Державна служба
спеціального зв'язку та захисту
інформації України

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Системи криптографічного захисту інформації



Інформаційний бюлетень
ISSN 3154-8814 (print)

№ 1 ◦ 2026

Державна служба
спеціального зв'язку та захисту
інформації України

Інформаційний бюлетень №1

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

системи криптографічного захисту інформації

виходить щомісяця

Київ ◦ 2026

УДК 001.92(051)

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ:

системи криптографічного захисту інформації

Інформаційний бюлетень №1 ◦ 2026

Редакційна колегія:

Головний редактор: д-р техн. наук, професор Олександр ПОТІЙ, Держспецзв'язку.

Заступник головного редактора: д-р юрид. наук, професор Володимир ТРОФИМЕНКО, Держспецзв'язку.

Відповідальний редактор: д-р техн. наук, професор Володимир ПАВЛІКОВ, ДержНДІ технологій кібербезпеки.

Технічний редактор: д-р техн. наук, доцент Семен ЖИЛА, ДержНДІ технологій кібербезпеки.

Члени редакційної колегії:

ДержНДІ технологій кібербезпеки: Дмитро БОНДАРЕНКО; канд. техн. наук Олександр ДИРДА; Сергій ЛИСЕНКО; Ігор НАВРОЦЬКИЙ; канд. техн. наук Максим КОМАРОВ; Максим ІЩУК; канд. геогр. наук Микола ДОБИШ.

Департамент захисту інформації Адміністрації Держспецзв'язку: Михайло РИБКА; Микола СНІЖИНСЬКИЙ; Олександр ЧЕРНАЧУК.

Департамент цифрової трансформації Адміністрації Держспецзв'язку: Наталя ДОРОФЄЄВА.

Департамент кіберзахисту Адміністрації Держспецзв'язку: Олександр МАТВІЙЧУК-ЮДІН.

Державний центр кіберзахисту Держспецзв'язку: Артем ЖИЛІН.

Управління з кіберзахисту інформаційно-комунікаційних систем Адміністрації Держспецзв'язку: Віталій БЕЗШТАНЬКО.

Департамент протидії технічним розвідкам та інструментального контролю стану захисту інформації Адміністрації Держспецзв'язку: Вадим СИВКО; Сергій БЕЗВЕРХИЙ; Василь БАРЧЕНКО.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) – державний орган, який призначений для забезпечення функціонування та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону.

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації (ДержНДІ технологій кібербезпеки) – провідна науково-дослідна установа Держспецзв'язку, яка реалізує науково-технічні завдання у сферах криптографічного та технічного захисту інформації, розроблення і впровадження новітніх технологій кібербезпеки в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, а також технологій протидії технічним засобам розвідки.

Департамент захисту інформації Адміністрації Держспецзв'язку відповідає за реалізацію державної політики у сфері захисту інформації, забезпечуючи безпеку даних в державних інформаційних системах та об'єктах критичної інфраструктури.

ISSN 3154-8814 (print)

© Державна служба спеціального зв'язку та захисту інформації України, 2026

© Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, 2026



Шановні колеги!

Стрімкий розвиток інформаційних технологій, штучного інтелекту та нанонауки вимагає постійного оновлення навичок наукового та технічного персоналу. Саме професійна компетентність працівників прямо впливає на інноваційний потенціал галузей економіки держави та є стратегічною необхідністю для її сталого розвитку та економічної стабільності. Враховуючи ці тренди, підвищення професійної компетентності фахівців є однією з найважливіших складових місії Держспецзв'язку. Саме для досягнення цієї стратегічної мети ми започатковуємо видання періодичного інформаційного бюлетеня «Контури інформаційної безпеки», який охоплюватиме найважливіші вектори нашої діяльності:

- криптографічний захист інформації,
- технічний захист інформації,
- захист державних інформаційних ресурсів,
- кібербезпеку,
- протидію технічним розвідкам,
- процеси цифрової трансформації.

Сподіваюся, що це видання матиме тривалу та успішну історію і стане вагомим кроком у напрямі підвищення професійної компетентності фахівців. Нехай воно стане консолідуючим фактором, який стимулюватиме авторів та читачів до підвищення своєї наукової кваліфікації, інтенсифікації досліджень та публікації актуальних статей.

Бажаю авторам і читачам видання віри у свої сили, творчої наснаги і успіхів у напрямі зміцнення інформаційної безпеки держави.

Голова Держспецзв'язку **Олександр ПОТІЙ**



Шановні колеги!

У сучасних умовах цифрової трансформації суспільства питання інформаційної безпеки набувають особливої ваги. Комплексний підхід до безпеки, що включає криптографічний та технічний захист інформації, надійне збереження державних інформаційних ресурсів, кібербезпеку, протидію технічним розвідкам та безпечну цифрову трансформацію, є ключовим чинником забезпечення стабільної роботи держави. Це є гарантією стійкості системи державного управління та чутливої критичної інфраструктури до викликів воєнного стану.

Запровадження інформаційного бюлетеня «Контури інформаційної безпеки» має на меті систематичне інформування працівників за всіма цими напрямами про новини, оновлення законодавчої бази, актуальні статті, затверджені інструкції, досягнуті результати досліджень та практичні рекомендації.

Переконаний, що це видання стане важливим інструментом підвищення рівня обізнаності, перш за все, співробітників Держспецзв’язку та більш широкого загалу, а також значним кроком у напрямі формування загальної культури безпеки.

Бюлетень є результатом спільної роботи фахівців Адміністрації Держспецзв’язку та ДержНДІ технологій кібербезпеки. Упевнений, що така співпраця принесе обом сторонам тільки взаємну користь і дасть можливість досягнути синергетичного ефекту.

Закликаю кожного працівника уважно ознайомитися з матеріалами бюлетеня та вживати заходів щодо застосовування результатів цього ознайомлення для підвищення якісних показників своєї науково-практичної діяльності. Таким чином, спільними зусиллями ми зможемо підняти рівень обізнаності персоналу та активізувати його творчий потенціал.

Заступник
Голови Держспецзв'язку **Володимир ТРОФИМЕНКО**



Шановні читачі!

Щодня Україна веде війну за свою незалежність, суверенітет і належне майбутнє наступних поколінь. Ця війна не обмежується окремими гарячими точками або лініями на карті нашої країни. Ця війна набагато масштабніша і сягає усіх сфер діяльності громадян. Значний сегмент протистояння відбувається у інформаційній сфері, захист якої у нашій державі покладається на Державну службу спеціального зв'язку та захисту інформації (далі – Служба). При цьому передові наукові дослідження в інтересах Служби виконує Державний науково-дослідний інститут технологій кібербезпеки і захисту інформації (далі – Інститут).

Науковці Інституту – золотий фонд України - формують надійний щит інформаційної безпеки України. Саме вони проводять прикладні та фундаментальні дослідження, вибудовуючи надійну базу для захисту інформації.

Окрім наукових результатів науковці значну увагу приділяють популяризації безпеки через зрозумілі широким верствам населення (від учнів шкіл і ліцеїв до державних службовців) статті та огляди.

Друзі, саме такі статті і огляди підготовані у доступній для легкого сприйняття формі подаватимуться у започаткованій серії інформаційних бюлетенів «Контури інформаційної безпеки». Ці бюлетені інформуватимуть Вас про тренди у криптографічному і технічному захисті інформації, кібербезпеці, захисті державних інформаційних ресурсів, цифрової трансформації Служби та протидії технічними розвідкам. Щиро сподіваюся, що Ви отримаєте і задоволення від прочитання статей та оглядів, і користь від посилення власних знань з профілактики власної безпеки у сучасному цифровому просторі.

З повагою до науковців-авторів та кожного читача.

Начальник ДержНДІ
технологій кібербезпеки **Володимир ПАВЛІКОВ**

Зміст

ВСТУП 7

НОВИНИ 8

Запуск першого супутника з постквантовою криптографією у 2026 році – від теорії квантової загрози до реальної інфраструктури 9

Підготовка до епохи постквантової криптографії – виклики, стандарти та стратегії переходу 12

Криптографічні обмеження систем безпеки штучного інтелекту–теоретичні межі та практичні наслідки 16

РЕФЕРАТИ СТАТЕЙ 20

Статистичний аналіз і оптимізація механізмів багатофакторної автентифікації для захисту приватних криптографічних ключів 21

Проєктування довірених багаторівневих механізмів атестації 24

Ефективна гомоморфна обробка цілих чисел на основі схеми CKKS 27

Оцінка введення помилок із статистичним аналізом 30

ОНОВЛЕННЯ НОРМАТИВНОЇ БАЗИ 33

Нормативно-правові акти 2025 – першої половини 2026 років 34

МЕТОДИКИ ТА ІНСТРУКЦІЇ 38

Забезпечення випробувальної лабораторії методиками проведення перевірок криптоалгоритмів 39

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ 42

Дослідження шляхів створення квантової системи розподілу ключів 43

АКТУАЛЬНА ІНФОРМАЦІЯ 50

Блокчейн-технології. Основні переваги та сфери застосування 51

Принципи відновлення інформації на криптомодулях методами реверс-інжинірингу 63

Шляхи запобігання «квантовому апокаліпсису» 75

Щодо криптографічної стійкості криптоалгоритмів та криптопротоколів, які використовуються в Україні 80

ВИСНОВКИ 86

Вступ

У сучасному світі місце та роль держави визначає її спроможність виробляти і застосовувати нові знання та технології, у тому числі новітні інформаційно-комунікаційні технології в усіх сферах життєдіяльності людини, суспільства та держави.

Відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» одними з основних завдань Державної служби спеціального зв'язку та захисту інформації України визначено забезпечення розвитку і нормативно-правового регулювання у сфері криптографічного захисту інформації (КЗІ) та проведення робіт з підтвердження відповідності засобів КЗІ. Враховуючи це, місія ДержНДІ технологій кібербезпеки полягає у підвищенні рівня інституційної спроможності та науково-технічної діяльності, а саме: продукування нових знань та впровадження світових стандартів у сфері КЗІ, супровід повного життєвого циклу вітчизняних засобів КЗІ та підвищення професійної компетентності фахівців у сфері КЗІ. Зокрема, на Інститут покладається завдання вирішення комплексу системних проблем наукового, нормативно-правового, технологічного та організаційного характеру, без подолання яких неможливе забезпечення сталого розвитку системи КЗІ, її інтеграції у міжнародний безпековий простір та забезпечення потреб ключових державних стейкхолдерів.

Основним спрямуванням Інформаційного бюлетеня є підвищення професійної компетенції фахівців у сфері КЗІ, яка розглядається як основа для підвищення продуктивності праці, пришвидшення адаптації вітчизняної системи КЗІ до викликів, які породжуються світовим технічним прогресом (у тому числі виклики, пов'язані з можливою появою квантових комп'ютерів), формування здатності фахівців щодо генерування нових ідей та впровадження сучасних технічних рішень.

Покликання видання окреслюється завданнями щодо ознайомлення фахівців з новинами у сфері КЗІ, останніми публікаціями у фахових журналах, результатами виконаних НДДКР, рефератами, які висвітлюють перспективні напрями розвитку сфери КЗІ (криптоалгоритми і програмне забезпечення для їх реалізації, сучасні високошвидкісні технічні засоби оброблення інформації, квантова і постквантова криптографія тощо).

НОВИНИ



Запуск першого супутника з постквантовою криптографією у 2026 році – від теорії квантової загрози до реальної інфраструктури

Ігор МАРТИНЮК, ДержНДІ технологій кібербезпеки

У січні 2026 року компанія **WISeKey International Holding Ltd** (“WISeKey”) організувала у Давосі спеціальний круглий стіл, присвячений питанням **квантової безпеки космічної інфраструктури**. Захід об’єднав експертів з космічної індустрії, кібербезпеки, оборонного сектору та квантових технологій для обговорення того, як розвиток квантових комп’ютерів може вплинути на безпеку супутникових систем.

Учасники підкреслили, що сучасні криптографічні алгоритми (зокрема RSA та ECC) у майбутньому можуть стати вразливими до квантових атак, що створює ризики для супутникових комунікацій, систем управління та передачі даних.

Уперше постквантова криптографія перестала бути експериментальною або лабораторною технологією й була інтегрована безпосередньо у діючу орбітальну систему. Компанія WISeKey International Holding разом із підрозділом WISeSat.Space оголосила про завершення розробки та початок орбітальних випробувань супутника, в якому квантовостійкі криптографічні механізми закладені на рівні базової архітектури безпеки.

Ця подія має принципово інший характер, ніж більшість попередніх заяв про готовність до квантової епохи. Йдеться не про пілотні стенди або емуляцію протоколів у дата-центрах, а про систему, що повинна стабільно працювати в умовах обмежених обчислювальних ресурсів, підвищеної затримки сигналу та багаторічного життєвого циклу без фізичного доступу до обладнання. Саме ці фактори роблять супутникові системи одним із найскладніших середовищ для впровадження постквантових алгоритмів.

Ключовою ідеєю реалізованого рішення стала **гібридна криптографічна модель**. Замість повної відмови від класичних алгоритмів використовується комбінація традиційної криптографії на еліптичних кривих і постквантових механізмів встановлення ключів. Такий підхід дозволяє одночасно зберігати сумісність із наявною наземною інфраструктурою та забезпечувати захист від майбутніх квантових атак. У практичному сенсі це означає, що сеансові ключі формуються з використанням як класичних, так і квантово-стійких компонентів і компрометація одного з них не призводить до

розкриття зашифрованого каналу.

> Причина

Причина, з якої саме **супутникові системи** стали одним із перших **реальних полігонів для постквантової криптографії**, пов'язана з їхнім життєвим циклом. Типовий супутник проєктується на десятиліття роботи, і **криптографічні алгоритми, які вважаються безпечними сьогодні, можуть втратити цю властивість задовго до завершення експлуатації апарата.** У цьому контексті загроза моделі **«записати зараз – розшифрувати пізніше»** набуває особливої актуальності. Перехоплений сьогодні супутниковий трафік може зберігатися роками й бути розшифрованим у момент, коли квантові обчислювальні системи досягнуть практичної ефективності.

Технічна реалізація постквантової криптографії у космічному апараті вимагала вирішення низки нетривіальних інженерних задач. Решіткові алгоритми, які лежать в основі більшості сучасних PQC-стандартів, потребують значно більших обчислювальних ресурсів і пам'яті, ніж класичні ECC-схеми. Для супутника це означає додаткове енергоспоживання, збільшення часу криптографічних операцій і ризик перевищення допустимих затримок у каналі зв'язку. У відповідь на це розробники застосували оптимізовані реалізації алгоритмів, часткову попередню генерацію криптографічного матеріалу на землі та апаратні захищені модулі для зберігання ключів і виконання критичних операцій.

Принципова **новизна** цього проєкту полягає не лише у самому факті використання постквантових алгоритмів, а й у тому, що вони розглядаються як складова повноцінної системи управління безпекою (а не як ізольований криптографічний модуль). **Архітектура передбачає можливість логічної криптоагільності – зміну політик використання алгоритмів при заданих апаратних обмеженнях.** Таким чином, система не «замикається» на одному наборі примітивів, а зберігає потенціал адаптації до нових стандартів і рекомендацій.

Для галузі космічних технологій цей проєкт означає **початок формування нового базового рівня вимог до інформаційної безпеки.** Якщо раніше квантовостійка криптографія розглядалася як перспектива віддаленого майбутнього, то у 2026 році вона стала практичним інженерним рішенням. Для криптографічної спільноти це важливий сигнал про те, що **постквантові алгоритми виходять за межі академічних публікацій і починають накопичувати експлуатаційну статистику**, яка має критичне значення для оцінки їх реальної надійності.

З практичної точки зору цей кейс демонструє, що організації, які розробляють системи з великим терміном служби, більше не можуть ігнорувати квантову загрозу. **Перехід до гібридних криптографічних моделей, закладання криптоагільності та орієнтація на постквантові стандарти мають відбуватися на етапі проєктування, а не як реакція на майбутні інциденти**. Запуск супутника з постквантовою криптографією у 2026 році фактично став точкою, з якої квантовостійка безпека перестала бути абстрактною концепцією й перетворилася на частину критичної глобальної інфраструктури.

WISeSat.Space Brought Together Global Thought-Leaders to Davos to Address Quantum Security in Space
https://www.globenewswire.com/news-release/2026/01/30/3229529/0/en/WISeSat-Space-Brought-Together-Global-Thought-Leaders-to-Davos-to-Address-Quantum-Security-in-Space.html

Підготовка до епохи постквантової криптографії - виклики, стандарти та стратегії переходу

Ігор МАРТИНЮК, ДержНДІ технологій кібербезпеки

На початку 2026 року в експертному середовищі кібербезпеки знову активізувалася дискусія щодо необхідності своєчасної підготовки до переходу на постквантову криптографію, PQC (Post-Quantum Cryptography). У публікації наведено позицію експертів, які наголошують, що організації повинні розпочинати підготовку до квантової ери вже зараз, навіть попри те, що повноцінні квантові комп'ютери ще не досягли практичного рівня застосування.

> Причина

Основною **причиною** такої позиції є **ризик атак** типу "Harvest Now, Decrypt Later" (HNDL) – **«збирай зараз, розшифруй пізніше»**. За цієї стратегії зловмисники можуть перехоплювати та накопичувати зашифровані дані сьогодні, щоб у **майбутньому розшифрувати їх за допомогою квантових обчислювальних систем**. Якщо дані мають довготривалу цінність (наприклад, державні документи, наукові дослідження, військові або технологічні розробки) їх **конфіденційність може бути поставлена під загрозу** навіть через десятиліття.

Ця проблема стала однією з причин активної роботи міжнародної криптографічної спільноти над **новими стандартами, здатними забезпечити стійкість до квантових атак.**

Більшість сучасних систем інформаційної безпеки базуються на криптографії з відкритим ключем. До найпоширеніших алгоритмів належать RSA, Diffie–Hellman та криптографія на основі еліптичних кривих (ECC). Безпека цих схем ґрунтується на складності певних математичних задач, зокрема факторизації великих чисел або обчислення дискретного логарифма.

Однак, розвиток квантових комп'ютерів може суттєво змінити ситуацію. Використовуючи **квантові алгоритми (алгоритм Шора)**, теоретично можна ефективно розв'язувати задачі, які лежать в основі сучасної криптографії. У разі створення достатньо потужного квантового комп'ютера це може призвести до компрометації значної частини наявних криптографічних систем.

У науковій літературі для опису такого пристрою використовується термін криптографічно значущий квантовий комп'ютер (Cryptographically Relevant Quantum Computer, CRQC). За оцінками дослідників, **подібні системи можуть з'явитися у проміжку між 2030 та 2035 роками**, однак точні терміни залишаються предметом дискусій.

Саме тому криптографічна спільнота прагне заздалегідь підготувати нові алгоритми, які залишатимуться безпечними навіть у разі появи квантових обчислювальних систем.

Центральну роль у формуванні нових криптографічних стандартів відіграє National Institute of Standards and Technology (NIST, US), який з 2016 року проводив міжнародний конкурс щодо відбору алгоритмів постквантової криптографії.

Після кількох етапів оцінювання та криптоаналізу у 2024 році були опубліковані **перші стандарти PQC**:

- **FIPS 203 ML-KEM** — алгоритм інкапсуляції ключів, що базується на решітковій криптографії (походить від алгоритму CRYSTALS-Kyber);
- **FIPS 204 ML-DSA** — алгоритм цифрового підпису (похідний від CRYSTALS-Dilithium);
- **FIPS 205 SLH-DSA** — геш-орієнтований алгоритм цифрового підпису, заснований на схемі SPHINCS+.

Ці **алгоритми** мають різні криптографічні властивості та **призначені для різних сценаріїв використання**. Зокрема:

- **ML-KEM** застосовується для **обміну ключами** у протоколах захищеного зв'язку;
- **ML-DSA** використовується для створення **цифрових підписів**;
- **SLH-DSA** забезпечує **альтернативний механізм підпису** з іншими криптографічними припущеннями.

Важливою особливістю цих алгоритмів є їх **стійкість до атак як класичних, так і квантових комп'ютерів.**

Попри появу перших стандартів, міграція до постквантової криптографії залишається складним багаторічним процесом. Вона охоплює не лише оновлення криптографічних алгоритмів, але й зміну архітектури інформаційних систем, програмного забезпечення та інфраструктури управління ключами.

