadiantCapital/radiant-capital-incident-update-e56d8c23829e
29. FBI. FBI, DC3 and NPA identification of North Korean cyber actors tracked as TraderTraitor. 23.12.2024. https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom
30. BleepingComputer. FBI links North Korean hackers to $308 million crypto heist. 24.12.2024. https://www.bleepingcomputer.com/news/security/fbi-links-north-korean-hackers-to-308-million-crypto-heist
31. Sky Mavis. Back to Building: Ronin Security Breach. 2022. https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364
32. The Block. How a fake job offer took down the world's most popular crypto game. 06.07.2022. https://www.theblock.co/post/156038/how-a-fake-job-offer-took-down-the-worlds-most-popular-crypto-game
33. BleepingComputer. FBI links largest crypto hack ever to North Korean hackers. 14.04.2022. https://www.bleepingcomputer.com/news/security/fbi-links-largest-crypto-hack-ever-to-north-korean-hackers
34. LastPass. Security Incident Update and Recommended Actions. 01.03.2023. https://blog.lastpass.com/posts/2023/03/security-incident-update-recommended-actions

35. LastPass. Incident 2: Additional details of the attack. 2023. https://support.lastpass.com/help/incident-2-additional-details-of-the-attack
36. CircleCI. CircleCI incident report for January 4, 2023 security incident. 12.01.2023. https://circleci.com/blog/jan-4-2023-incident-report
37. U.S. Department of the Interior, Office of Inspector General. Management Advisory: USGS IT Security Vulnerabilities. 17.10.2018. https://www.oversight.gov/sites/default/files/oig-reports/ManagementAdvisory%20_USGSITSecurityVulnerabilities_101718_0.pdf
38. CNN. Arup revealed as victim of $25 million deepfake scam. 16.05.2024. https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk
39. The Standard (Hong Kong). HK's first deepfake video conference scam. 04.02.2024. https://www.thestandard.com.hk/news/article/213122/HKs-first-deepfake-video-conference-scam-involving-HK200-million
40. MGM Resorts International. Form 8-K. 05.10.2023. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm
41. Coinbase Global. Form 8-K. 14.05.2025. https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm
42. KnowBe4. How a North Korean fake IT worker tried to infiltrate us. 23.07.2024. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
43. Okta. Unauthorized access to Okta's support case management system: root cause and remediation. 03.11.2023. https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause/
44. Uber. Security update. 2022. https://uber.com/newsroom/security-update
45. BleepingComputer. Bitget hacked via zero-day in third-party security products. 30.09.2026. https://www.bleepingcomputer.com/news/security/bitget-hacked-via-zero-day-in-third-party-security-products/amp/
46. The Defiant. Chainalysis links $387 million Bitget hack to North Korea. 02.10.2026. https://thedefiant.io/news/hacks/chainalysis-links-387-million-bitget-hack-to-north-korea

Статистика і контекст

47. The Record (дані Chainalysis). Over $3 billion in crypto stolen in 2025. 18.12.2025. https://therecord.media/over-3-billion-crypto-stolen-2025-north-korea
48. PYMNTS (дані TRM Labs). Bitget suffers year's largest crypto hack. 09.2026. https://www.pymnts.com/cryptocurrency/2026/bitget-suffers-years-largest-crypto-hack-as-losses-top-387-million/
49. Decrypt (дані TRM Labs). North Korean hackers have stolen $6 billion in crypto. 30.04.2026. https://decrypt.co/366241/north-korean-hackers-stolen-6-billion-crypto-trm
50. WorldECR. North Korea stole $2.84B in crypto over 21 months, monitoring team reports. 30.10.2025. https://www.worldecr.com/news/north-korea-stole-2-84b-in-crypto-over-21-months-allied-monitoring-team-reports/

Аналітика загроз і офіційні попередження

51. CISA, FBI, U.S. Treasury. AA22-108A: TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies. 18.04.2022. https://www.cisa.gov/ncas/alerts/aa22-108a
52. FBI. PSA I-090324-PSA: North Korea aggressively targeting crypto industry. 03.09.2024. https://www.ic3.gov/PSA/2024/PSA240903
53. FBI. PSA I-012325-PSA: North Korean IT workers conducting data extortion. 23.01.2025. https://www.ic3.gov/PSA/2025/PSA250123
54. Microsoft Threat Intelligence. Contagious Interview: malware delivered through fake developer job interviews. 11.03.2026. https://microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews
55. Google Cloud. Threat Horizons Report H2 2025 (UNC4899). 2025. https://services.google.com/fh/files/misc/cloud_threat_horizons_report_h22025.pdf
56. Palo Alto Networks Unit 42. Slow Pisces targets developers with coding challenges. 14.04.2025. https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/
57. Palo Alto Networks Unit 42. Two campaigns by North Korea bad actors target job hunters. 21.11.2023. https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
58. MITRE ATT&CK. Group G1052: Contagious Interview. https://attack.mitre.org/groups/G1052
59. MITRE ATT&CK. Group G0032: Lazarus Group. https://attack.mitre.org/groups/G0032