Експерти пропонують **структурований підхід** до такої міграції, який складається з кількох наступних основних етапів.

1. **Підготовка.** На початковому етапі організація повинна визначити актуальність переходу до PQC, оцінити ризики та сформувати стратегічне бачення. Це включає створення

робочих груп, визначення відповідальних осіб та налагодження взаємодії з постачальниками програмного забезпечення.

2. **Оцінювання поточного стану.** Наступним кроком є інвентаризація криптографічних активів. Організація повинна визначити:
   - де саме використовується криптографія;
   - які алгоритми застосовуються;
   - які системи мають критичну залежність від криптографічних механізмів.

   Особливу увагу приділяють даним із довготривалим життєвим циклом.
3. **Планування переходу.** Після проведення аналізу формується стратегія переходу. Вона повинна включати технічні рішення, бюджет, графік модернізації та процедури тестування нових алгоритмів.
4. **Реалізація.** На цьому етапі відбувається впровадження нових криптографічних механізмів. Часто використовується гібридний підхід, коли класичні алгоритми застосовуються разом із постквантовими. Така схема дозволяє забезпечити сумісність із наявними системами.
5. **Безперервний моніторинг.** Оскільки постквантова криптографія є відносно новою галуззю, важливо постійно відстежувати нові дослідження, результати криптоаналізу та оновлення стандартів.

Крім того, перехід до PQC супроводжується низкою **технічних і організаційних викликів**:

1. **Нові алгоритми** часто мають значно **більші розміри ключів і підписів**, що може впливати на продуктивність систем і пропускну здатність мереж.
2. Багато **сучасних інформаційних систем** містять так звану **жорстко закодовану криптографію, коли алгоритми зашиті безпосередньо у програмному коді або апаратному забезпеченні**. Це ускладнює їхню заміну.
3. Значну проблему становлять **застарілі системи та пристрої з обмеженими ресурсами**, зокрема, IoT-пристрої або смарт-карти, для яких інтеграція нових алгоритмів може бути складною.

Окрім технічних аспектів, важливими є також організаційні фактори – **нестача кваліфікованих фахівців, відсутність чітких стратегій та обмежене фінансування**.

Незважаючи на складність переходу, розвиток постквантової криптографії вже став одним із ключових напрямів сучасної кібербезпеки. Провідні технологічні компанії починають

інтегрувати PQC-алгоритми у свої продукти, а міжнародні організації розробляють рекомендації щодо поступового переходу до нових стандартів.

Очікується, що у **найближчі роки відбудеться:**

- розширення набору **стандартизованих алгоритмів PQC**;
- **поява нових інструментів** для управління криптографічними міграціями;
- **інтеграція постквантових алгоритмів** у мережеві протоколи, хмарні платформи та системи цифрового підпису.

Expert Recommends: Prepare for PQC Right Now
https://thehackernews.com/2026/02/expert-recommends-prepare-for-pqc-right.html

Криптографічні обмеження систем безпеки штучного інтелекту - теоретичні межі та практичні наслідки

Ігор МАРТИНЮК, ДержНДІ технологій кібербезпеки

Стрімкий розвиток великих мовних моделей (LLM) призвів до широкого використання систем штучного інтелекту у різних сферах – від інформаційних сервісів до програмної інженерії та кібербезпеки.

> Потреба

Водночас зростає **потреба у механізмах контролю**, які запобігають генерації небезпечного або забороненого контенту. Такі механізми зазвичай реалізуються у вигляді **зовнішніх фільтрів** або guardrails, що аналізують запити користувача перед передачею їх до моделі. Однак останні дослідження криптографів показують, що подібні системи мають фундаментальні обмеження, які не можуть бути усунуті виключно інженерними методами.

У роботах, присвячених аналізу безпеки систем штучного інтелекту, доведено, що будь-які **фільтри**, які використовують менше обчислювальних ресурсів, ніж сама модель, **принципово не можуть гарантувати повний захист від обходу**.

Цей результат є важливим прикладом того, як криптографічне мислення дозволяє формально досліджувати межі безпеки сучасних систем штучного інтелекту.

Більшість сучасних **моделей штучного інтелекту** використовують **багаторівневу архітектуру безпеки**. У спрощеному вигляді вона складається з двох компонентів:

1. **Фільтр або модуль перевірки запитів** – система, що аналізує введений користувачем текст і визначає, чи є він небезпечним;
2. **Основна мовна модель** – потужна нейронна мережа, що генерує відповідь.

Фільтр працює як бар'єр – якщо запит містить заборонений зміст (наприклад, інструкції щодо виготовлення зброї або шкідливого програмного забезпечення), він блокується ще до передачі моделі.

Такий підхід є популярним з кількох причин:

- його легко впроваджувати після запуску системи;
- він не потребує повторного навчання моделі;

- нові правила можна швидко додавати у відповідь на знайдені вразливості.

Саме тому **більшість сучасних платформ застосовують зовнішні фільтри** як основний механізм захисту.

Однак, така архітектура має важливу структурну особливість – **фільтр зазвичай значно простіший і швидший за основну модель**. Саме ця асиметрія і створює фундаментальні проблеми безпеки.

З точки зору криптографії, система «фільтр + модель» нагадує двоступеневу схему, де **слабший компонент намагається контролювати сильніший**.

Розгляд ситуації через призму обчислювальної складності дає можливість прийти до висновку, що якщо **фільтр має менше ресурсів, ніж модель**, тоді існують задачі, які:

- **фільтр не може** розв'язати,
- **модель може** розв'язати.

Тобто можна створити запит, який виглядає **безпечним для фільтра**, але містить **приховану інформацію, яку модель зможе розкодувати**.

Це нагадує класичні криптографічні сценарії, де повідомлення ховається у зашифрованій формі, доступній лише для сторони з достатніми обчислювальними можливостями.

Дослідники показали, що у **подібній архітектурі завжди існуватимуть уразливості**, оскільки розрив у потужності створює простір для атак.

Одним із практичних прикладів такого обходу є використання **простого шифру підстановки**.

Суть методу полягає у тому, що **небезпечний запит кодується** шляхом заміни кожної літери іншою. Наприклад: **bomb → cpnc.**

Далі модель отримує інструкцію щодо розшифрування тексту та виконання отриманого запиту.

Оскільки **фільтр не здатний виконати декодування**, він пропускає повідомлення до моделі. **Модель**, маючи більші обчислювальні можливості, **розкодовує текст і відповідає на справжній запит**.

Такий тип атаки отримав назву controlled-release prompting. Цей приклад демонструє важливу ідею: навіть дуже **прості криптографічні прийоми** можуть бути достатніми для обходу захисних механізмів.

Ще складніший варіант атаки базується на криптографічному об’єкті, відомому як time-lock puzzle.

> **Time-lock puzzle** – це **механізм**, що дозволяє **«зашифрувати» інформацію** так, щоб її можна було **відкрити** лише після **виконання** певної кількості обчислень. Зазвичай це реалізується через повторне піднесення числа до квадрату або інші послідовні операції.

Ідея атаки полягає у такому:

1) небезпечний **запит ховається** всередині time-lock puzzle;

2) зовнішній фільтр **не може виконати** необхідні обчислення;

3) модель **розв’язує головоломку і отримує прихований запит**.

У деяких системах дослідники навіть використовували випадковий параметр (seed) генерації тексту як контейнер для такої головоломки. У цьому випадку сам запит виглядає безпечним (наприклад, «напиши вірш»), але зашифроване повідомлення приховане у випадковому числі. Після проходження фільтра модель розкодовує повідомлення і виконує приховану інструкцію.

На основі цих прикладів дослідники сформулювали загальний теоретичний результат – якщо **система безпеки використовує менше обчислювальних ресурсів, ніж сама модель, то завжди існуватимуть способи її обходу**.

Інакше кажучи, жодна **система фільтрів не може гарантувати повний контроль над поведінкою** більш потужної **моделі**.

Це твердження має фундаментальний характер і не залежить від конкретної архітектури або реалізації системи.

Таким чином, **проблема безпеки** LLM переходить із площини **інженерії** у площину **теоретичних обмежень** обчислювальних систем.

Отримані результати мають кілька важливих **наслідків:**

1. **Неможливість ідеальних guardrails (бар'єрів безпеки)**. Жодна система фільтрації не може повністю гарантувати, що модель не згенерує небажану інформацію.
2. **Постійна еволюція атак.** Як і в криптографії, між атакуючими та захисниками виникає постійна «гонка озброєнь».
3. **Необхідність багаторівневого підходу.** Безпека повинна включати не лише технічні механізми, але й організаційні, правові та процедурні заходи.

4. Значення криптографічних методів. **Криптографія може стати ключовим інструментом для формального аналізу безпеки систем штучного інтелекту.**

Дослідження криптографів демонструють, що сучасні системи захисту штучного інтелекту мають **фундаментальні обмеження**, пов'язані з їхньою **архітектурою**. Використання **зовнішніх фільтрів** для контролю більш потужної моделі створює **структурний розрив** у обчислювальних можливостях, який може бути використаний для обходу системи.

З точки зору теорії криптографії це означає, що **абсолютна безпека** таких систем **недосяжна**. Натомість **практичні системи** повинні орієнтуватися на **зниження ризиків**, а **не на повне усунення можливості атак**.

Hall, P. (2025, December 10). Cryptographers show that AI protections will always have holes. Quanta Magazine.
https://www.quantamagazine.org/cryptographers-show-that-ai-protections-will-always-have-holes-20251210/

РЕФЕРАТИ СТАТЕЙ



Статистичний аналіз і оптимізація механізмів багатофакторної автентифікації для захисту приватних криптографічних ключів

Назар ЗАЇКА, ДержНДІ технологій кібербезпеки

У сучасну інформаційну епоху асиметрична криптографія є однією із поширених технологій забезпечення інформаційної безпеки, яка використовується у критично важливих застосуваннях, зокрема у системах електронної пошти, інфраструктурі відкритих ключів, захисті фінансових транзакцій та криптовалютних мереж.

Центральним елементом таких систем є приватний криптографічний ключ, що використовується для підписання транзакцій та підтвердження автентичності операцій. Втрата або компрометація приватного ключа може призвести до катастрофічних наслідків, включаючи втрату доступу до цифрових активів або порушення безпеки інформаційних систем.

У зв'язку з цим значна увага приділяється розробці механізмів багатофакторної автентифікації (Multi-Factor Authentication, MFA), здатних забезпечити надійний захист приватних ключів у розподілених середовищах.

Робота присвячена статистичному аналізу та оптимізації архітектури MFA, орієнтованої на захист приватних ключів шляхом генерації ефемерних криптографічних ключів. Основною метою роботи є створення системи автентифікації, здатної функціонувати в умовах розподілених середовищ нульової довіри (zero-trust environments) та реалізовувати концепцію zero-knowledge MFA.

У запропонованій моделі **всі фактори автентифікації перевіряються одночасно**, що запобігає **послідовним атакам** на окремі фактори. На відміну від традиційних систем MFA, які зазвичай забезпечують лише бінарний результат перевірки доступу, запропонована архітектура спрямована **на генерацію ключів у бітах**. Будь-яка **зміна одного з факторів автентифікації** призводить до неможливості відновлення ключа та автоматичного блокування транзакції.

Ключовим елементом дослідження є використання **безшаблонної біометрії** (template-less biometrics) у поєднанні з **апаратними фізично неклонованими функціями** (Physical Unclonable Function, PUF), коли паролі користувачів

зберігаються на основі Static Random Access Memory (SRAM), статичної оперативної пам’яті з довільним доступом та яка зберігає дані доти, поки подається живлення.

Запропоновано **новий метод оптимізації біометричних даних**, що отримав назву **bit-chopping**, який передбачає **видалення найбільш значущих бітів (MSB)** із значень відповіді, отриманих із біометричних характеристик обличчя. Такий підхід дозволяє усунути **грубі варіації у вимірюваннях**, які можуть **спричиняти хибні прийняття**, зберігаючи при цьому специфічні для користувача деталі, що забезпечують унікальність біометричних ознак.

Методологія дослідження базується на **комплексному статистичному аналізі впливу** різних параметрів системи на її точність і надійність. Зокрема, було досліджено вплив точності аналого-цифрового перетворення (ADC) у діапазоні від 4 до 8 бітів, а також кількість видалених найбільш значущих бітів у межах від 0 до 4. Метою такого аналізу було визначення **оптимального балансу** між показниками **помилкового прийняття** (False Acceptance Rate, FAR) та **помилкового відхилення** (False Reject Rate, FRR).

Для проведення експериментів було використано набір даних, що включав 6000 зображень, згенерованих штучним інтелектом, які представляють 400 різних осіб. Для кожної особи було сформовано 25 зображень, серед яких 10 характеризувалися незначними варіаціями, а 15 — значними. Із цього набору було відібрано 200 осіб, половина з яких використовувалася для процесу реєстрації (enrollment), а інша половина — для тестування. Для оцінювання FAR було проведено 150 000 тестів шляхом порівняння реєстраційних таблиць із зображеннями інших осіб, тоді як для оцінювання FRR виконано 15 000 тестів, які повторювалися десять разів для забезпечення порівнянності результатів.

Окремо було проведено дослідження апаратного фактору автентифікації — SRAM-PUF-токенів. Для цього було використано 10 пристроїв, які генерували множинні зчитування бітових значень SRAM-пам’яті після циклів вимкнення та увімкнення живлення. На основі цих даних формувалися трійкові таблиці, що містили значення 0, 1 або X. Стабільні комірки з незмінними значеннями використовувалися для формування ключових бітів, тоді як нестабільні комірки позначалися символом X і виключалися з подальших обчислень. Результати аналізу показали, що приблизно **двадцяти циклів** увімкнення-вимкнення живлення **достатньо для виявлення нестабільних комірок та формування надійної таблиці реєстрації.**

Процес формування ключа здійснюється шляхом поєднання **біометричних даних**, результатів **PUF-зчитувань та пароля** користувача. Сервер передає клієнту інформацію про трійкову таблицю разом із випадковими значеннями Random Number (RN1 та RN2). Обидві сторони незалежно генерують ключ, використовуючи однакові параметри та алгоритм Response-Based Cryptography (RBC), що дозволяє компенсувати можливі помилки, спричинені шумом під час реального використання. У результаті клієнт і сервер отримують **однаковий криптографічний ключ**, який може використовуватися як безпечне початкове значення для постквантових криптографічних алгоритмів або безпосередньо застосовуватися для **шифрування та дешифрування** з метою **захисту приватних ключів**.

Результати дослідження свідчать про те, що **застосування запропонованого методу** видалення найбільш значущих бітів суттєво **підвищує** як **точність**, так і **безпеку системи**. Встановлено, що надто **низька точність вимірювання відстаней** у біометричній системі призводить до **підвищення показника помилкового прийняття**, тоді як **надмірна точність збільшує кількість помилкових відхилень**. **Оптимальне співвідношення** між цими показниками досягається при використанні **6–7 бітів точності ADC** та **видаленні 1–2 найбільш значущих бітів**. Така конфігурація забезпечує ефективне зменшення випадків помилкового прийняття без істотного впливу на коректну автентифікацію легітимних користувачів.

Отримані **результати** демонструють **потенціал інтеграції безшаблонної біометрії та PUF-технологій** у системах **багатофакторної автентифікації** для захисту криптографічних ключів. Запропонована архітектура забезпечує генерацію стабільних ефемерних ключів без помилок і може застосовуватися у розподілених криптографічних системах, зокрема у середовищах блокчейн-мереж, цифрових підписів та інших застосуваннях сучасної криптографії. Перспективи подальших досліджень включають інтеграцію додаткових факторів автентифікації, використання сенсорних PUF-пристроїв у переносних системах, а також розширення біометричної моделі шляхом використання тривимірних біометричних даних.

Mahafujul Alam, Julie B. Heynssens, Bertrand Francis Cambou (2026, March 6). “Statistical Analysis and Optimization of the MFA Protecting Private Keys” https://arxiv.org/abs/2603.05978

Проєктування довірених багаторівневих механізмів атестації

Назар ЗАЇКА, ДержНДІ технологій кібербезпеки

У сучасних інформаційних системах забезпечення довіри до віддалених обчислювальних середовищ є однією з ключових проблем криптографії та кібербезпеки. У багатьох сценаріях взаємодію між системами необхідно гарантувати, щоб віддалена система, до якої передається чутлива інформація або від якої отримуються дані, перебувала у безпечному та контрольованому стані.

Одним із механізмів, що дозволяє вирішувати задачу гарантування довіри до віддалених обчислювальних систем, є атестація (attestation), тобто надання доказів того, що певна система заслуговує на довіру для виконання чутливих операцій. Атестація вже застосовується у таких сферах, як контроль доступу до мережі, управління безпекою інформаційних систем та середовища довіреного виконання. Проте на практиці такі механізми часто охоплюють лише обмежену кількість компонентів системи, що створює потенційні можливості для зловмисників маніпулювати результатами перевірки та вводити в оману сторону, яка довіряє цим результатам.

Дослідження присвячене розробці принципів побудови надійних механізмів багаторівневої атестації, здатних забезпечити більш обґрунтовану оцінку довіри до віддалених обчислювальних систем.

> Проблема

Основна проблема, яка розглядається у роботі, полягає у тому, що **поверхневі або часткові механізми атестації** не здатні забезпечити повне уявлення про стан системи. У таких випадках навіть добре реалізовані механізми безпеки можуть бути пошкоджено зловмисниками, які здатні змінювати компоненти системи або приховувати свою присутність, наприклад, шляхом використання шкідливого програмного забезпечення з привілеями адміністратора або за рахунок вбудованих у ядро операційної системи механізмів.

У роботі запропоновано підхід до побудови надійних механізмів атестації, що базується на **принципі багаторівневості**. Суть цього підходу полягає у формуванні п**ослідовності шарів атестації**, кожен з яких надає докази щодо стану наступного компонента системи. Така структура дозволяє **поступово розширювати довіру** від базового рівня до вищих рівнів системної архітектури. Важливою передумовою цього підходу є

наявність **кореня довіри** (root of trust), на основі якого формується подальший **процес підтвердження** довіри до інших компонентів системи. Зокрема, використання апаратних механізмів дозволяє забезпечити більш надійну основу для формування таких доказів, оскільки **апаратний рівень є менш вразливим до атак**, спрямованих на програмне забезпечення.

Автори демонструють можливість практичної реалізації запропонованого підходу на прикладі конкретної системи, що використовує поширені апаратні та програмні компоненти. Зокрема, у ролі апаратного кореня довіри використовується модуль довіреної платформи Trusted Platform Module (TPM), а програмна частина системи базується на операційній системі Linux із механізмами посиленої безпеки Security-Enhanced Linux (SELinux). Додатково застосовується архітектура Integrity Measurement Architecture, яка дозволяє виконувати вимірювання стану системних компонентів. Така комбінація апаратних і програмних механізмів формує основу для створення багаторівневої інфраструктури атестації.

Одним із ключових аспектів дослідження є використання **формалізованої моделі противника**. У роботі розглядається сценарій, у якому зловмисник може модифікувати або підміняти компоненти системи, а також намагатися відновлювати їх для того, щоб обійти механізми перевірки. У цьому контексті система атестації розглядається як своєрідна **стратегічна взаємодія** між **механізмами безпеки та діями противника**. Завдання механізму атестації полягає у виявленні змін у системі та наданні достовірної інформації стороні, що оцінює її стан. Якщо система визнається надійною попри наявність компрометації, це означає успіх противника; в іншому випадку механізм атестації вважається ефективним.

У межах дослідження було розроблено та реалізовано прикладну систему, що виконує функції міждоменного шлюзу (Cross-Domain Solution, CDS). Така система використовується для обробки повідомлень між мережами з різними рівнями безпеки. CDS виконує функції фільтрації та перетворення повідомлень перед їх передачею через межу безпеки між мережами. Для цієї системи було реалізовано механізми безпеки та атестації, які дозволяють перевіряти стан компонентів системи та підтверджувати її відповідність визначеним вимогам безпеки.

У процесі дослідження було сформульовано набір **принципів проєктування**, які допомагають **розробляти та оцінювати системи багаторівневої атестації** та визначають **підходи до структурування** системи та організації взаємодії між її компонентами. Запропоновані принципи спрямовані на те, щоб механізми атестації могли надавати достатній обсяг доказів

для обґрунтованої оцінки довіри до системи навіть у присутності досить потужного противника.

Окрему увагу приділено оцінюванню ефективності запропонованих механізмів. Проведений аналіз показує, що використання багаторівневої архітектури атестації дозволяє **забезпечити надійність перевірки стану системи при мінімальному впливі на продуктивність**. Зокрема, експериментальна оцінка демонструє, що додаткове навантаження, пов'язане з використанням механізмів атестації, становить приблизно 1,3 %, що свідчить про **практичну придатність** запропонованого підходу для реальних інформаційних систем.

Для демонстрації універсальності запропонованих принципів автори також розглядають альтернативні варіанти реалізації системи. Зокрема, досліджується можливість використання іншого **апаратного кореня довіри**, заснованого на технологіях **конфіденційних обчислень**. У цьому випадку застосовується середовище довіреного виконання, реалізоване за допомогою технології AMD SEV-SNP, технології безпеки для процесорів Advanced Micro Devices. При цьому, SEV-SNP (Secure Nested Paging) забезпечує криптографічний захист пам'яті віртуальної машини від доступу або модифікації з боку гіпервізора чи інших віртуальних машин. Технологія працює таким чином, щоб пам'ять кожної віртуальної машини шифрувалася окремим ключем, та апаратні механізми процесора перевіряли цілісність сторінок пам'яті. З метою забезпечення безпеки зашифрованих даних у налаштуваннях гіпервізора, адміністраторами встановлено заборону на читання та модифікацію даних у пам'яті ВМ.

Аналіз показує, що запропоновані принципи побудови багаторівневих механізмів атестації **можуть ефективно застосовуватися** і в інших архітектурах.

Результати

Результати дослідження мають важливе значення для розвитку криптографічних механізмів забезпечення довіри у розподілених інформаційних системах. Запропонований підхід демонструє **можливість створення надійних механізмів атестації** на основі наявних апаратних і програмних засобів, що дозволяє **підвищити рівень безпеки** систем, які виконують критично важливі операції. Зокрема, використання багаторівневих механізмів атестації може бути корисним у системах обробки чутливої інформації, інфраструктурах довірених обчислень, мережах із підвищеними вимогами до безпеки та інших застосуваннях сучасної криптографії.

W. Thomas, L. Schmalz, A. Petz, P. Alexander, Joshua D., G. Paul, D. Rowe, J. Carter (2026, March 6). Designing Trust worthy Layered Attestations
https://arxiv.org/abs/2603.06326

Ефективна гомоморфна обробка цілих чисел на основі схеми CKKS

Ігор МАРТИНЮК, ДержНДІ технологій кібербезпеки

Зростання використання хмарних обчислень і розподілених систем обробки даних підвищує вимоги до забезпечення конфіденційності під час обробки інформації. Одним із перспективних підходів є повністю гомоморфне шифрування (Fully Homomorphic Encryption, FHE), яке дозволяє виконувати обчислення без розшифрування даних.

> CKKS

Серед сучасних **систем гомоморфного шифрування** значну популярність має схема **CKKS (Cheon-Kimm-Kimm-Song)**, яка дозволяє **ефективно виконувати обчислення над зашифрованими даними**, зокрема над наближеними дійсними числами. Однак виконання точних цілочисельних операцій у CKKS є складною задачею через **обмеження масштабування та накопичення шуму**, що потребує виконання дорогих операцій bootstrapping (спеціальної операції оновлення зашифрованих даних, яка дає можливість зменшити накопичення шуму та дозволяє робити необмежену кількість обчислень над шифротекстами).

Метою дослідження є розроблення ефективного методу виконання арифметичних операцій над цілими числами у середовищі CKKS, а також оптимізація складності таких операцій при гомоморфному обчисленні.

У класичних FHE-схемах найшвидше **зростання шуму в шифротексті** пов'язане з виконанням складних **арифметичних операцій**, що, відповідно, потребує достатньо частого застосування операції bootstrapping.

Особливу складність має реалізація таких операцій, як додавання та віднімання великих цілих чисел, порівняння значень, множення та операції зсуву. Зважаючи на це, основними проблемами є **висока обчислювальна складність гомоморфних операцій**, велика кількість необхідних bootstrapping-операцій та значна глибина обчислювальних схем.

Для вирішення цих проблем у роботі досліджуються **оптимізовані алгоритми арифметичних операцій** у схемі CKKS та їх ефективність.

Об'єкт дослідження – гомоморфні криптографічні системи та

алгоритми обробки зашифрованих даних.

Предмет дослідження – методи виконання арифметичних операцій над цілими числами у схемі CKKS з використанням гомоморфного шифрування.

Методологія дослідження базується на теоретичному аналізі гомоморфних обчислень у схемі CKKS та розробленні алгоритмів для виконання операцій над зашифрованими цілими числами.

Основні елементи методики включають:

- **використання дискретного варіанту CKKS**, що дозволяє працювати з цілими числами;
- **побудову алгоритмів** для арифметичних операцій над шифротекстами;
- **застосування операції bootstrapping** для підтримки допустимого рівня шуму;
- **аналіз складності** запропонованих алгоритмів.

Зокрема, у роботі розглянуто алгоритми додавання та віднімання, порівняння, множення та зсуву бітів. Для кожної операції проводиться оцінка кількості необхідних bootstrapping-операцій та обчислювальної складності.

Наукова новизна дослідження полягає у наступному:

- запропоновано **ефективний метод** реалізації гомоморфних арифметичних операцій над цілими числами у схемі CKKS;
- розроблено **алгоритмічні процедури** для основних арифметичних операцій із зменшеною кількістю bootstrapping-операцій;
- проведено **теоретичний аналіз складності операцій**, що дозволяє оцінити ефективність запропонованого підходу;
- показано можливість **практичного використання CKKS** для виконання складніших криптографічних задач.

Таким чином, у роботі представлено метод побудови ефективного гомоморфного цілочисельного обчислювача на основі схеми CKKS. Показано, що **запропоновані алгоритми** дозволяють виконувати основні арифметичні операції з **обмеженою кількістю операцій bootstrapping**. Зокрема, проведено оцінку складності для операцій додавання, порівняння, множення та зсуву, що продемонструвало покращення ефективності порівняно з існуючими підходами.

Отримані результати підтверджують можливість **використання CKKS** для побудови більш складних криптографічних протоколів, включаючи **обробку зашифрованих даних**, виконання приватних запитів до баз даних та **реалізацію**

криптографічних підписів у гомоморфному середовищі.

Запропонований підхід сприяє розвитку практичних застосувань повністю гомоморфного шифрування у системах захищеної обробки даних.

Kim, J. (2025). Efficient Homomorphic Integer Computer from CKKS. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(4), 873-898. https://doi.org/10.46586/tches.v2025.i4.873-898

Оцінка введення помилок із статистичним аналізом

Ігор МАРТИНЮК, ДержНДІ технологій кібербезпеки

Атаки з введення помилок (Fault Injection Attacks, FIA) є **однією з ключових загроз для апаратних реалізацій криптографічних алгоритмів**. Такі атаки можуть реалізовуватися шляхом навмисного порушення роботи пристрою (наприклад, через електромагнітні імпульси, лазерні впливи або збої живлення), що призводить до появи помилок у обчисленнях та витоку даних обмеженого доступу. Особливо небезпечними є сучасні статистичні методи аналізу помилок, такі як SIFA та SFA, які потребують значно меншої точності введення помилок.

> Мета досладження

Метою дослідження є аналіз підходу до автоматизованої оцінки стійкості криптографічних апаратних схем до атак уведення помилок із використанням статистичних методів.

Авторами запропоновано **фреймворк FIESTA**, який дозволяє оцінювати **ймовірність успішної атаки** на великі цифрові схеми **без необхідності повного перебору всіх можливих комбінацій помилок**.

Захист криптографічних пристроїв від атак уведення помилок традиційно ґрунтується на моделі threshold fault model, яка припускає, що зловмисник може **змінити обмежену кількість логічних елементів схеми**. Однак, **сучасні фізичні методи атак** (наприклад, **EMFI**) здатні одночасно **впливати на значну кількість елементів**, що робить класичну модель недостатньо реалістичною.

Існує проблема масштабованості (сучасні криптографічні схеми можуть містити тисячі логічних елементів), тому повний перебір усіх можливих комбінацій помилок стає обчислювально неможливим.

Основними **завданнями дослідження** є:

- **формалізація моделей** противника при атаках уведення помилок;
- **розроблення методу** статистичної оцінки ймовірності успіху атак;
- **створення інструменту** для автоматизованого аналізу великих апаратних схем;
- **перевірка підходу** на прикладі реалізацій криптографічних алгоритмів (зокрема AES).

Об'єкт дослідження – апаратні криптографічні схеми та їх стійкість до атак уведення помилок.

Предмет дослідження – методи статистичного аналізу ефективності атак уведення помилок і інструментальні засоби оцінювання безпеки апаратних реалізацій криптографічних алгоритмів.

Методологічна основа дослідження включає:

1. **Формальні моделі противника**:
   - threshold fault model;
   - random fault model;
   - general random fault model.
2. **Моделювання цифрових схем**. Схема подається у вигляді орієнтованого ациклічного графа логічних елементів, де моделюється поширення сигналів і можливе виникнення помилок.
3. **Статистичне оцінювання.** Для оцінки ймовірності успішної атаки використовується статистичне моделювання з багаторазовим випадковим вибором:
   - наборів помилок;
   - вхідних даних.
4. **Ймовірнісний аналіз.** Кількість ефективних помилок розглядається як випадкова величина з біноміальним розподілом, після чого обчислюється довірчий інтервал для ймовірності успіху атаки.
5. **Довірчі інтервали.** Для оцінки меж ймовірності використовується інтервал Клоппера–Пірсона, що забезпечує консервативну оцінку ймовірності успішної атаки.

Наукова новизна розглянутої роботи полягає у наступних досягнутих результатах:

- **запропоновано статистичний підхід** до оцінювання стійкості криптографічних схем до атак введення помилок без повного перебору всіх варіантів;
- **розроблено фреймворк FIESTA**, який дозволяє аналізувати великі цифрові схеми з тисячами логічних елементів;
- **запропоновано метод інтеграції фізичних характеристик мікросхеми** (наприклад, розташування елементів у **GDSII**-файлі) у процес оцінювання атак;
- **продемонстровано можливість** оцінювання реалістичних моделей противника з використанням статистичних методів.

У **результаті** проведеного дослідження показано, що статистичний підхід дозволяє **ефективно оцінювати стійкість криптографічних схем до атак введення помилок** навіть для великих апаратних реалізацій.

Фреймворк FIESTA забезпечує автоматизований аналіз схем на рівні логічних елементів та дозволяє визначати довірчі межі ймовірності успішної атаки. Це робить можливим **аналіз складних криптографічних систем без необхідності повного перебору всіх комбінацій помилок**.

Запропонований підхід може бути **використаний** для:

- **перевірки безпеки апаратних реалізацій** криптографічних алгоритмів;
- **порівняння ефективності** різних **механізмів захисту** від атак введення помилок;
- **оцінювання ризиків** для криптографічних пристроїв ще на етапі проєктування.

Таким чином, результати роботи демонструють перспективність використання статистичних методів для аналізу безпеки апаратних криптографічних систем та підвищення їх стійкості до фізичних атак.

Uhle F., Müller N., Moradi A. Fault Injection Evaluation with Statistical Analysis: How to Deal with Nearly Fabricated Large Circuits. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025, No. 4, pp. 215–253. https://doi.org/10.46586/tches.v2025.i4.215-253

ОНОВЛЕННЯ НОРМАТИВНОЇ БАЗИ



Нормативно-правові акти 2025 – першої половини 2026 років

Вадим РАДЧЕНКО, Департамент захисту інформації Адміністрації Держспецзв'язку

Щодо нормативно-правових актів у сфері криптографічного захисту інформації

> Наказ Адміністрації Держспецзв'язку **«Про затвердження Порядку допуску до експлуатації засобів криптографічного захисту службової інформації та інформації, що становить державну таємницю, та визначення криптографічних алгоритмів для застосування у засобах криптографічного захисту інформації»** зареєстровано Міністерством юстиції України у січні 2026 року.

Зазначений нормативний акт **розроблено на заміну** Положення про порядок допуску до експлуатації засобів криптографічного захисту інформації (що діяло з 2010 року), в якому, зокрема:

- **вилучено поняття** «засіб спеціального зв'язку» та «комплекс спеціального зв'язку»;
- **удосконалено процедури допуску** до експлуатації засобів криптографічного захисту службової та секретної інформації;
- **додано новий напрям тематичних досліджень** – компаративні дослідження (для засобів КЗІ, які мають сертифікат про відповідність міжнародному стандарту ISO/IEC 15408 з рівнем гарантії оцінювання не нижче EAL4 або внесені до каталогу сертифікованих продуктів НАТО, та які плануються до застосування для криптографічного захисту службової інформації).

> Наказ Адміністрації Держспецзв'язку **«Про затвердження Порядку надання та використання послуг електронної ідентифікації та електронних довірчих послуг, які використовуються в інформаційно-комунікаційних системах, в яких обробляються службова інформація та державна таємниця»** від 28.01.2026 № 67/ДСК зареєстровано Міністерством юстиції України 20.01.2026 за № 90/45484.

Зазначений нормативний акт **розроблено** відповідно до положень пункту 37 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» **з метою унормування порядку надання та**

використання послуг електронної ідентифікації та електронних довірчих послуг в інформаційно-комунікаційних системах, у яких обробляються службова інформація та державна таємниця.

Щодо змін нормативно-правових актів у сфері надання електронних довірчих послуг

> Наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 29.07.2025 № 250 **«Про скасування міждержавних стандартів»** з 01.01.2026 скасовано міждержавний стандарт ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Ця подія потребує уважного ставлення, зважаючи на те, що до поточного часу цей стандарт **широко використовувався** для надання **кваліфікованих електронних довірчих послуг** кваліфікованими надавачами електронних довірчих послуг, а саме обчислення функції гешування при формуванні та перевірянні цифрових підписів у відповідності до національного стандарту ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».

> Примітка

Важливим є той факт, що ДСТУ 4145-2002 дозволяється використання також будь-якої **іншої функції гешування, рекомендованої уповноваженим органом** державної влади у сфері криптографічного захисту інформації.

На поточний час, **одним із дозволених національних стандартів**, що визначають вимоги до функцій гешування, є ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» («Купина»). Ця функція гешування є **стійкою відносно класичних та квантових методів криптоаналізу**, тому її **можна використовувати** як цільову заміну геш-функції за ГОСТ 34.311-95 для створення та обробки електронних підписів за алгоритмом, визначеним ДСТУ 4145-2002.

Зважаючи на це, наразі, Міністерством цифрової трансформації України, з метою підвищення стійкості електронних підписів та цифрових даних до сучасних кіберзагроз, **здійснюються заходи** щодо переходу кваліфікованих надавачів електронних довірчих послуг до **створення та оброблення електронних підписів за алгоритмом, визначеним ДСТУ 4145-2002**, з функцією

гешування відповідно до ДСТУ 7564:2014.

Щодо змін міжнародних нормативно-правових актів у сфері інформаційної безпеки

Україна у жовтні 2025 року завершила процес приєднання до **Угоди про визнання загальних критеріїв CCRA** (Common Criteria Recognition Arrangement) відповідно до європейського та євроатлантичного вектору розвитку з метою впровадження кращих світових практик та інтеграції до європейського і світового ринків і простору безпеки.

> Довідково

CCRA – це міжнародна домовленість, побудована **на стандартах Common Criteria (ISO/IEC 15408)** та **Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045)**, які встановлюють єдині підходи до оцінювання засобів захисту інформації та підтвердження рівня довіри до такої оцінки, а також методології її проведення. ISO/IEC 15408 поділяє обсяг та глибину оцінки на 7 рівнів (Evaluation Assurance Levels, EAL), а CCRA передбачає взаємне визнання всіма авторизованими учасниками Угоди результатів такої оцінки за рівнями 1 та 2 (EAL1 – EAL2) або за відповідним профілем захисту для визначених цілей за рівнем 4 (EAL4), що усуває необхідність повторного тестування та сертифікації засобів у кожній окремій країні.

Приєднання держави до цієї угоди дає можливість **значно розширити номенклатуру засобів захисту інформації**, які використовуються для забезпечення безпеки інформаційно-комунікаційних систем. Основним результатом приєднання України до CCRA є **визнання сертифікатів, виданих країнами-учасниками CCRA**, завдяки чому продукція, яка вже має такі сертифікати, не потребує додаткової сертифікації. Це значно **спрощує запровадження сучасних систем захисту інформації** в інформаційно-комунікаційній системі (ІКС) та дає можливість уникнути зайвої бюрократичної тяганини.

Зокрема, приєднання до CCRA дає можливість **економити кошти за рахунок виключення процедур сертифікації в Україні**, підвищувати довіру до ІТ-продукції, зокрема до засобів захисту інформації, завдяки незалежному оцінюванню їх безпеки у акредитованих лабораторіях, а також відкриває перспективи виходу національної ІТ-продукції на міжнародні ринки.

Наразі Україна є користувачем CCRA, але невпинно **розвиває спроможності** та проходить регламентні процедури для набуття повноправного членства в Угоді з можливістю проведення всередині країни оцінки відповідності засобів

технічного та/або криптографічного захисту інформації, результати якої визнаватимуться всіма учасниками Угоди.

Ключовим механізмом імплементації положень CCRA на національному рівні є **зміни до Закону України** «Про захист інформації в інформаційно-комунікаційних системах», які були прийняті у 2025 році після ухвалення Закону України № 4336-IX. Зокрема, ці зміни передбачають, **можливість використання** в ІКС засобів технічного/криптографічного захисту інформації, які мають документ про відповідність (крім ІКС, в яких обробляється службова інформація або інформація, що становить державну таємницю), **виданий українським, або визнаним іноземним органом** з оцінки відповідності.

Зважаючи на **приєднання держави до CCRA**, постановою Кабінету Міністрів України від 26.11.2025 № 1531 **внесено зміни** до постанови Кабінету Міністрів від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», які передбачають **можливість використання** для забезпечення безпеки ІКС засобів захисту, які **оцінені у рамках CCRA**.

Крім того, для ІКС, в яких обробляється:

- **службова інформація**, дозволяється використання засобів захисту інформації, які мають **документ про їх оцінку відповідності з рівнем гарантії не нижче четвертого (EAL4)**, або які внесені до переліку сертифікованих продуктів НАТО (NATO Information Assurance Product Catalogue) (при цьому, додатково необхідна наявність експертного висновку у сфері захисту інформації, щодо відповідності результатів такої оцінки вимогам законодавства у сфері захисту інформації, отриманого за результатами проведення спрощеної процедури за компаративним принципом);
- **будь-яка інформація (за виключенням службової інформації або інформації, що становить державну таємницю)**, дозволяється використання засобів захисту інформації, які мають **документ про їх оцінку відповідності з рівнем гарантії не нижче другого (EAL2)**.

Перелік засобів захисту інформації, оцінених у рамках CCRA, та інформація щодо рівня їх оцінювання (EAL) наведені на офіційному порталі Common Criteria за посиланням:
https://www.commoncriteriaportal.org/products/index.cfm

Перелік продуктів, які внесені до переліку сертифікованих продуктів НАТО (NATO Information Assurance Product Catalogue), розміщено за посиланням:
https://www.ia.nato.int/search

МЕТОДИКИ ТА ІНСТРУКЦІЇ



Забезпечення випробувальної лабораторії методиками проведення перевірок криптоалгоритмів

Наталія ЛИСЕНКО, ДержНДІ технологій кібербезпеки

> Випробувальна лабораторія

Наукова підтримка діяльності **Випробувальної лабораторії** ДержНДІ технологій кібербезпеки (акредитована Національним агентством з акредитації України відповідно до вимог ДСТУ EN ISO/IEC 17025:2019, атестат акредитації № 201086) щодо випробувань засобів КЗІ реалізується шляхом розроблення методик, які визначають порядок проведення перевірок криптоалгоритмів та набори тестових прикладів для перевірки всіх наявних режимів їх роботи.