Стандарти, регулювання і технічні специфікації

60. NIST. The NIST Cybersecurity Framework (CSF) 2.0. CSWP 29. 26.02.2024. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
61. NIST. SP 800-207: Zero Trust Architecture. 2020. https://csrc.nist.gov/pubs/sp/800/207/final

62. NQA. ISO/IEC 27002:2022 mapping (номери контролів Annex A ISO/IEC 27001:2022). https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27002-Mapping.pdf
63. CryptoCurrency Certification Consortium (C4). CCSS v9.0. 17.12.2024. https://cryptoconsortium.org/ccss-table-v9/
64. Регламент (ЄС) 2023/1114 про ринки криптоактивів (MiCA). https://eur-lex.europa.eu/eli/reg/2023/1114/oj
65. ESMA. Interactive Single Rulebook, MiCA, статті 68, 75, 143. https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mica/article-75-providing-custody-and
66. Регламент (ЄС) 2022/2554 про цифрову операційну стійкість (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
67. FMA Austria. DORA: ICT-related incidents (строки звітування за RTS 2025/301). https://www.fma.gv.at/en/dora-ict-related-incidents/
68. Ethereum Improvement Proposals. EIP-7702: Set Code for EOAs. https://eips.ethereum.org/EIPS/eip-7702
69. The Block. Wintermute warns Pectra upgrade leaves Ethereum users at risk of automated attacks. 01.06.2025. https://www.theblock.co/post/356481/wintermute-warns-pectra-upgrade-leaves-ethereum-users-at-risk-of-automated-attacks
70. Microsoft. Privileged access devices. https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices

Україна

71. Інтерфакс-Україна. Друге читання законопроєкту про віртуальні активи відкладено. 31.07.2026. https://interfax.com.ua/news/political/1189726.html
72. CERT-UA. Попередження про кампанію UAC-0145. 12.08.2026. https://cert.gov.ua/article/6318863
73. DOU. Російські хакери атакують через фейкові вакансії і VPN. 08.2026. https://dou.ua/lenta/news/russian-hackers-attack-vpn/
74. Hromadske. Верховна Рада підтримала легалізацію ринку криптовалют (перше читання № 10225-д). 03.09.2025. https://hromadske.ua/en/politics/250673-verkhovna-rada-backs-cryptocurrency-market-legalization-details

Додаткові незалежні реконструкції та оновлення

75. Elliptic. The largest theft in history: North Korea likely behind the $6.4 billion Binance hack. 30.10.2026. https://www.elliptic.co/insights/binance-largest-hack-in-history/
76. Bitquery. Binance Hack: $6.3B Drained on 9 Chains, $2.7B Frozen. 30.10.2026. https://www.bitquery.io/investigations/binance-hack
77. Cointelegraph. Live updates: Binance $6.3B hack linked to North Korea's TraderTraitor (повідомлення про додаткові точки проникнення, 08:37 UTC). 30.10.2026. https://cointelegraph.com/news/live-updates-binance-63b-hack-linked-to-north-koreas-tradertraitor
78. The Crypto Times. Binance $6.3B Hack Update: More Breach Points, Withdrawals to Restart in 45 Hours. 30.10.2026. https://www.cryptotimes.io/2026/10/30/binance-hack-update-more-breach-points-withdrawals-to-restart-in-45-hours/
79. SecurityWeek. $6 Billion Binance Hack Bears Hallmarks of North Korea's TraderTraitor. 30.10.2026. https://www.securityweek.com/6-billion-binance-hack-bears-hallmarks-of-north-koreas-tradertraitor/
80. DefiLlama. Hacks dashboard (втрати 2026 року станом на 26.10.2026). https://defillama.com/hacks
81. Cointelegraph. North Korea's TraderTraitor linked to $6.3B Binance hack (оцінка Chainalysis 6,4 млрд). 30.10.2026. https://cointelegraph.com/news/north-korea-linked-to-63b-binance-hack-by-crypto-investigators
82. Reuters (CP24). Binance's possible hack triggers US$3 billion freeze in crypto assets (заява Binance.US). 29.10.2026. https://www.cp24.com/news/money/2026/10/30/binances-possible-hack-triggers-us3-billion-freeze-in-crypto-assets/
83. TokenPost. Binance to Pause Ethereum Deposits and Withdrawals for Wallet Maintenance. 27.10.2026. https://www.tokenpost.com/news/technology/41825
84. Yahoo Finance (Unchained). Binance Says User Funds Are 'Completely Safe' After $3.5 Billion Drains From Its Hot Wallets. 29.10.2026. https://finance.yahoo.com/markets/crypto/articles/binance-says-user-funds-completely-214417766.html
85. ChainCatcher. Discuss the incident of Binance being hacked (Binance 14 як власник Hot Wallet 34). 30.10.2026. https://www.chaincatcher.com/en/article/2300203
86. CryptoTicker. Binance Hack: Around $2.8 Billion Drained From a Hot Wallet (хронологія, допис Spreek). 29–30.10.2026. https://cryptoticker.io/en/binance-hack-hot-wallet-drained/

© 2026 Національна асоціація кібербезпеки · Аналітичний центр НАК · NCAU-RR-2026-02