Атестат акредитації Національного агентства з акредитації України



НАЦІОНАЛЬНЕ АГЕНТСТВО З АКРЕДИТАЦІЇ УКРАЇНИ

НАЦІОНАЛЬНИЙ ОРГАН УКРАЇНИ З АКРЕДИТАЦІЇ

АТЕСТАТ ПРО АКРЕДИТАЦІЮ

Зареєстрований у Реєстрі
13 вересня 2021 року
за № 201086
чинний до 12 вересня 2026 року

Дата первинної акредитації: 13 вересня 2021 року

НАЦІОНАЛЬНЕ АГЕНТСТВО З АКРЕДИТАЦІЇ УКРАЇНИ ЦИМ ЗАСВІДЧУЄ КОМПЕТЕНТНІСТЬ

Випробувальної лабораторії
ДЕРЖАВНОГО НАУКОВО-ДОСЛІДНОГО ІНСТИТУТУ
ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

03142, м. Київ, вул. М. Залізняка, буд. 3, корп. 6.

3 4 7 3 2 3 3 1
(Код ЄДРПОУ)

ВІДПОВІДНО ДО ВИМОГ ДСТУ EN ISO/IEC 17025:2019 (EN ISO/IEC 17025:2017, IDT; ISO/IEC 17025:2017, IDT) У СФЕРІ:

випробування продукції на відповідність вимогам з криптографічного та технічного захисту інформації.

Сфера акредитації визначена додатком до цього атестата.
Додаток є невід'ємною частиною цього атестата і складається з 05 аркушів.

В.о. директора Сергій ПОПИК

м. Київ, 01133, вул. Генерала Алмазова, 18/7

НААУ є підписантом: 1) Угоди EA MLA у сферах «Випробування», «Калібрування», «Сертифікація персоналу», «Сертифікація систем менеджменту» та «Медичні лабораторії»; 2) Угоди ILAC MRA у сферах «Випробування», «Калібрування» та «Медичні лабораторії»; 3) Угоди IAF MLA у сферах «Сертифікація персоналу», «Сертифікація систем менеджменту».

Зокрема, для перевірки правильності реалізації криптоалгоритмів у засобах КЗІ, упродовж низки останніх років, було розроблено **комплект методик**, до складу якого були включені наступні нормативні документи:

1. **Методика перевірки правильності реалізації алгоритмів формування та перевіряння цифрового підпису**, визначених **ДСТУ 4145-2002** «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», за

допомогою тестових прикладів, **ЄАБА.460001.001.**

2. **Методика перевірки правильності реалізації криптографічних алгоритмів обчислення геш-функцій,** визначених **ДСТУ ISO/IEC 10118-3:2005** «Методи захисту. Геш-функції» за допомогою тестових прикладів.
3. **Методика перевірки правильності реалізації процедур шифрування, формування та перевіряння цифрового підпису**, визначених в «PKCS#1 v2.1: The RSA Cryptography Standard», за допомогою тестових прикладів, **ЄАБА.460001.006**.
4. **Методика перевірки правильності реалізації алгоритму формування та перевіряння цифрового підпису DSA**, за допомогою тестових прикладів, **ЄАБА.460001.014**.
5. **Методика перевірки правильності реалізації формування та перевіряння електронного цифрового підпису ECDSA**, за допомогою тестових прикладів, **ЄАБА.460001.015**.
6. **Методика перевірки правильності реалізації криптографічного алгоритму шифрування DES** за допомогою тестових прикладів, **ЄАБА.460001.027**.
7. **Методика перевірки правильності реалізації криптографічного алгоритму шифрування TDEA** за допомогою тестових прикладів, **ЄАБА.460001.007**, з доповненням № 1.
8. **Методика перевірки правильності реалізації криптографічного алгоритму шифрування AES** за допомогою тестових прикладів. **ЄАБА.460001.008**, з доповненням № 1.
9. **Методика перевірки правильності реалізації алгоритму симетричного шифрування RC2** за допомогою тестових прикладів, **ЄАБА.460001.016**.
10. **Методика перевірки правильності реалізації алгоритмів шифрування PBES1, PBES2** за допомогою тестових прикладів, **ЄАБА.460001.017.**
11. **Методика перевірки правильності реалізації алгоритму захисту ключа AESWrap** за допомогою тестових прикладів, **ЄАБА.460001.018**.
12. **Методика перевірки правильності реалізації алгоритмів захисту ключа 3DESWrap та RC2Wrap** за допомогою тестових прикладів, **ЄАБА.460001.019.**
13. **Методика перевірки правильності реалізації алгоритму автентифікації повідомлень CMAC** за допомогою тестових прикладів, **ЄАБА.460001.021**.
14. **Методика перевірки правильності реалізації алгоритму автентифікації повідомлень HMAC** за допомогою тестових прикладів, **ЄАБА.460001.025.**
15. **Методика перевірки правильності реалізації алгоритмів установлення ключів** відповідно до

ДСТУ ISO/IEC 15946-3:2006 з використанням кофакторного множення, **ЄАБА.460001.022.**

16. **Методика перевірки правильності реалізації алгоритмів протоколу узгодження ключів за схемою Діффі-Геллмана** за допомогою тестових прикладів, **ЄАБА.460001.026.**

Упродовж 2022 – 2023 років вищеозначений комплект методик доповнено наступними нормативними документами:

17. **Методика оцінки відповідності криптографічного модуля** вимогам **ДСТУ ISO/IEC 19790:2015**, **СТП ДНДІ ТКЗІ 01-22.**
18. **Методика перевірки правильності реалізації алгоритму обчислення ґеш-значення** відповідно до **ДСТУ 7564:2014** за допомогою тестових прикладів, **ЄАБА.460001.028.**
19. **Методика перевірки правильності реалізації криптографічного алгоритму симетричного блокового перетворення** відповідно до **ДСТУ 7624:2014** за допомогою тестових прикладів, **ЄАБА.460001.029.**
20. **Методика перевірки правильності реалізації алгоритму симетричного потокового криптографічного перетворення** відповідно до **ДСТУ 8845:2019** за допомогою тестових прикладів, **ЄАБА.460001.030**.

Наразі, методики 1–18 успішно апробовані під час проведення експертних досліджень та випробувань програмних та програмно-апаратних засобів КЗІ.

Апробація методик 19 та 20 буде проведена при перевірці реалізації криптоалгоритмів, визначених ДСТУ 7624:2014 та ДСТУ 8845:2019.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ



Дослідження шляхів створення квантової системи розподілу ключів

канд. техн. наук, доцент Олександр ЛИПСЬКИЙ, ДержНДІ технологій кібербезпеки

У ДержНДІ технологій кібербезпеки завершено виконання науково-дослідної роботи (НДР), присвяченої **дослідженню шляхів створення квантової системи розподілу ключів**. При виконанні цієї НДР проведено **аналіз сучасних систем квантового розподілу ключів**, а також проаналізовано **стандарти сучасних систем квантового розподілу ключів** та досліджено **основні вимоги** до них.

> Актуальність

Сучасна криптографія гарантує безпеку операцій, покладаючись на складні математичні обчислення. Серед найвідоміших методів – симетричні алгоритми (AES, ChaCha20), асиметричні (RSA, ECC), протоколи на кшталт SSL/TLS та геш-функції (SHA-256). Розв'язання цих задач вимагає значних обчислювальних ресурсів, які наразі відсутні.

Із розвитком квантових комп'ютерів ситуація у криптографії може змінитися. На відміну від звичайних комп'ютерів, квантові працюють за принципами квантової механіки (суперпозиції та заплутаності), що надає їм унікальні можливості. Ключовою особливістю квантових комп'ютерів є те, що замість бітів використовуються кубіти, кожен із яких здатен одночасно перебувати у станах 0, 1 або обох станах одночасно. Тому n-кубітний регістр може представляти 2^n станів одночасно. Це означає, що квантовий комп'ютер здатен обробляти всі ці варіанти одночасно в одному стані суперпозиції.

> Алгоритми

При появі достатньо потужного квантового комп'ютера майже всі класичні алгоритми асиметричної криптографії (RSA, DSA, ECDSA) можуть бути зламані. При цьому, симетричні алгоритми менш вразливі до таких атак і алгоритми з ключами 512 біт і більше залишаються безпечними.

Реакцією на загрози, пов'язані із високою імовірністю створення квантового комп'ютера, є формування **квантової та постквантової криптографій**.

Квантова криптографія базується на **фізичних принципах квантової механіки** для створення абсолютно захищених каналів зв'язку, тоді як **постквантова криптографія** – це **класичні алгоритми**, спеціально розроблені так, щоб

залишатися стійкими, навіть, при атаках квантових комп'ютерів.

Іншими словами, **квантова криптографія** використовує **квантові технології**, а **постквантова – захищає** класичні системи **від квантових загроз**.

Основні відмінності між цими напрямами, візуалізовані за допомогою ШІ «CoPilot», наведені у таблиці.

Відмінності між квантовою та постквантовою криптографією

Ознака	Криптографія	
	квантова	постквантова
Принцип роботи	Використання законів квантової фізики	Використання класичних математичних задач, які складно розв'язувати навіть квантовим комп'ютером
Приклад технології	Квантовий розподіл ключів (QKD)	Алгоритми на основі решіток, кодів, багатоваріантних рівнянь
Мета	Забезпечує абсолютну безпеку передачі даних	Зберігає стійкість сучасних систем шифрування після появи квантових комп'ютерів
Інфраструктура	Потребує спеціального квантового обладнання (фотонні канали, детектори)	Може працювати на звичайних комп'ютерах та мережах
Стан розвитку	Експериментальні проєкти	Активна стандартизація (NIST)
Загроза для класичних систем	Не загрожує напряму, але потребує нової інфраструктури	Прямо захищає від атак квантових комп'ютерів
Області використання	Рішення для урядів, військових та критично важливих систем (максимальна гарантія безпеки)	Прямо захищає від атак квантових комп'ютерів

На поточний час розробляється декілька квантових методів безпеки. **Основною технологією реалізації квантової криптографії** є **квантовий розподіл ключів** (Quantum Key Distribution, QKD).

Окрім QKD розробляються також інші (поки що менш розповсюджені) квантові методи безпеки, зокрема:

- **Quantum Secure Direct Communication (QSDC)** – дозволяє **передавати інформацію безпосередньо, без попереднього обміну ключами**. Втручання виявляють одразу, що забезпечує повну конфіденційність для критично важливих даних;
- **Quantum Bit Commitment** – дає змогу **зафіксувати інформацію та зберегти її прихованою до моменту розкриття**. Це корисно для безпечного голосування або угод, де важливо зберегти дані.

Наразі, серед вищеозначених методів безпеки, найбільш пристосованим для практичного використання є QKD. До найвідоміших з протоколів QKD відносяться протоколи BB84 та E91, а також Device-Independent QKD (розширений E91, де безпека доводиться навіть якщо обладнання недовірене). Наразі, ефективність цих протоколів доведена під час контрольованих експериментів і пілотних проєктів, шляхом підтвердження можливості безпечного обміну ключами через квантові канали.

Протокол BB84, який використовує **суперпозицію квантових станів** для передачі ключів, розроблений Чарльзом Беннеттом і Жилем Брассаром у 1984 році. Спроба перехоплення **змінює стан фотонів**, що одразу стає помітним. Протокол простий у концепції, але його реалізація вимагає точного обладнання для передачі та вимірювання квантових станів, що ускладнює впровадження.

Протокол E91, який застосовує **квантову заплутаність для передачі ключів**, запропонований Артуром Екертом у 1991 році. Заплутані пари фотонів генеруються джерелом і розподіляються між двома сторонами (Аліса і Боб). Кожна сторона вимірює свій фотон у випадковій фазі. Завдяки заплутаності результати вимірювань – корельовані. Заплутані частинки залишаються корельованими, навіть якщо вони розділені на великі відстані. Ключ формується із цих корельованих результатів. Якщо зловмисник (Єва) намагається несанкціоновано виміряти фотон, порушується квантовий стан і **кореляція між фотонами** Аліси і Боба **зменшується**, що сигналізує про атаку. Хоча реалізація протоколу E91 складніша, він забезпечує більш високий рівень захисту.

Зважаючи на **простішу реалізацію**, на поточний час у квантовій

криптографії у системах QKD найбільший розвиток отримало **застосування принципу суперпозиції** квантових станів (поляризації) фотонів.

У загальному випадку, QKD гарантує безпечний обмін ключами: будь-яке втручання одразу виявляють через зміну стану фотонів.

Порядок формування ключів:

1. **Передача фотонів:** дві сторони, наприклад, Аліса і Боб, обмінюються фотонами через оптоволоконний кабель. Фотони кодують інформацію через різні стани поляризації, які представляють біти інформації та використовують для передачі секретного ключа.
2. **Вимірювання фотонів:** будь-яка спроба перехоплення змінює стан фотонів через принцип невизначеності Гейзенберга. Якщо третя сторона, наприклад, Єва, спробує втрутитися, то зміна квантових станів одразу виявить спробу втручання.
3. **Вибір ключа:** після обміну фотонами Аліса і Боб порівнюють результати вимірювань. Якщо дані збігаються, вони використовують ці біти для створення секретного ключа.

Аналіз систем QKD

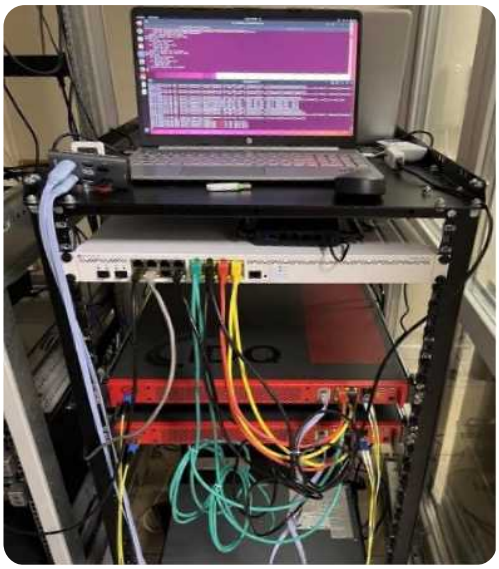
У результаті аналізу систем QKD визначено **перелік світових наукових центрів**, які проводять дослідження у сфері квантової криптографії, а також компаній, які постачають на світовий ринок відповідне технічне обладнання. Серед найбільш відомих постачальників обладнання названі компанії:

- id Quantique, Inc. (Швейцарія);
- MagiQ Technologies, Inc. (США);
- SmartQuantum, Inc. (Франція);
- QuintessenceLabs, Pty Ltd (Австралія);
- D-Wave Systems (Канада);
- Toshiba Research Europe Ltd (Великобританія);
- QinetiQ (Великобританія);
- NEC (Японія).

Для практичного ознайомлення із роботою QKD створено **макет квантової криптографічної системи** на базі рішення Cerberis XG компанії IDQ, загальний вигляд якого представлено на рисунку.

Запропоноване рішення дозволяє **розгорнути мережу вузлів** Cerberis XG QKD для квантового розповсюдження ключів у різних топологіях. Керування комплексом забезпечується з **центрального сервера** QNET шляхом конфігурування кожного вузла QKD і контролю його стану та роботи при перегляді централізованих журналів і журналів подій, статистики та даних про топологію.

Макет квантової \
криптографічної системи



Кожен вузол QKD складається з 2 субмодулів: передавача (Аліса) і приймача (Боб). **Квантовий зв'язок** між Алісою та Бобом здійснюється через стандартне **оптичне волокно SMF-28**. Синхронізація годинника QKD і постобробка здійснюються через двонаправлений оптичний канал QKD-Service. З'єднання QKD KMS (Key Management System) можуть бути мідними кабелями Ethernet або оптичними з використанням спеціального SFP-трансивера. Система управління ключами вузла QKD з'єднується безпосередньо через мідні кабелі Ethernet з шифрувальником і виступає у ролі арбітра між системами розподілу.

Можливості використання Cerberis XGR

Cerberis XGR виконує стандартні функції управління ключами між вузлами, включаючи **генерацію ключів, зберігання ключів і управління життєвим циклом ключів**. Cerberis XGR містить розширені надійні **компоненти безпеки**, такі як **виявлення несанкціонованого доступу, захищений модуль пам'яті**, а також чіп IDQ QRNG, який забезпечує **перевірену випадковість для всіх пов'язаних криптографічних функцій.** Це гарантує найвищі стандарти безпеки протягом усього процесу управління ключами, від генерації ключів до їх доставки (включаючи зберігання).

Адміністратори QKD мають можливість конфігурувати і контролювати мережі QKD через вбудований архітектурний стиль для веб-сервісів REST WebAPI або через веб-консоль системи управління елементами (EMS), встановлюючи споживачів, провайдерів на кожному вузлі мережі QKD.

WebAPI безперервно збирає кілька важливих параметрів, таких як стан системи, вентилятора, джерела живлення, температури, частота передачі квантових ключів, QBER (Quantum Bit Error Rate), буфери ключів KMS, і може передавати їх стороннім

системам моніторингу за допомогою поширених протоколів, таких як SNMP, syslog тощо. Події моніторингу також генеруються, коли QBER стає занадто високим, попереджаючи, що на квантовому каналі QKD може бути зловмисник.

Крім того, система квантового менеджменту (QMS) забезпечує єдину платформу управління та моніторингу для всіх продуктів і компонентів QKD. Це скорочує час і зусилля для управління великою та складною мережею QKD.

На поточний час вживаються заходи щодо створення на базі макетного зразка дослідного зразка системи QKD та проведення комплексу його випробувань.

Стандарти систем QKD

Ключовим аспектом систем квантового розподілу ключів є стандарт **ETSI GS QKD 014**, який визначає **протокол взаємодії та формат даних**, що використовуються для отримання криптографічних ключів від систем квантового розподілу ключів.

Документ описує програмний інтерфейс API (Application Programming Interface), який включає прикладні програми, що взаємодіють із системою керування ключами (Key Management Entity – KME). Загалом, REST інтерфейс API дає можливість генерувати нові ключі, отримувати ключовий матеріал та керувати використанням ключів.

Наявність архітектурного стилю REST дозволяє реалізувати: передачу даних через HTTPS, формат повідомлень JSON, використання стандартних HTTP-запитів. Стандарт забезпечує **сумісність між обладнанням різних виробників** (різні QKD-системи можуть працювати разом, прикладні програми можуть використовувати один стандартний API незалежно від типу обладнання).

Згідно із стандартом ETSI GS QKD 014 **основні компоненти системи QKD**:

1. **SAE** (Secure Application Entity). Прикладна система, яка використовує ключі, наприклад: VPN, TLS-шифрування і захищені канали зв’язку.
2. **KME** (Key Management Entity). Система керування ключами, яка отримує ключі від QKD-систем, зберігає їх та розподіляє їх між прикладними програмами.
3. **QKD-мережа**. Інфраструктура, яка генерує секретні ключі за допомогою квантових технологій.
4. Типовий **процес роботи**:

- QKD-пристрої генерують спільний секретний ключ;
- ключ передається до KME;

- прикладна система (SAE) надсилає запит через REST API;
- KME повертає ключ у форматі JSON;
- прикладна система використовує цей ключ для шифрування даних.

5. **Основні функції API** включають запит нового ключа, отримання ключового матеріалу, отримання ідентифікаторів ключів та перевірку стану системи.

Вся передача даних захищена HTTPS та механізмами автентифікації.

Таким чином, ETSI GS QKD 014 – це стандарт, який визначає REST-орієнтований API для отримання криптографічних ключів, створених QKD.

Результати

Отримані при виконанні НДР результати можуть бути покладені в основу створення **вітчизняної захищеної квантової криптосистеми.**

АКТУАЛЬНА ІНФОРМАЦІЯ



Блокчейн-технології. Основні переваги та сфери застосування

д-р техн. наук, професор Людмила КОВАЛЬЧУК, ДержНДІ технологій кібербезпеки

Блокчейн як базова технологія довіри

Потреба у довірі до наявних даних постійно існує у практичних задачах державного сектору та критичної інфраструктури: при веденні реєстрів, при фіксації юридично значущих подій, у сфері охорони здоров'я, у процедурах проведення тендерів та закупівель тощо.

За своєю структурою, саме блокчейн є найзручнішою платформою для захищеного зберігання інформації у цифровому вигляді. Одну з основних властивостей блокчейну можна неформально визначити так – зі збільшенням часу зберігання даних зменшується ймовірність успішної підміни цих даних. Ця властивість (у поєднанні з криптографічними механізмами і протоколом консенсусу) відкриває широкий спектр застосувань, де критично важлива незмінність та відтворюваний аудит.

Блокчейн–технології за останнє десятиліття перетворились з інструменту для криптовалютних транзакцій на універсальну платформу для побудови розподілених систем довіри – тобто таких систем, у яких учасники можуть довіряти певній інформації (щодо подій, транзакцій, стану реєстру тощо) в умовах повної недовіри та без наявності централізованого посередника [1, 2].

Разом з тим, блокчейн не є «чарівною паличкою». Переваги технології проявляються лише за умов правильного та безпечного використання цієї технології, з урахуванням всіх загроз та із застосуванням криптопримітивів із доведеною стійкістю. Окрема увага має приділятися стійкості до атак, специфічних для блокчейна (наприклад, атаки розгалуження, подвійної витрати, цензурування, маніпуляцій порядком транзакцій, атак на мережеву синхронізацію, атаки на смарт-контракти) [3–6].

Структура блокчейну та його основні властивості, що зумовлюють напрямки застосування

На поточний час є безумовне розуміння того, що неефективне паперове діловодство, яке створює величезну кількість паперових документів і бюрократичних механізмів, необхідно

замінити цифровими технологіями, які можуть ефективно забезпечувати співробітництво, довіру, доступ, прозорість, усунення посередників та людського фактору, конфіденційність і, при цьому, гарантувати непідмінність документа, підтвердження авторства та невідмовність. Таким принципам відповідає новітня і перспективна технологія блокчейн, в яку інтегровані певні криптографічні механізми.

Деякі концепції технології блокчейн було описано ще 30 років тому, проте справжнім початком використання цієї технології можна вважати 2008 рік, коли була написана робота [7]. Перше її практичне застосування відбулося у 2009 році, коли була створена криптовалюта Bitcoin. З кожним днем ця технологія стає все більш популярною, набуває ширшого спектру застосування.

> Блокчейн це новий **вид зберігання інформації**, який можна охарактеризувати як **децентралізовану базу даних**, що має певну структуру.

На відміну від **«класичних» баз даних**, де **інформація структурована у вигляді таблиць**, у **блокчейні інформація подається блоками**, причому **кожен наступний блок містить у собі геш-значення від попереднього блоку**. Внаслідок такої структури **блоки** у блокчейні **мають лінійний порядок**, зокрема кожен блок має чітко визначених «сусідів» – попередній та наступний блоки. Також **неможливо «непомітно» вилучити, додати або змінити блок** у блокчейні. Крім того, **вся інформація**, що є в блокчейні, зберігається децентралізовано – **дублюється на великій кількості серверів** (нодів), які розташовані **у різних точках світу**. Тому блокчейн є надійним та безпечним методом зберігання інформації, більш того – при цьому також **зберігається порядок, в якому ця інформація була додана до блокчейну**.

Спочатку блокчейн використовувався виключно для зберігання цифрових активів, але дуже швидко сфера його використання розширилась і він почав використовуватись для зберігання ідентифікаційної інформації, захисту авторського права, голосування тощо. Все більше передових (у галузі цифровізації) країн починають використовувати блокчейн у державному секторі, збільшуючи надійність даних та зменшуючи значимість людського фактору, що призводить, зокрема, до зниження корупції. Блокчейн – повністю прозора система, оскільки кожен бажаючий може отримати інформацію про будь-який блок.

Блокчейн використовує різні криптографічні механізми для забезпечення роботи системи.

Базовими криптографічними механізмами для блокчейну можна вважати:

- **геш-функції** (базовий механізм блокчейну, що забезпечує безпосередньо його структуру та функціонування);
- **цифрові підписи** (кожен користувач, який вносить якусь інформацію у блок, повинен підписати цю інформацію своїм секретним ключем і кожен бажаючий може перевірити коректність підпису).

Також у сучасних «просунутих» блокчейнах можуть опційно використовуватись **додаткові механізми**, зокрема, **доведення без розголошення, гібридне та гомоморфне шифрування, децентралізовані протоколи генерації ключа, децентралізоване розшифрування, кільцеві підписи** тощо. Ці механізми створюють додаткові властивості блокчейну та розширюють його функції, наприклад, забезпечують **підвищену анонімність**, можливість **приватного голосування** з покроковою перевіркою коректності, можливість **проведення тендерів** тощо.

Поняття протоколу консенсусу

Функціонування блокчейну регулюється так званим **протоколом консенсусу**. Іншими словами, протокол консенсусу це збірка правил, за якими блокчейн функціонує. Правила «записані» у вигляді програмного коду у самому першому блоці блокчейну (генезіс-блок), і не можуть бути порушені.

До цих правил належать:

- спосіб і правила генерації блоків у блокчейн;
- формат блоку;
- винагорода майнерам (особам, які генерують блоки);
- протокол вирішення конфліктів (за наявності конфліктуючих транзакцій), формат транзакцій тощо.

Мета протоколу консенсусу – дати можливість всім чесним **учасникам мережі домовитися про єдиний правильний погляд** на поточний стан блокчейну.

Найбільш поширеними протоколами консенсусу у блокчейні є протоколи **Proof-of-Work (PoW)** [7] та **Proof-of-Stake (PoS**) [8].

Протокол PoW був першим і наразі залишається домінуючим, хоча має ряд недоліків. Зокрема, він **потребує від майнерів постійного перебування у мережі** і постійного виконання великої кількості обчислювальної роботи (підбору такого прообразу геш-функції, для якого значення геш-функції належить деякій «невеликій» підмножині множини всіх можливих образів).

Оскільки для **створення кожного наступного блоку** потрібно виконати велику обчислювальну роботу, будь-яка **спроба непомітно змінити «давню» інформацію**, тобто **підмінити відповідний блок, потребує узгодженої підміни всіх наступних блоків** і є практично нездійсненною (за умови, що більшість учасників мережі чесно виконують правила, визначені протоколом консенсусу [1, 2, 9, 10]).

Чим більше блоків даних розташовано після вибраного блоку, тим складніше цей блок підмінити. У більшості блокчейнів ймовірність успішної атаки на підміну блоку (за наявності певних припущень щодо частки зловмисника та параметрів мережі) швидко спадає (експоненційно) зі зростанням кількості блоків, створених після нього [1, 5, 6, 7]. Користувачі мережі самі можуть вибирати, яку кількість блоків вважати достатньою для впевненості у незворотності транзакції.

У протоколі PoW була використана ідея, що лежить в основі протоколу HashCash [11], який вимагає від відправників електронного листа або запиту виконання невеликого об'єму обчислень перед надсиланням, щоб зменшити кількість спаму, що розсилається. Такі обчислення практично нічого не коштували для звичайного відправника, але це суттєво ускладнювало процес масового розсилання.

Протокол PoS – найпопулярніша альтернатива PoW. Це механізм консенсусу, який спрямовано на **усунення** деяких **недоліків протоколу PoW**, таких як **проблеми масштабування та енергоспоживання**. У цьому протоколі учасникам не потрібно використовувати потужне обладнання, щоб змагатися за можливість створення блоку. Натомість їм необхідно здійснити стейкінг, тобто заблокувати власну криптовалюту у блокчейні як депозит. Чим більша частка стейку (заблокованих коштів) у певного учасника, тим більша ймовірність того, що він буде слотлідером, тобто отримає право створення блоку у певному таймслоті (часовому відрізку) і, відповідно, отримає більшу винагороду за створення блоків.

Останнім часом з'являється багато робіт щодо **модифікацій блокчейну** та існуючих протоколів консенсусу з метою **збільшення пропускної здатності мережі** та (або) **зменшення часу очікування підтвердження блока**, тобто часу до його стабілізації у мережі [12].

Ідеї, що пропонуються у цих роботах, можна розділити на два типи:

1. **перехід від блокчейну до блокграфу** (directed acyclic graph);
2. **використання** різних **«багаторівневих» блокчейнів**, які можна вважати частковими випадками блокграфа.

Серед робіт першого типу – роботи [13–15], автори яких анонсували суттєве підвищення пропускної здатності мережі і зменшення часу очікування стабільності блоку. Проте жодна з названих робіт не містить строгих доведень заявлених результатів. У кращому випадку, замість доведень наведено напівемпіричні міркування. Більш того, у деяких з цих робіт є серйозні математичні помилки (наприклад, у [13–15]).

У роботах другого типу [16–19] містяться більш обґрунтовані твердження та більш строгі доведення.

Проте всі ці роботи спрямовані на вирішення лише однієї з вищеозначених проблем – збільшення пропускної здатності блокчейну.

Друга проблема (зменшення часу очікування підтвердження блока, тобто часу до його стабілізації у мережі) донині залишається невирішеною.

Огляд сфер застосування блокчейну

Як було зазначено, блокчейн є специфічною структурою для зберігання інформації в цифровому вигляді, і ця структура має таку властивість: чим довше в ній зберігається інформація, тим меншою є імовірність атаки на підміну інформації. Наприклад, у мережі біткоїн імовірність атаки на підміну блоку, що був створений добу тому, є меншою за 10^{-4}. Така властивість блокчейну забезпечується виключно використанням певного набору криптографічних інструментів, а для її доведення у різних моделях блокчейну потрібно використовувати потужний математичний апарат, у першу чергу методи теорії імовірності, алгебри тощо.

Саме ця властивість блокчейну забезпечує широкий спектр його можливих використань, серед яких криптовалюти є далеко не єдиним і не найголовнішим.

Далі наведено **найактуальніші приклади** таких **застосувань**.

Смарт-контракти

Смарт контракти – це **контракти**, які формалізовані, **записані у вигляді програмного коду** і **виконуються автоматично при настанні певних умов**. Смарт-контракти дозволяють переносити частину бізнес-логіки у середовище, де виконання правил є перевіреним, відтворюваним і (в ідеалі) незалежним від окремих виконавців [1, 20, 21].

> Приклад

> **Найпростішим аналогом роботи** смарт-контракту є робота **застосунків виклику таксі**. Коли користувач активує застосунок, з його карти автоматично списуються гроші, **які резервуються до завершення поїздки**. Коли поїздка завершена, ці гроші

надсилаються перевізнику. Якщо перевізник не надав послуги, він їх не отримує. При цьому з процесу виконання контракту практично повністю усувається «людський фактор», що суттєво знижує ризики недоброчесного виконання домовленостей.



Зображення створено за допомогою ШІ

> Приклад

Ще одним цікавим прикладом використання смарт-контрактів є **p2p-продаж електроенергії**, яка була згенерована децентралізовано (наприклад, продаж «зеленої» електроенергії від одного домогосподарства іншому). Такі смарт-контракти є дуже поширеними і вже майже 10 років використовуються у США, Великій Британії, Австралії, Новій Зеландії та в інших країнах. При використанні таких смарт-контрактів економія електроенергії досягає 10% [22].



Зображення створено за допомогою ШІ

Смартконтракти особливо корисні для побудови автоматизованого процесу виконання визначеної послідовності дій у наступних галузях:

- автоматизовані розрахунки та взаєморозрахунки (settlement) між багатьма учасниками;

- p2p-ринки (у тому числі енергетичні) з прозорими правилами;
- організація автоматизованого керування правами доступу та подіями (наприклад, видача/відкликання дозволів, фіксація фактів отримання послуг тощо);
- автоматизація управління ланцюгами постачання та обліком походження активів (traceability).

Разом з тим використання смарт-контрактів несе певні **ризики**, які необхідно враховувати при створенні автоматизованої системи. До таких ризиків належать, зокрема, **типові програмні помилки** (vulnerabilities), **логічні баги**, **непередбачені взаємодії між контрактами**, а також **атаки, зумовлені особливістю використання смарт-контрактів** у блокчейн. Оскільки виконання будь-якого смарт-контракту активується певною транзакцією, то атаки на виконання транзакцій, наприклад маніпуляція порядком виконання транзакцій, є потенційними атаками на смарт-контракти. Одна з найпоширеніших атак – атака випередження (frontrunning), яка має кілька варіантів виконання.

У роботі [4] запропоновано модель оцінки ймовірності успішності варіантів frontrunning-атаки (зокрема insertion/displacement) і показано залежність ризику від мережевих параметрів та співвідношення комісій за конкуруючі транзакції.

Для **забезпечення коректного та безпечного використання** смарт-контрактів можна сформулювати наступні **рекомендації**:

- **використовувати типові смарт-контракти**, які перевірені тривалим часом використання;
- **проводити незалежні аудити коду смарт-контракту** та моделі загроз, застосовувати стандартизовані підходи до тестування його роботи;
- **мінімізувати складність смарт-контрактів** і кількість зовнішніх входів-виходів;
- проєктувати механізми оновлення (upgrade) обережно і впроваджувати їх у реальні системи лише після всебічного тестування;
- для сценаріїв аукціонів/торгів і p2p-ринків враховувати ризики, спричинені відомими атаками, та виконувати рекомендації щодо захисту від таких атак.

Ведення державних та приватних реєстрів

Використання блокчейн-технологій для ведення державних та приватних реєстрів практично зводить до нуля імовірність успішних дій зловмисника спрямованих, на підміну інформації, яка була внесена до реєстру раніше. Наприклад, така структура повністю захищає від так званих «чорних нотаріусів» і рейдерства [12].

Завдяки захищеності, прозорості та швидкодії технологія блокчейн якнайкраще **підходить** для впровадження у **сфері державних реєстрів**, зважаючи на те, що:

- **немає єдиного місця зберігання**;
- **зміни вносяться відразу** до всіх примірників бази;
- **дані** (через певний час) після внесення вже **не можуть бути змінені**;
- **кожен користувач** у будь-який момент може **ознайомитися з усіма записами** та **побачити всю історію транзакцій** щодо внесення інформації.

Крім того, впровадження цієї технології дозволить забезпечити надійну синхронізацію даних, що унеможливить їх підміну у результаті зовнішнього втручання, гарантує прозорість, а також дасть можливість здійснювати суспільний контроль за системою.

Для практичної реалізації такого підходу пропонується використовувати [12]. Ця модель передбачає використання ієрархічної моделі блокчейнів, в якій на вершині ієрархії перебуває єдиний «головний» державний блокчейн. Йому, в свою чергу, підпорядковується мережа наявних державних реєстрів, які розташовані на окремих (можливо, частково приватних або частково керованих) блокчейнах та періодично роблять чекпоінти (контрольні точки) у «головному» блокчейні. При цьому «головний» блокчейн теж періодично робить чекпоінти, але вже в якомусь з відомих надійних незалежних блокчейнів, наприклад, у блокчейні Ефіріум або його сайдчейнах. Це означає, що періодично геш-значення блоків «головного» реєстру (наприклад, геш-значення кожного сотого блоку) записується у певний блок надійного незалежного децентралізованого блокчейну як спеціальна транзакція. Після створення такого чекпоінту вся історія блокчейн-реєстру вже не може бути змінена без виконання складної атаки на незалежний блокчейн, при чому, у разі успіху цієї атаки відбудеться втрата величезної кількості капіталу (наприклад, еквівалентної багатьом мільярдам доларів).

Слід також пам’ятати, що однією із основних проблем «криптовалютних» блокчейнів, з доведеною стійкістю та надійністю, є дуже низька швидкість обробки транзакції. Так, наприклад, у мережі BTC (Bitcoin) швидкість обробки становить 3–7 транзакцій за секунду, що у тисячі разів менше, ніж у банківських платіжних системах. Причина цього полягає у тому, що стійкість блокчейну до основних атак (наприклад, до атаки подвійної витрати та до атаки розгалуження) зменшується як при збільшенні розміру блоку, так і при збільшенні інтенсивності генерації блоків.

Така ж проблема буде виникати і при використанні блокчейна для обробки інформації. **Час очікування** до включення інформації у блокчейн, а потім до підтвердження стабільності блоку, до якого вона включена, **може тривати години і навіть кілька діб**. Така ситуація є неприпустимою, якщо інформація, що обробляється, є важливою та терміновою, наприклад, інформація про розповсюдження інфекційних хвороб у якійсь місцевості або про пожежі, паводки та інші серйозні загрози життю та здоров'ю великої кількості людей.

Тобто з одного боку, для **зберігання та обробки інформації** такого рівня важливості **потрібна надійна мережа**, яка захистить її від підробки та знищення, а, з іншого, така інформація повинна оброблятись та розповсюджуватись **практично миттєво** і мати надійний рівень захисту та підтвердження.

Проблема знаходження компромісу між надійністю зберігання інформації та швидкістю її обробки виникає і при створенні каскадного реєстру на блокчейнах. На поточний час існує багато робіт, спрямованих на розв'язання такої проблеми для криптовалютних блокчейнів. Оскільки для функціонування блокчейну не має значення, яку саме інформацію він зберігає, фінансову чи якусь іншу, розв'язання такої проблеми для криптовалютних блокчейнів автоматично розв'язало б її і для всіх інших.

З огляду на аналіз існуючих протоколів консенсусу у блокчейні, найбільш підходящим **рішенням** видається побудова каскадного реєстру саме на основі **ідеї, запропонованої у протоколі PoP**.

Проведення тендерів

Аналогічна схема забезпечує можливість проведення прозорих чесних тендерів, у яких ніхто (включаючи членів комісії) не може побачити інформацію аж до завершення подачі документів на конкурс, і, при цьому, конкурсанти після подачі не зможуть таємно змінювати свої пропозиції.

Неформально **процедуру проведення тендеру** з використанням блокчейну можна описати наступним чином:

1 етап – розміщення інформації про тендер. Тендерна комісія розміщує всю інформацію про тендер (терміни, вимоги, критерії оцінювання) у блокчейні.

2 етап – формування заявок. Етап відкривається після того, як пройшло достатньо часу для фіналізації блоку з тендерною інформацією.

Компанії, які бажають взяти участь у тендері, формують свої заявки у вигляді електронного документу, обчислюють його геш-значення і підписують його секретним ключем. При цьому,

сертифікати відкритих ключів кожної компанії мають бути у загальному доступі для виконання перевірки коректності підпису.

3 етап – прийняття геш-значень заявок.

Кожна компанія розміщує у блокчейні підписане геш-значення своєї заявки.

4 етап – розкриття повного тексту заявки.

Кожна компанія надає уповноваженим особам повний текст заявки. Якщо заявки не містять інформації з обмеженим доступом, їх можна просто викладати у блокчейні.

5 етап – перевірка коректності геш-значень та коректності підпису.

Уповноважені особи перевіряють коректність геш-значень та коректність підпису для кожної заявки, а також дотримання термінів надання геш-значення і самої заявки. Некоректні заявки відсіюються.

6 етап – безпосереднє оцінювання кожної заявки за заздалегідь відомими критеріями.

У результаті оцінювання заявок обираються переможці.

При реалізації вищенаведеної процедури, все, що відбувається на кожному етапі, є **прозорим та видимим** для всіх небайдужих, зокрема, для антикорупційних активістів. При дотриманні такої процедури проведення тендерів на їх результати неможливо несанкціоновано вплинути на жодному із етапів.

Обережність при використанні блокчейн-технологій

Слід наголосити, що на практиці всі зазначені використання блокчейн-технологій можливі лише за умови стійкості блокчейну до основних атак з боку зловмисника. На поточний час провідними науковцями світу активно досліджується напрям стійкості блокчейну. Наприклад, лише за 2023 рік у видавництві MDPI, яке випускає журнали 1 та 2 квартилю наукометричної бази Scopus, вийшло близько 30 окремих спеціальних випусків за цією темою, зокрема:

- Advancement in Blockchain Technology and Applications;
- Blockchain in Information Security and Privacy;
- Advances in Security and Blockchain Technologies;
- Emerging Networks and Blockchain Technology та інші.

Крім того, сотні статей опубліковані у журналах категорії «peer review» Mathematics, Censors та Cryptology, які дуже вимогливо ставляться до статей, представлених до публікації.

За цими фактами можна зробити висновки, що провідні науковці світу активно працюють у галузі блокчейну, особливу увагу приділяючи його стійкості до різних атак. Тому кожен випадок упровадження блокчейну, особливо у державному секторі, потребує залучення провідних науковців, що є спеціалістами у цій галузі, для проведення ряду досліджень стосовно його безпеки та ефективності.

Висновки

Блокчейн-технологія надає нові можливості у різних галузях (від фінансових сервісів до енергетики та державного управління) і має багато актуальних практичних застосувань. При цьому, криптовалюти є лише одним із можливих сценаріїв (і, часто, не найголовнішим) для державного сектору.

Реальна вигода від застосування блокчейну проявляється тоді, коли потрібно забезпечити наступні вимоги: **незмінність історії, відтворюваний аудит, автоматизацію виконання угод, зниження залежності від посередника** і, взагалі, від людського фактору. Для реєстрів і процедур, де довіра є необхідністю, таку вигоду складно переоцінити.

Побудова стійких до атак блокчейн-систем вимагає серйозних наукових та інженерних досліджень із залученням математиків і криптологів. Зокрема, **математичні моделі дозволяють кількісно оцінювати ризики атак** (double-spend, вплив затримок, ефект чекпоїнтів, ймовірність frontrunning) та обирати параметри системи [3–6].

Нарешті, для впровадження у державному секторі **доцільно застосовувати поетапний підхід**: чітка постановка задачі, формування вимог, вибір архітектури блокчейну та його параметрів, створення моделі загроз, кількісні оцінки ризиків, розробка формалізованих регламентів, апробація пілотних версій та незалежний аудит за результатами випробувань.

Перелік джерел посилання

1. Yaga D., Mell P., Roby N., Scarfone K. Blockchain Technology Overview. NISTIR 8202. National Institute of Standards and Technology; 2018. https://doi.org/10.6028/NIST.IR.8202.
2. IBM. What Is Blockchain? IBM Think (web resource). Available: https://www.ibm.com/think/topics/blockchain (accessed 23 Feb 2026).
3. Kovalchuk L., Kolomiiets A., Korchenko O., Rodinko M. Security Analysis of Double-Spend Attack in Blockchains with Checkpoints for Resilient Decentralized Energy Systems in Smart Regions. Sustainability. 2026;18(3):1673. https://doi.org/10.3390/su18031673.
4. Kovalchuk L.V., Vykhlo A.A. Estimation of the Probability of Success of a Frontrunning Attack on Smart Contracts. Cybernetics and Systems Analysis. 2024; №60, p. 881–890. https://doi.org/10.1007/s10559-024-00725-z.

5. Kovalchuk L., Kostanda V., Marukhnenko O., Pozhylenkov O. Achieving Security in Proof-of-Proof Protocol with Non-Zero Synchronization Time. Mathematics. 2022; №10(14), 2422. https://doi.org/10.3390/math10142422.
6. Kovalchuk L., Rodinko M., Oliynykov R., Kaidalov D., Nastenko A. Probability of Double Spend Attack for Network with Non-Zero Time Delay. Publicationes Mathematicae Debrecen Supplementum. 2022; №100, p. 597–615. https://doi.org/10.5486/PMD.2022.Suppl.4.
7. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available: https://bitcoin.org/bitcoin.pdf (accessed 23 Feb 2026).
8. Saleh F. Blockchain without Waste: Proof-of-Stake. Review of Financial Studies. 2021; №34(3), pp. 1156–1190. https://doi.org/10.1093/rfs/hhaa075.
9. ISO. ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary. International Organization for Standardization; 2024. Available: https://www.iso.org/standard/82208.html (accessed 23 Feb 2026).
10. Charalambous M., Damvakeraki T. Blockchain for Beginners: Basic Guiding Principles. EU Blockchain Observatory and Forum; April 2024. Available: https://blockchain-observatory.ec.europa.eu/document/download/1063effa-59cc-4df4-aeee-d2cf94f69178_en?_filename=Blockchain_For_Beginners_A_EUBOF_Guide.pdf (accessed 23 Feb 2026).
11. Back A. Hashcash — A Denial of Service Counter-Measure. Hashcash.org. URL: http://hashcash.org/papers/hashcash.pdf (дата звернення: 26.03.2023).
12. М.С. Кондратенко. Використання технології блокчейну при побудові ієрархічної структури на множині державних реєстрів для захисту від підробки інформації // Електрон. моделювання. 2023. Т. 45. № 3, стор. 43-56, ISSN 0204–3572. https://doi.org/10.15407/emodel.45.03.043.
13. Sompolinsky Y., Zohar A. Accelerating bitcoin's transaction processing: fast money grows on trees, not chains. IACR Cryptology ePrint Archive, 2013/881. https://eprint.iacr.org/2013/881.
14. Sompolinsky Y., Lewenberg Y., Zohar A. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. IACR Cryptology ePrint Archive 2016/1159.
15. Sompolinsky Y., Zohar A. Phantom. IACR Cryptology ePrint Archive, Report 2018/104. https://eprint.iacr.org/2018/104.pdf.
16. Fitzi M., Gazi P., Kiayias A., Russell A. Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition. Cryptology ePrint Archive, Report 2018/1119. https://eprint.iacr.org/2018/1119.
17. Pass R., Shi E. FruitChains: A fair blockchain. 36th ACMPODC, p.315–324. ACM, July 2017.
18. Garoffolo A., Kaidalov D., Oliynykov R. Zendoo: a zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains. IEEE. Institute of Electrical and Electronic Engineers. https://ieeexplore.ieee.org/document/9355752.
19. Grunspan C., Pérez-Marco R. Double spend races. CoRR abs/1702.02867 (2017). http://arxiv.org/abs/1702.02867.
20. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform (Ethereum White Paper). 2014. Available: https://ethereum.org/en/whitepaper/ (accessed 23 Feb 2026).
21. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper). 2014. Available: https://ethereum.github.io/yellowpaper/paper.pdf (accessed 23 Feb 2026).
22. Neves, D.; Scott, I.; Silva, C.A. Peer-to-peer energy trading potential: An assessment for the residential sector under different technology and tariff availabilities. Energy, 205 (2020), 118023. https://doi.org/10.1016/j.energy.2020.118023.

Принципи відновлення інформації на криптомодулях методами реверс-інжинірингу

канд. техн. наук, доцент Анатолій БОРОДА, ДержНДІ технологій кібербезпеки

> Реверс-інжиніринг

Отримана із мікрочипів інформація (реверс-інжиніринг) може використовуватися під час судової експертизи, для дослідження безпеки відповідних апаратних засобів та аналізу причини їх відмов, сертифікації цих засобів (наприклад, за вимогами Common Criteria), а також відновлення даних із пошкоджених апаратних носіїв для спеціальних використань.

Згідно із загальною моделлю реверс-інжинірингу, під час відновлення інформації із криптомодулів (мікрочипів) виконуються три **комплекси заходів**: аналіз захисних механізмів мікрочипу, відновлення логічної структури його будови та зчитування прошивки (витяг) певних даних з пам'яті мікрочипу.

Аналіз захисних механізмів здійснюється на фізичному рівні, шляхом вивчення структури кристалу мікрочипу. Метою є виявлення механізмів захисту мікрочипу від несанкціонованого доступу, розташування комірок з бітами захисту від читання пам'яті, зокрема, плавких вимикачів читання пам'яті.

Під час **відновлення логічної структури** проводиться аналіз мікроархітектури чипу на топологічному рівні, тобто встановлення областей розташування на чипі блоку процесора (якщо він є), блоків пам'яті, зовнішніх інтерфейсів, провідників та шин їх з'єднання, а також ідентифікація на схемах топології цих блоків структур, що відповідають певним логічним елементам, наприклад, «AND» («І»), «OR» («АБО»), «XOR» («ВИКЛЮЧНЕ АБО», «NAND» («І-НІ») та окремим транзисторам.

Процес **зчитування (витягу) даних** виконується на логічному рівні реверс-інжинірингу і полягає у вичитуванні вмісту з наявних блоків пам'яті типу Flash/EEPROM з метою пошуку у цих даних прошивок певних функцій (наприклад, криптографічних), ключів шифрування, параметрів конфігурації тощо.

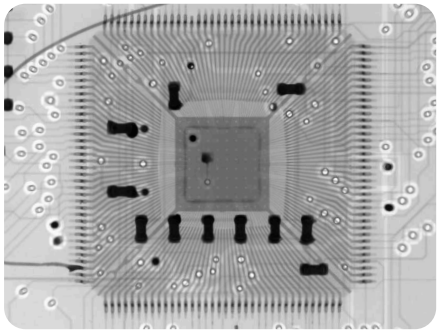
Неруйнівні методи реверс-інжинірингу

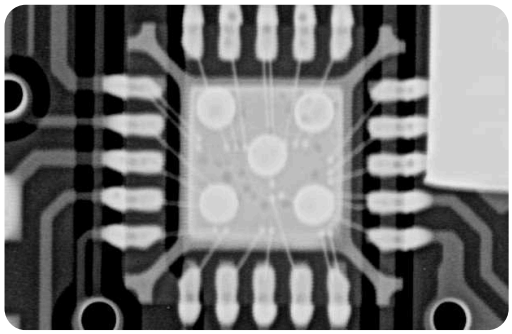
Прецизійна рентгеноскопія

Рентгеноскопія з високою роздільною здатністю дозволяє **виявити на мікрочипі різні за функціональністю блоки** (пам'яті, зовнішні інтерфейси тощо), розведення інтерфейсних шин та підпайку до зовнішніх контактів, знайти плавкі перемикачі,

виявити можливості підключення до інтерфейсних шин мікрочипу тощо [7].

Виявлення особливостей топології мікрочипу методом рентгеноскопії





Іноді секретні мікрочипи робляться навмисно без маркування. Виробники шифраторів часто видаляють маркування на мікросхемах (шліфувальною машинкою або лазерним гравером тощо). Тоді важко здогадатися про призначення мікрочипу, але **відновлення маркування можливе шляхом аналізу корпусу мікрочипу** за допомогою мікроскопа. Якщо це не допомагає, тоді ідентифікація мікрочипу також можлива за допомогою прецизійної рентгеноскопії, шляхом **порівняння схеми розпаювання мікрочипу з бібліотекою схем розпаювання відомих зразків.**

Аналіз електричних інтерфейсів

Більшість **мікросхем пам'яті є незахищеними.** Вони розроблялися без урахування вимог безпеки, тому прочитати їх вміст можна звичайним програматором [7].

Послідовні EEPROM можна зчитувати прямо з працюючого пристрою зазвичай через SPI або I2C інтерфейс, записуючи тактові імпульси і дані.

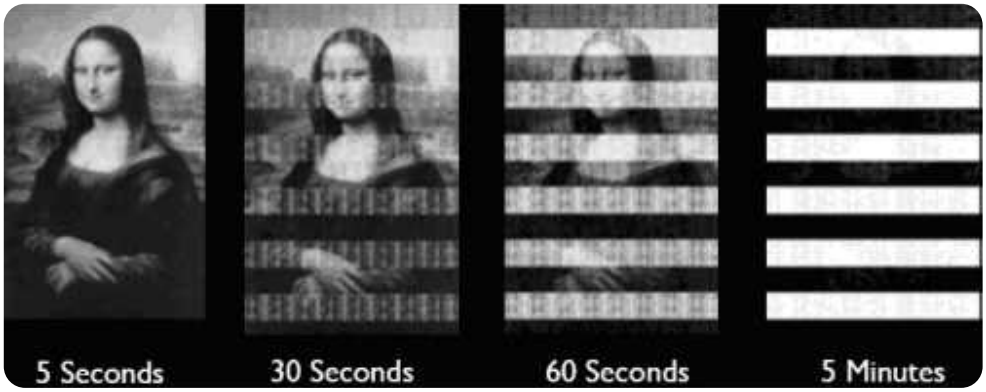
Логічні схеми, що програмуються, такі як FPGA на основі SRAM, є **уразливими до атак**, тому що вимагають завантаження конфігурації із зовнішньої пам'яті і цей потік бітів можна зареєструвати, щоб отримати зліпок конфігурації FPGA у завантажувальному форматі. Труднощі складає тільки випадок, коли потік бітів є зашифрованим.

Для визначення функціональних можливостей невеликих **одноразово програмованих логічних схем PLD застосовують атаку щодо сканування входів/виходів**, перебираючи всі можливі комбінації входів та записуючи значення отриманих виходів.

Незахищена **оперативна пам'ять типу RAM** та енергонезалежна пам'ять також **уразливі стосовно атак** щодо витягування їх вмісту, тому що сліди даних можуть існувати і вилучатись з такої пам'яті протягом деякого часу після відключення живлення [5] або форматування енергонезалежної пам'яті. Це

може бути використано для витягування коду програм, тимчасових даних, криптографічних ключів тощо.

Результати атаки «за холодним завантаженням» пам'яті типу RAM



Захищені мікросхеми пам'яті

Біти «захисту» пам'яті мікрочипів у включеному стані («1») дозволяють тільки «одноразовий запис» у захищену область пам'яті та запобігають завантаженню (виконанню) програмного коду, який може бути використаний для її повного читання. Такий захист у більшості випадків можна **обійти за допомогою цільової атаки на комірку з бітом «захисту»** [3], яка скидає біт «захисту», або атак з ініціювання електричних несправностей пам'яті, які дозволяють отримувати на шині даних значення певних комірок пам’яті, незважаючи на встановлений біт «захисту».

Аналіз зовнішніх інтерфейсів

Зазвичай ці інтерфейси призначені для комунікації між мікрочипом і зовнішнім світом, а саме: для зв'язку з периферійними пристроями (каналами зв'язку), для виробничих випробувань, програмування мікрочипу, оновлення/налагодження. Прикладами являються інтерфейси Ethernet, RS232, USB, Firewire, Smartcard, Serial, USB, JTAG, I2C, SPI тощо.

Доступний **зовнішній інтерфейс може стати «лазівкою» для криптоаналітичних атак**, наприклад, інтерфейси Smartcard, Serial, USB, JTAG, I2C, SPI, Ethernet і т.ін. Особливий інтерес становить робота з інтерфейсом для програмування/налагодження. Якщо його використовує виробник, то і нападник теж може його застосувати, наприклад, для «налагодження» ділянки прошивки мікрочипу, яка виконує криптографічні функції з використанням секретного ключа і, таким чином, витягнути секретний ключ. Загалом, будь-який **інтерфейс, до якого може підключатися третя сторона, може містити інформацію, яка корисна для атаки**, тому що створюються можливості для отримання даних, секретних параметрів тощо.

Засоби та способи аналізу інтерфейсів

Для **аналізу інтерфейсів застосовуються осцилограф, логічний аналізатор, спеціалізовані аналізатори (сніфери) протоколів** та багато інших програмних засобів. Застосовуючи мультиметр або осцилограф можна досліджувати і визначати

функціональне призначення ліній інтерфейсу. Спостереження логічних станів лінії може допомогти здогадатися про її призначення, а саме: шляхом подачі на контакти сигналів високого або низького рівня та аналізу отриманих результатів (у тому числі, їх повторюваності).

Для **моніторингу стандартних інтерфейсів**, звичайно, використовуються **спеціалізовані апаратні або програмні аналізатори** протоколів, такі як PortMon (для RS232 і паралельного порту), SnoopyPro або SourceUSB (для USB) та аналізатори шини даних, наприклад, Bus Pirate.

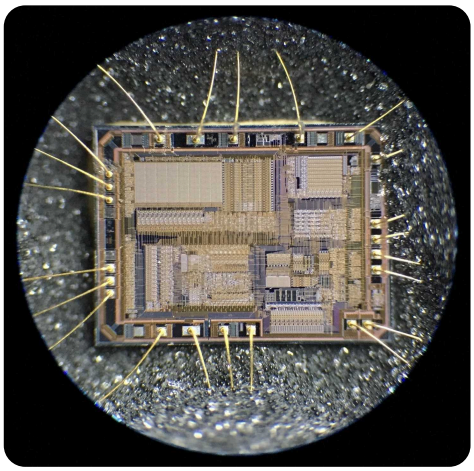
Напівруйнівні методи реверс-інжинірингу

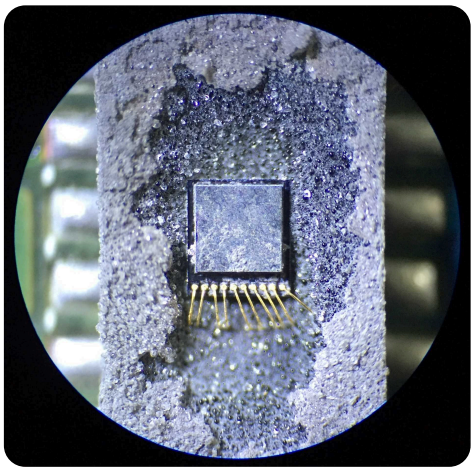
Застосовуються для аналізу мікрочипів з одношаровою топологією.

Декапсуляція корпусу мікрочипу

За допомогою спеціальної станції декапсуляції виконується «делікатна» декапсуляція верхньої частини корпусу мікрочипу. Використовуються хімічні, механічні методи (або обидва), а також лазерне і плазмове травлення. При видаленні зовнішнього матеріалу корпусу зберігається цілісність кристалу кремнію мікрочипу. Можливе застосування методів декапсуляції, що зберігають функціональність мікрочипу. За результатами роботи відкривається доступ до топології кристалу мікрочипу [2, 7].

Вигляд декапсульованих мікрочипів



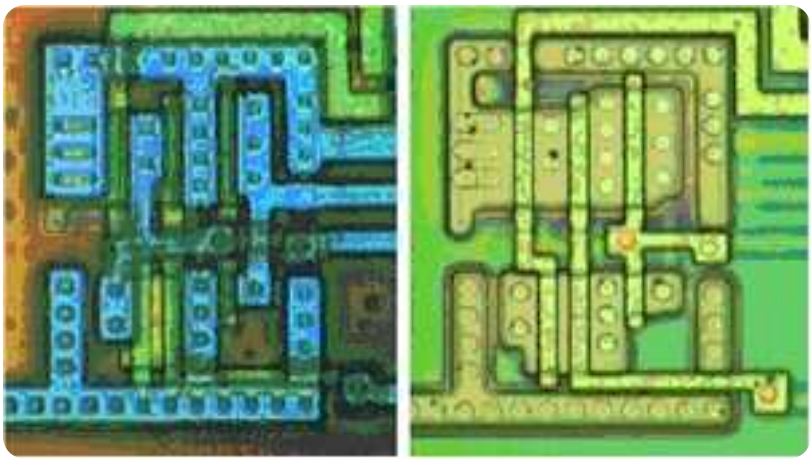


Оптична мікроскопія

Наступним кроком є створення **карти топології мікрочипу**. Використовується **оптичний мікроскоп** із ПЗС-камерою для створення декількох квадратних метрів мозаїки поверхні мікрочипу зі знімків високої роздільної здатності. Основні архітектурні структури, такі як шини даних і адреси, можуть бути швидко **ідентифіковані** шляхом вивчення **точок підключення і відстеження металевих ліній**, які перетинають чітко видимі межі модулів (ROM, RAM, EEPROM, ALU, декодер інструкцій тощо) [1, 7].

На рисунку нижче ліворуч наведено зображення логічного елемента AND у конфокальному мікроскопі (технологія CMOS), праворуч – цей же елемент після видалення металевого покриття за допомогою травлення плавиковою кислотою (з'єднання полікремнію і дифузійні зони тепер повністю відкриті).

Логічний елемент AND



Всі вузли обробки, як правило, підключені до основної шини за допомогою легко пізнаваних замків і драйверів шини. Але для їх розпізнавання необхідно добре знати методи проектування мікрочипів типу CMOS і архітектуру мікроконтролерів.

Оптичне вичитування пам'яті технології CMOS RAM

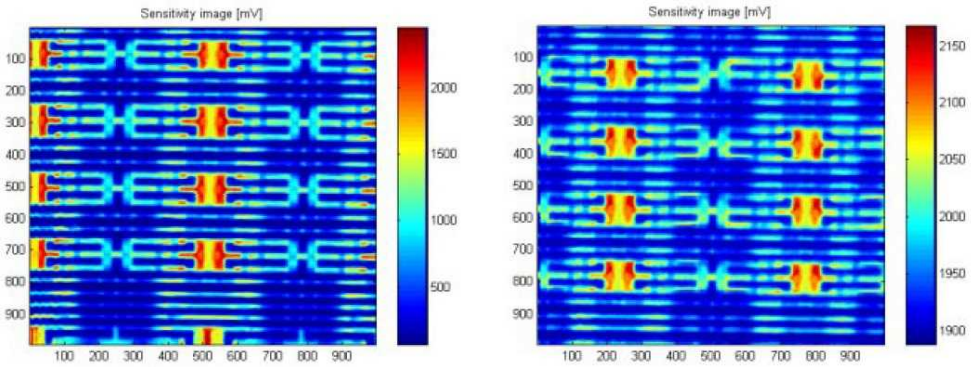
Для аналізу **структури пам'яті SRAM** використовується **червоний лазер**, сфокусований на поверхні чипу за допомогою мікроскопа. Оскільки фотони з червоного лазера (довжина хвилі 650 нм) мають енергію, більшу ніж **заборонений проміжок зони кремнію**, вони будуть **іонізувати активні області усередині** чипу. Якщо фотони досягають області біля **p-n** переходів, то буде продукуватися фотострум (через фотоелектричний ефект). Коли фотони потраплять в область **p-** або **n-**каналу, це зменшує опір каналу внаслідок введення вільних носіїв [6].

Прикладом застосування цієї методики є експеримент із побудови карти активних областей у мікроконтролері шляхом вимірювання фотоструму, індукованого лазерним скануванням поверхні чипу. Чип, на який не подане живлення, був встановлений на дослідницький стенд, який міг рухатися за координатами X-Y із роздільною здатністю 0,1 мкм. Результат сканування показано на рисунку ліворуч. Можна побачити активні області, оскільки вони виробляють більший струм. Але більша частина чипа покрита металевими шарами, крізь які лазерний промінь не може проникнути, тому ці ділянки не виробляють струму.

Наступний експеримент зроблений із чипом під напругою. Чип було запрограмовано таким чином, щоб завантажувати будь-які значення у його оперативну пам'ять, а потім зупиняти роботу

чипу.

Лазерне сканування пам'яті без подавання живлення (ліворуч) та сканування під напругою (праворуч)



Результат сканування комірок пам'яті, що завантажені випадковими даними, показаний на рисунку праворуч. Видно, що комірки пам'яті мають різні стани: там, де в комірці є "1", верхня частина яскравіша, а де "0" – має меншу інтенсивність.

Таким чином, встановлено, що шістнадцять біт, які розташовані у відсканованих комірках, мають, наведені нижче значення:

1	1	0	0
1	1	1	0
1	1	1	1
1	1	1	1

Сканувальна електронна мікроскопія

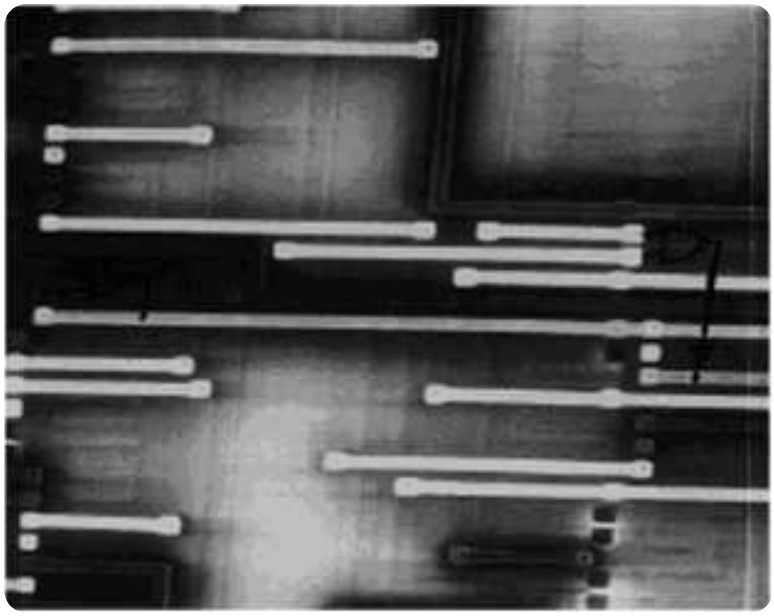
Перспективним напрямом реалізації напівагресивних методів реверс-інжинірингу є застосування електронно-променевих тестерів (Electron Beam Prober – EBP) [2, 7].

> **Електронно-променевий тестер** – це сканувальний електронний мікроскоп (SEM) з **функцією контролю контрастності електронного променя** (сигналу тестування).

Типові напруги прискорення і струми пучка для первинних електронів складають 2.5 kV та 5 nA відповідно. Число і енергія вторинних електронів є індикацією локального електричного поля на поверхні чипу, що дозволяє спостерігати сигнальні лінії (шини) з субмікронною роздільною здатністю. Сигнал, що генерується під час тестування електронним променем, по суті, являє собою результат низькочастотної фільтрації струму пучка, помножений на функцію напруги сигналу у лінії плюс шум. EBT можуть вимірювати зразки сигналів з пропускною здатністю кілька ГГц, але тільки періодичних сигналів, де

можуть бути використані стробоскопічні методи і періодичне усереднення. Якщо використовувати контрастний режим у реальному часі, де промінь безперервно спрямовується в одну точку і записується сигнал від реєстрації зашумленого потоку вторинних електронів, то ширина смуги частот сигналу обмежується декількома МГц. Хоча така пропускна здатність може бути просто достатньою для спостереження за однією сигнальною лінією смарт-картки з тактовою частотою 3,5 МГц, вона занадто мала, щоб спостерігати всю шину з частотою дискретизації кілька МГц для кожної лінії.

Програмне забезпечення ЕВР обробляє вказаний сигнал і, таким чином, виявляє відхилення напруги на шинах чипу і відображає їх як зображення різної контрастності. За допомогою цієї технології також можливо вичитувати інформацію з комірок пам'яті типу Flash ROM.



Отримане на ЕВТ зображення проходження сигналів по послідовній шині чипу (на зображенні – найбільша за довжиною)

Електронно-променеві тестери дуже зручні інструменти аналізу, якщо тактова частота процесора, що аналізується, може бути зменшена нижче 100 кГц, щоб у масштабі реального часу записувати усі лінії шини або, якщо процесор може бути змушений генерувати періодичні сигнали, безперервно повторюючи ту ж саму операцію під час вимірювання.

Стандартний ЕВТ має такі режими роботи:

- **Стробоскопічний режим** з усередненням – призначений для вимірювання періодичного сигналу зі смугою до декількох ГГц.
- **Режим реального часу** – здатний вимірювати довільні сигнали зі смугою у декілька Мгц.
- **Одночасний контроль** всіх сигналів чипу – при зниженні тактування процесора чипу до 100 кГц.

Руйнівні методи реверс-інжинірингу

Руйнівні методи застосовуються, коли мікрочип має **багатошарову топологію**. Етап повного відновлення топології таких мікрочипів часто необхідний для досягнення мети аналізу. Сама процедура аналізу топології подібна відновленню схеми та аналізу функціональності багатошарової друкованої плати на дискретних компонентах, тільки на мікроскопічному рівні. Для виконання аналізу потрібні мінімум 3 екземпляри мікрочипу.

Мета реверс-інжинірингу:

- **витягування вмісту мікросхем пам’яті** типу Flash, ROM, пам'яті FPGA та інших енергонезалежних пристроїв для отримання програмних прошивок і криптографічних ключів, що на них зберігаються;
- **зміна або руйнування затворів і інших кремнієвих структур**, наприклад, виключення «біт» захисту, які запобігають читанню пам'яті;
- **розкриття функціональності чипів** у частині, що цікавить, наприклад, криптографічних алгоритмів.

Пошарове травлення кристалу мікрочипу

Реалізується за допомогою **станції декапсуляції** типу ASAP-1 System компанії Nippon Scientific, яка може виконувати оптичне вирівнювання лазером шляхом пошарового видалення із точним позиціонуванням зразка за висотою, нахилом та XY-переміщеннями. Може працювати у режимах механіко-хімічної декапсуляції, тунельної декапсуляції, точкової декапсуляції. Здатна проводити декапсуляцію багатошарових чипів [7].

У процесі роботи видаляється шар металізації, здійснюється фотографування топології з високою роздільною здатністю, видаляється наступний шар мікрочипу, знову фотографується і т.д. Потім зображення шарів топології мікрочипу вирівнюються та синхронізуються між собою з урахуванням перемикань між шарами і формується 3D-модель електричної схеми мікрочипа. Далі продовжується робота з мікрочипом за допомогою станції зондування.

Зондування даних мікрочипа

Типова **ручна станція зондування** включає технологічний мікроскоп з полем зору порядку 1мм×1мм, встановлений на антивібраційній платформі, на якій змонтовані мікроманіпулятори для переміщення зондів. Зонди підключаються до ПК за допомогою спеціального інтерфейсу формування сигналів вводу-виводу [4, 7].

З мікроскопом сполучені лазер для свердління маленьких отворів у пасивації чипу і фотоапарат та/або цифрова камера,

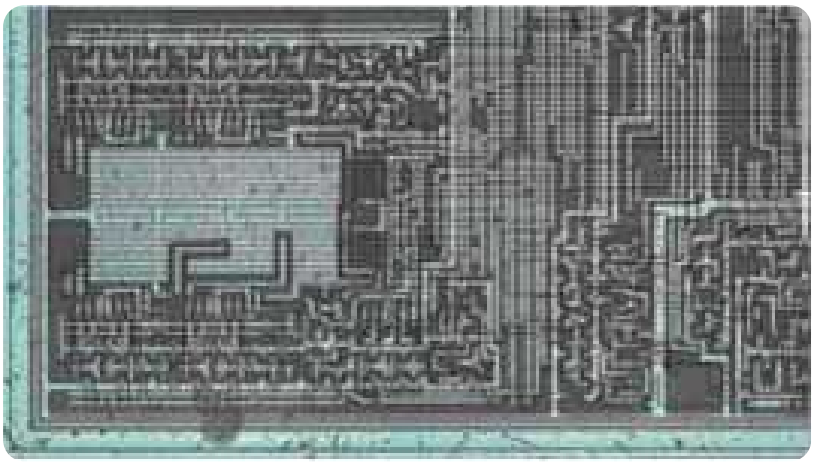
підключений до ПК.

За допомогою подібної станції зондування можливо **вивчення структури чипу по фотографіях**, реверс-інжиніринг **функціональності елементів топології чипу** (встановлення їх призначення на основі порівняння із зображеннями зразків бібліотеки топологічних елементів), **зондування шин даних і адреси чипу, управління регістром тактування команд** тощо.

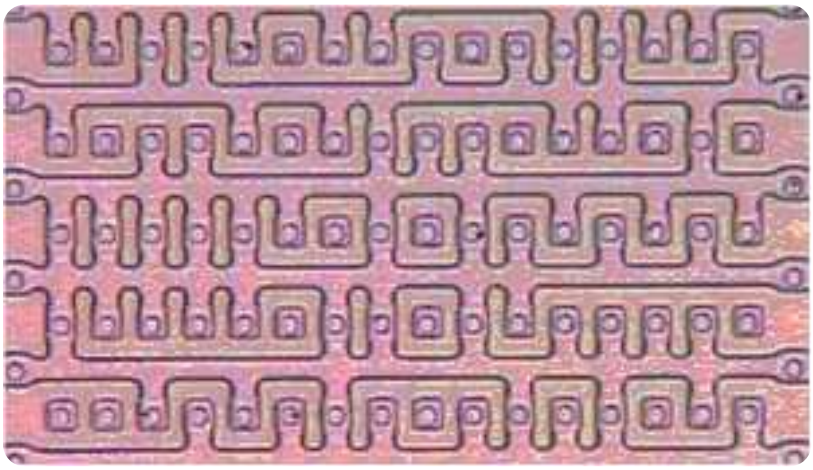
Застосування сканувального електронного мікроскопа

Використовується для проведення субмікронного аналізу топології чипу. Здатний видаляти металеві або інші шари матеріалу для доступу до елементів топології. Можливе візуальне відновлення вмісту пам'яті, у залежності від його розміру та типу [7].

Топологія чипу



Вміст пам'яті чипу



Отримані під мікроскопом зображення чипу можуть використовуватися для визначення виробника та/або ідентифікації технології виготовлення з метою його розкриття чи порівняльного аналізу, визначення напрямів реверс-інжинірингу функціональності чипу.

Застосування фокусного іонного мікроскопа

Іонний мікроскоп складається з вакуумної камери з іонною гарматою [2, 7]. Іони галію емітуються із рідкого металевого

катода, прискорюються і фокусуються за допомогою напруги 30 кВ у пучок менше 5-10 nm діаметром, при струмі пучка у межах від 1 pA до 10 nA. За допомогою **вторинних іонів** мікроскоп може отримувати зображення зразка з роздільною здатністю до 5 nm. При збільшенні струму пучка, матеріал чипу може видалятися із такою ж роздільною здатністю при продуктивності близько 0.25 $\mu m^3\ nA^{-1}\ s^{-1}$.

Кращі **швидкості** травлення можуть бути досягнуті шляхом **ін'єкції газу**, такого як йод, через голку до зони у межах декількох сотень мікрон від плями променя (місця засвітки). Молекули газу розташовуються на поверхні чипу і вступають у реакцію з матеріалом, що видаляється, з утворенням **летючих сполук**, які можуть бути **відкачані** і не відкладаються назад.

За допомогою цієї техніки травлення (із використанням газу) можуть бути створені під довільними кутами отвори, глибина яких до 12 разів більше ширини, щоб отримати доступ до глибоких шарів металу без пошкодження прилеглих структур. Вводячи до зони падіння пучка металоорганічний газ на основі платини, який розщеплюється на поверхні чипу за допомогою іонного пучка, можна осаджувати платину для утворення **нових контактів**. За допомогою іншої газової хімії, можуть бути утворені навіть **ізолятори**, щоб встановити контакти з поверхні з глибокими металевими шарами без контакту з будь-якими покриваючими шарами.

У режимі лазерного інтерферометра оператор мікроскопа може переміщати іонний пучок по поверхні чипу з точністю 0.15 mm, навіть якщо чип був вирівняний і не має впізнаваних поверхневих структур.

Чип також може бути **відполірований із зворотного боку** до товщини всього у кілька десятків мікрометрів.

Використовуючи режим **навігації з лазерним інтерферометром** або з інфрачервоним лазерним зображенням, можна знаходити **окремі транзистори** і зв'язуватися з ними через кремнієву підкладку за допомогою створення відповідних отворів.

Ця технологія заднього доступу здатна працювати і з новими захищеними мікрочипами.

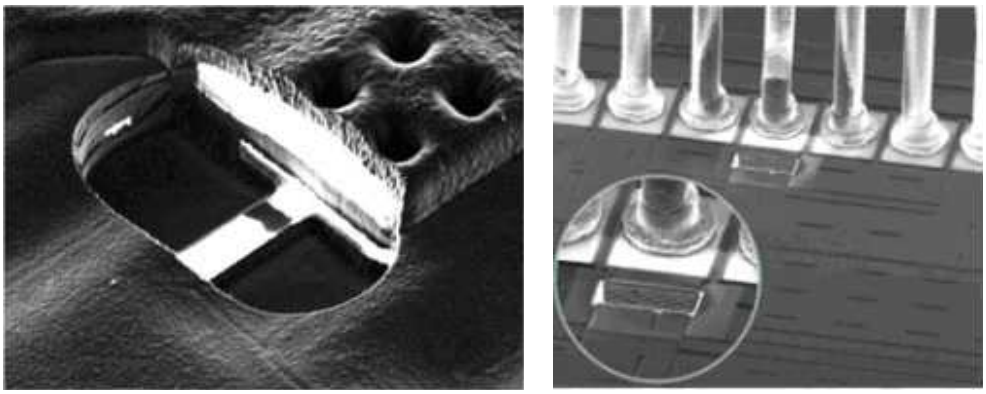
Основні режими роботи мікроскопа:

- **різка** (наприклад, відрізання контактної площадки або перетинання металевої доріжки на кристалі чипу);
- **осадження металізації** (наприклад, додавання з'єднання, повторне підключення доріжки на кристалі);
- **формування зображення** (отримується зображення топології

чипу з високою роздільною здатністю – до 5 nm). Поверхня чипу сканується пучком іонів малої інтенсивності, який вибиває з чипу вторинні іони, які скеровуються на мас-спектрометр. За його допомогою вторинні іони різної маси відображаються різними кольорами);

- **навігація по чипу** (за допомогою режиму лазерного інтерферометра обирається точка падіння на чип пучка іонів з точністю до 0.15 μm);
- **аналіз** (отримання елементного складу матеріалу у точці фокусу пучка іонів. Пучок іонів малої інтенсивності вибиває з чипу вторинні іони, які скеровуються на мас-спектрометр, за допомогою якого здійснюється прив'язка мас вторинних іонів до відповідних хімічних елементів).

Застосування фокусного іонного мікроскопа дозволяє подолати практично будь-який технологічний захист, за винятком стирання секретних ключів. За його допомогою можлива організація потрібних електричних контактів, а також свердління до потрібних компонентів отворів і створення (напилення) контактів на майданчики розпаювання. Тобто подолання захисту стає лише справою часу та витрачених коштів.



Отвори у кристалі чипу (ліворуч) та контактної площадки (праворуч), отриманих за допомогою мікроскопу

Висновки

Узагальнений алгоритм відновлення інформації на мікрочипах складається із наступних 8-ми кроків: **визначення типу пам'яті** мікрочипу, спроба **логічного доступу до інформації** за допомогою наявних інтерфейсів, **неруйнівна діагностика**, **декапсуляція** (за необхідністю), **аналіз кристалу мікрочипу**, **реконструкція структури топології, витяг (вичитування) даних, верифікація даних**.

Перелік джерел посилання

1. C. Ajluni, Two New Imaging Techniques Promise To Improve IC Defect Identification, Electronic Design, Vol. 43(14), July 1995, pp. 37-38.

2. R. Anderson, M. Kuhn, Tamper Resistance – A Cautionary Note, 2nd USENIX Workshop on Electronic Commerce, Nov 1996, pp 1-11, ISBN 1-880446-83-9.
3. R. Anderson, M. Kuhn, Low Cost Attacks on Tamper Resistant Devices, in Security Protocols (Proceedings of the 5th International Workshop (1997) Springer LNCS vol 1361 pp 125–136.
4. S. Skorobogatov, R. Anderson, Optical Fault Induction Attacks, Cryptographic Hardware and Embedded Systems Workshop, CHES 2002, Springer LNCS 2523, pp. 2-12.
5. SP Skorobogatov, Low temperature data remanence in static RAM, Technical report UCAM-CL-TR-536, university of Cambridge Computer Laboratory, June 2002.
6. David Samyde, Sergei Skorobogatov, Ross Anderson and Jean-Jacques Quisquater. On a New Way to Read Data from Memory. First International IEEE Security in Storage Workshop, 2002. Proceedings, pp 65–70.
7. Атаки на криптосистеми за побічними каналами: монографія / А.В. Борода, С.О. Клімович, В.В. Кузовков, В.О. Хорошко, Ю.Є. Хохлачова, М.Є. Шелест. – Київ: ФОП Ямчинський О.В., 2024. – 109 с.

Шляхи запобігання «квантовому апокаліпсису»

Михайло ТЕРЛЕЦЬКИЙ, ДержНДІ технологій кібербезпеки

Згідно з документом «**Меморандум про національну безпеку з просування лідерства США у галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем**» (National Security Memorandum on Promotion United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems) створення **криптоаналітично значущого квантового комп'ютера** (КЗКК) (Cryptanalytically Relevant Quantum Computer, CRQC) пов'язано зі значними ризиками для сучасної криптографії з відкритим ключем в усьому світі і може привести до так званого «**квантового апокаліпсису**».

> Ризики

У Меморандумі наголошено, що КЗКК «**буде здатний зламати більшу частину криптографії з відкритим ключем**, що використовується у цифрових системах США та усього світу. Коли він стане доступним, КЗКК може **поставити під загрозу цивільні та військові комунікації, підірвати системи нагляду та контролю за критичною інфраструктурою**, а також **зруйнувати протоколи безпеки для більшості фінансових операцій в Інтернеті**». «**Будь-яка цифрова система, яка використовує наявні публічні стандарти криптографії з відкритим ключем або планує перехід на таку криптографію, може бути вразливою для атаки КЗКК**».

> Квантовий комп'ютер

Квантовий комп'ютер (КК) – це обчислювальний пристрій, в якому для виконання операцій використовуються особливості квантової механіки. КК відрізняються від класичних комп'ютерів тим, що замість бітів (одиниць інформації, які можуть набувати двох значень – 0 або 1) вони оперують кубітами (квантовими бітами, які можуть знаходитись в суперпозиції двох станів одночасно).

Саме завдяки **суперпозиції** досягається так званий **квантовий паралелізм**, який дозволяє вирішувати ряд надзвичайно складних обчислювальних задач набагато швидше ніж на класичних комп'ютерах.

КЗКК – це потужний КК з достатньо великою кількістю кубітів, великим терміном перебування кубітів у стабільному стані та низькою ймовірністю помилки виконання квантових операцій, який може бути використаний на практиці для зламування реальних криптосистем.

Інтерес криптографічної спільноти до квантової обчислювальної техніки був ініційований роботами Шора та Гровера. Зокрема, у 1994 році американський математик П. Шор опублікував статтю, в якій описав квантовий алгоритм факторизації чисел з поліноміальною складністю [1], а у 1996 році Л. Гровером був розроблений субекспоненційний квантовий алгоритм швидкого пошуку у неупорядкованій базі даних [2]. Саме ці квантові алгоритми створюють загрозу сучасним криптографічним системам у випадку створення КЗКК.

Квантовий алгоритм Гровера може бути застосований при пошуку **секретного ключа** для будь-якого симетричного криптографічного алгоритму, однак складність алгоритму пошуку є **субекспоненційною**, отже, цей алгоритм несе **реальну загрозу тільки криптоалгоритмам з невеликою довжиною ключа**. Зокрема, у випадку застосування ключа **довжиною 256 бітів і більше** КЗКК, незалежно від кількості кубітів, **не зможе зламати криптосистеми з симетричним розподілом ключів**.

Зовсім інша ситуація з квантовим алгоритмом Шора, який **складає реальну загрозу майже всім наявним криптосистемам з асиметричним розподілом ключів**. Цей алгоритм може бути застосований для факторизації цілих чисел та дискретного логарифмування за поліноміальний час. А це означає, що у випадку створення КЗКК будуть зламані всі криптосистеми, які засновані на алгоритмах RSA, DH, ECDH, DSA, ECDSA, ECES, ДСТУ 4145-2002 тощо.

Саме такі алгоритми використовуються для надання кваліфікованих електронних довірчих послуг в Україні (у тому числі, в ID-картках, засобах кваліфікованого електронного підпису та печатки, на порталі «ДІЯ», сервісі «BankID» тощо). Наприклад, в ID-картках на базі чипа SLE78CLFX4000P використовуються алгоритми цифрового підпису ДСТУ 4145-2002 та ECDSA з ключами довжиною 191 та 256 біт відповідно.

Відносно квантового алгоритму Шора стійкість алгоритму ДСТУ 4145-2002 з довжиною ключа 191 біт оцінюється величиною $2.5 \cdot 10^9$ операцій квантового комп'ютера (квантових гейтів) при кількості кубітів 1378, а стійкість алгоритму ECDSA з довжиною ключа 256 бітів – величиною $6 \cdot 10^9$ квантових гейтів при кількості кубітів 1834.

Слід зазначити, що, наразі, **інфраструктура відкритих ключів** в Україні побудована **на трьох алгоритмах електронного цифрового підпису: ДСТУ 4145-2002, ECDSA** та **RSA**. Для зламу алгоритму ДСТУ 4145-2002 з максимальною довжиною ключа 509 біт знадобиться КК з 3609 кубітами, для зламу алгоритму

ECDSA з максимальною довжиною ключа 521 біт знадобиться КК з 3693 кубітами, а для зламу алгоритму RSA з довжиною ключа 4096 бітів знадобиться КК з 8192 кубітами. На сьогоднішній день КК з такою кількістю кубітів не існує, однак, **у випадку певного технологічного прориву, ситуація може змінитись і злам цих алгоритмів стане реальністю.**

Активні дослідження у галузі квантових технологій ведуть десятки країн, зокрема, США, Китай, Японія, росія, Канада тощо. У «перегонах» щодо створення потужних КК змагаються такі технологічні гіганти як Google, IBM, Microsoft, Apple, Amazon, Intel тощо.

Зростає кількість патентів у сфері квантових технологій. Станом на кінець 2023 року у Китаї зареєстровано 2700 патентів, у США – 2200, а в Японії – 885.

Спрогнозувати темпи розвитку квантових обчислювальних систем досить важко, але, за оцінкою фахівців, імовірність створення КЗКК з декількома тисячами кубітів **у найближчі 10 років є досить високою**. Саме тому у Меморандумі був визначений 2035 рік як граничний рік переходу США на постквантові криптографічні алгоритми та протоколи.

Одним із **методів нівелювання загрози появи КЗКК є використання квантового розподілу ключів** (КРК). Першим протоколом КРК є протокол ВВ84, який був розроблений Ч. Беннетом та Ж. Брассаром ще у 1984 році [3].

У системах з КРК ключові дані симетричного криптографічного алгоритму записуються у квантовий стан окремих фотонів і пересилаються оптичними каналами зв'язку. **Стійкість систем з КРК** заснована на **принципі невизначеності Гейзенберга, згідно з яким при спробі вимірювання стану фотону інформація знищується.**

Системи з КРК активно впроваджуються у світі, однак, їх **застосування обмежено необхідністю використання спеціального обладнання та оптоволоконних каналів зв'язку.**

Іншим дієвим методом нівелювання загрози появи КЗКК, який не має технічних обмежень, є **використання нових постквантових (post-quantum) криптографічних алгоритмів та протоколів, проти яких не може бути використаний квантовий алгоритм Шора**. Такі алгоритми і протоколи залишаться стійкими у постквантовому періоді (періоді після створення КЗКК) за умови, що для них не буде розроблений квантовий алгоритм криптоаналізу з поліноміальною складністю.

На сьогоднішній день розроблені десятки асиметричних

постквантових криптографічних алгоритмів та протоколів, зокрема:

- ML-KEM (FIPS 203);
- ML-DSA (FIPS 204);
- SLH-DSA (FIPS 205);
- FALCON (FIPS 206);
- LWE, SIDH, NTRU (ДСТУ ETSI TR 103 570:2022);
- CRYSTALS-Dilithium, FALCON, Rainbow (ДСТУ ETSI TR 103 616:2022);
- CRYSTALS-Kyber, ClassicMcEllice, SABER (ДСТУ ETSI TR 103 823:2022);
- «СКЕЛЯ» (ДСТУ 8961-2019);
- «ВЕРШИНА» (ДСТУ 9212-2023).

Усі ці алгоритми засновані на **математичних проблемах, для яких не існує ефективних алгоритмів квантового криптоаналізу**.

Існує декілька **типів квантово-стійких (quantum-safe) алгоритмів**, які можуть бути використані для розробки криптографічних систем, стійких до атак з використанням квантових обчислень, а саме:

- **криптографія на основі решіток** (lattice-based cryptography);
- **мультиваріативна криптографія** (multivariate cryptography);
- **криптографія на основі геш-функцій** (hash-based cryptography);
- **криптографія на основі кодів коригування помилок** (code-based cryptography);
- **криптографія на основі ізогенії еліптичних кривих** (isogeny-based cryptography).

У якості прикладів алгоритмів різних типів можна навести:

- lattice-based cryptography – «СКЕЛЯ», «ВЕРШИНА», ML-KEM, ML-DSA, CRYSTALS-Kyber, CRYSTALS-Dilithium, NTRU, SABER, FrodoKEM, FALCON.
- multivariate cryptography – Rainbow, GeMSS;
- hash-based cryptography – SLH-DSA, SPHINCS+;
- code-based cryptography – ClassicMcEllice, BIKE, HQC;
- isogeny-based cryptography – SIDH.

> Висновки

Ризики створення у найближчій перспективі КЗКК диктують нагальну **необхідність упровадження** у криптографічні системи, що використовуються в інформаційних та комунікаційних системах держави, **нових асиметричних постквантових криптографічних алгоритмів та протоколів, які є стійкими відносно методів квантового криптоаналізу**.

Перелік джерел посилання

1. Shor P. W., Polynomial-time algorithms for prime factorization and discretelogarithms on a quantum computer // Proceedings of the 35th Annual Symposiumon the Foundations of Computer Science, S. Goldwasser ed., IEEE Computer Society Press, Los Alamitos CA, 1994.
2. Grover's Quantum Search Algorithm [Електронний ресурс] – Режим доступу: https://web.archive.org/web/20201117095032/http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm.
3. Bennet C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of International Conference on Computers, Systems & Signal Processing, Dec 9-12, 1984, Bangalore, India. – IEEE, 1984. – P.175.
4. Post-Quantum Cryptography Project – Selected Algorithms 2022 [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/selected-algorithms.
5. FIPS 203 «Module-Lattice-Based Key-Encapsulation Mechanism Standard».
6. FIPS 204 «Module-Lattice-Based Digital Signature Standard».
7. FIPS 205 «Stateless Hash-Based Digital Signature Standard».
8. FIPS 206 «Falcon-based Digital Signature Algorithm».
9. ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм асиметричного шифрування та інкапсуляції ключів».
10. ДСТУ 9212:2023 «Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами».
11. ДСТУ ETSI TR 103 570:2022 «Кібербезпека. Квантово-безпечний обмін ключами».
12. ДСТУ ETSI TR 103 616:2022 «Кібербезпека. Квантово-безпечні підписи».
13. ДСТУ ETSI TR 103 823:2022 «Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів».

Щодо криптографічної стійкості криптоалгоритмів та криптопротоколів, які використовуються в Україні

Михайло ТЕРЛЕЦЬКИЙ, ДержНДІ технологій кібербезпеки

Загальний перелік криптографічних алгоритмів і протоколів, дозволених для реалізації у засобах криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, наведений у наказі Адміністрації Держспецзв'язку від 27.10.2020 № 687 [1]. До складу цього переліку включені: **блокові шифри, потокові шифри, асиметричні криптографічні алгоритми та протоколи, функції гешування, коди автентифікації повідомлень, алгоритми генерації псевдовипадкових чисел, протоколи узгодження ключів** тощо.

Криптоалгоритми та криптопротоколи відносяться до різних типів та побудовані на різних алгебраїчних структурах і використовують різні математичні перетворення.

Зокрема, використання перетворень у алгоритмах:

- **цифрового підпису ДСТУ 4145-2002** [2] – у групі точок еліптичних кривих (ЕК) у формі Монтгомері над скінченними полями Галуа характеристики 2;
- **ДСТУ 9041:2020** [3] – у групі точок скручених ЕК у формі Едвардса над простими полями Галуа;
- **ДСТУ 8961:2019** [4] – у кільці усічених поліномів над кільцем цілих чисел;
- **RSA** – у кільці цілих чисел.

При цьому, алгоритми AES, TDEA та «Калина» відносяться до блокових симетричних шифрів, алгоритми «Струмок» та SNOW 2.0 – до потокових симетричних шифрів, алгоритми RSA та ECDSA – до асиметричних алгоритмів цифрового підпису.

Саме тому при визначенні криптографічної стійкості алгоритмів та протоколів використовуються різні математичні підходи та результати.

Симетричні криптографічні алгоритми проєктуються таким чином, щоб **для них були відсутні методи криптоаналізу**, обчислювальна складність яких є меншою за алгоритм тотального перебору ключів, складність якого дорівнює $O(2^n)$ операцій, де n – довжина ключа в бітах.

Щодо квантового криптоаналізу, на сьогоднішній день для

пошуку секретного ключа симетричних криптографічних алгоритмів можливо використати тільки **субекспоненційний квантовий алгоритм Гровера**, складність якого оцінюється величиною $O(2^{n/2})$ операцій (квантових гейтів) на квантовому комп'ютері з n кубітами [5, 6].

Слід зазначити, що для **алгоритму Гровера** математично доведено, що ця кількість квантових гейтів не може бути зменшена навіть при використанні більшої кількості кубітів.

Типовими довжинами ключів сучасних симетричних криптографічних алгоритмів є **80, 128, 192, 256, 384, 512 бітів**. Для таких довжин маємо показники криптографічної стійкості симетричних криптографічних алгоритмів, які наведені у таблиці.

Довжина ключа, біт	Оцінка стійкості для класичного криптоаналізу, ~O (кількість операцій)	Оцінка стійкості для квантового криптоаналізу, ~O (кількість квантових гейтів, кількість кубітів)
64	10^{19}	10^{9}, 64
80	10^{24}	10^{12}, 80
128	10^{39}	10^{19}, 128
192	10^{58}	10^{29}, 192
256	10^{77}	10^{38}, 256
384	10^{115}	10^{58}, 384
512	10^{154}	10^{77}, 512

> Примітка

У наведеній таблиці і наступних таблицях вказано:

- значення кількості операцій за правилами математики, яке округлене до десятків;
- кількість «робочих» кубітів, які безпосередньо використовуються в алгоритмі (без врахування кубітів для корекції помилок).

Для **асиметричних криптографічних алгоритмів**, які побудовані на операціях у групі точок ЕК, **найкращим неквантовим алгоритмом дискретного логарифмування** є **алгоритм Поларда**, складність якого оцінюється величиною $O(\sqrt{n})$ операцій, де n – порядок базової точки еліптичної кривої [7].

Оцінка порядку базової точки ЕК **за теоремою Хассе** обчислюється за формулою

$$n \geq \frac{q + 1 - 2\sqrt{q}}{k},$$

де $q=2^m$, m – степінь поля, k – кофактор ЕК.

Для оцінки криптографічної стійкості можливо використовувати асимптотичну рівність n~q.

Для дискретного логарифмування у групі точок ЕК можливо використати **квантовий алгоритм Шора**, який має поліноміальну складність $O(360t^3)$ операцій квантового комп'ютера з $O(7t+4\log_2 t+10)$ кубітами, де t = m для скінчених полів $GF(2^m)$, $t=\log_2 p$ для скінчених полів GF(p) [8].

Для **еліптичних алгоритмів** у відповідних стандартах (описах) визначені **рекомендовані ЕК** у наступних полях:

- ДСТУ 4145-2002 у поліноміальному базисі – 163, 167, 173, 179, 191, 233, 257, 307, 367, 431;
- ECDSA для GF(p) – 192, 224, 256, 384, 521;
- ECDSA для $GF(2^m)$ – 163, 233, 283, 409, 521;
- ДСТУ 9041:2020 – 256, 384, 512, 768.

Показники оцінки криптографічної стійкості асиметричних еліптичних алгоритмів, які наведені у таблиці нижче.

Розмір порядку базової точки ЕК, біт	Оцінка стійкості для класичного криптоаналізу, ~O (кількість операцій)	Оцінка стійкості для квантового криптоаналізу, ~O (кількість квантових гейтів, кількість кубітів)
163	10^{24}	10^9, 1181
167	10^{25}	10^9, 1209
173	10^{26}	10^9, 1181
179	10^{27}	10^9, 1293
191	10^{29}	10^9, 1378
192	10^{29}	10^9, 1385
224	10^{34}	10^9, 1610
233	10^{35}	10^9, 1673

Розмір порядку базової точки ЕК, біт	Оцінка стійкості для класичного криптоаналізу, ~O (кількість операцій)	Оцінка стійкості для квантового криптоаналізу, ~O (кількість квантових гейтів, кількість кубітів)
256	10^{38}	10^{10}, 1834
257	10^{38}	10^{10}, 1842
283	10^{42}	10^{10}, 2024
307	10^{48}	10^{10}, 2193
367	10^{55}	10^{10}, 2614
384	10^{58}	10^{10}, 2733
409	10^{61}	10^{10}, 2908
431	10^{65}	10^{10}, 3063
521	10^{78}	10^{11}, 3693
571	10^{86}	10^{11}, 4044
701	10^{105}	10^{11}, 4955
768	10^{115}	10^{11}, 5425

Для **асиметричних криптографічних алгоритмів**, які засновані на операціях у числовому полі, зокрема, алгоритму RSA, для факторизації числа N можливо використати алгоритм загального решета числового поля, складність якого обчислюється за формулою

$$O(\exp(\delta(\ln N)^{\gamma}(\ln\ln N)^{1-\gamma})),$$

де $\delta=1.92$, $\gamma=1/3$.

На квантовому комп'ютері для факторизації числа можливо використати поліноміальний алгоритм Шора, складність якого оцінюється величиною $O(4t^3)$ операцій квантового комп'ютера з $O(2t)$ кубітами, де $t=\log_2 N$.

Для алгоритму RSA маємо показники криптографічної стійкості, які наведені у таблиці нижче.

Розмір модуля, біт	Оцінка стійкості для класичного криптоаналізу, ~O (кількість операцій)	Оцінка стійкості для квантового криптоаналізу, ~O (кількість квантових гейтів, кількість кубітів)
512	10^{19}	10^{9}, 1024
768	10^{23}	10^{9}, 1536
1024	10^{26}	10^{9}, 2048
2048	10^{35}	10^{10}, 4096
3072	10^{41}	10^{11}, 6144
4096	10^{47}	10^{11}, 8192
8192	10^{62}	10^{12}, 16384

Для асиметричних алгоритмів шифрування та протоколів узгодження ключів (ПРК) криптографічна стійкість визначається аналогічно у залежності від математичних перетворень, на яких вони засновані.

За даними сайту www.top500.org, станом на листопад 2025 року найпотужнішою обчислювальною системою є суперкомп'ютер "El Capitan" (США) з 11 340 000 ядрами, продуктивність якого складає 1 809 PFlop/s (~10^{18} операцій за секунду).

Слід зазначити, що **збільшення потужності обчислювальних систем** відбувається за рахунок **розпаралелювання обчислень** та збільшення **тактової частоти роботи окремих процесорів** приблизно на один десятковий порядок кожні 3-5 років. Такий темп зростання продуктивності обчислювальних систем не може скласти загрозу сучасним криптографічним алгоритмам та протоколам, які використовуються на практиці.

Що стосується квантових обчислювальних систем, то на сьогоднішній день створені тільки **прототипи квантових комп'ютерів**, які мають порівняно **невелику кількість кубітів**, при цьому час знаходження кубітів у стабільному стані занадто малий.

Враховуючи те, що у теперішній час проводяться активні дослідження у сфері квантових технологій, оцінити термін розробки реальних квантових обчислювальних систем, які зможуть бути використані для цілей криптоаналізу, досить

складно.

Крім кількості кубітів не менш важливим показником є **час знаходження кубітів** у стабільному стані. За цим показником існуючі на теперішній час прототипи квантових комп'ютерів не можуть бути використані для криптоаналізу реальних криптосистем навіть з використанням поліноміального алгоритму Шора.

Перелік джерел посилання

1. Наказ Адміністрації Держспецзв'язку від 27.10.2020 № 687 «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» (зі змінами), що зареєстрований в Міністерстві юстиції України 21 грудня 2020 року за №№ 1272/35555, 1272/35556.
2. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих».
3. ДСТУ 9041:2020 «Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса».
4. ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм асиметричного шифрування та інкапсуляції ключів».
5. Grover's Quantum Search Algorithm [Електронний ресурс] – Режим доступу: https://web.archive.org/web/20201117095032/http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm.
6. Горбенко Ю.І. Аналіз стійкості популярних криптоситем проти квантового криптоаналізу на основі алгоритму Гровера / Ю.І. Горбенко, Р.С. Ганзя // Науково-практичний журнал «Захист інформації». – 2014. Том 16, №2. – С. 22–28.
7. Горбенко, І.Д. Прикладна криптологія. [Текст]: монографія / І.Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. - 868 с.
8. Shor P. W., Polynomial-time algorithms for prime factorization and discretelogarithms on a quantum computer //Proceedings of the 35th Annual Symposiumon the Foundations of Computer Science, S. Goldwasser ed., IEEE Computer Society Press, Los Alamitos CA, 1994.

ВИСНОВКИ

Порушені в Інформаційному бюлетені питання є черговим кроком у напрямі підвищення професійного рівня фахівців, що створює підґрунтя для досягнення основних стратегічних цілей у сфері КЗІ, які визначають формування загальної стратегії та процес прийняття рішень у межах функціонування напрямку дослідження ДержНДІ технологій кібербезпеки, зокрема:

- розроблення національних Стандартів у сфері КЗІ;
- проведення прикладних НДДКР за напрямами розвитку системи КЗІ;
- забезпечення життєвого циклу засобів КЗІ;
- проведення сертифікаційних випробувань засобів КЗІ.

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ:
системи криптографічного захисту інформації

Інформаційний бюлетень
№1 ◦ 2026

Заснований у 2026 році
Виходить щомісяця

Відповідальний за дизайн та верстку:
Ольга ІНКАРБАЄВА, ДержНДІ технологій кібербезпеки.

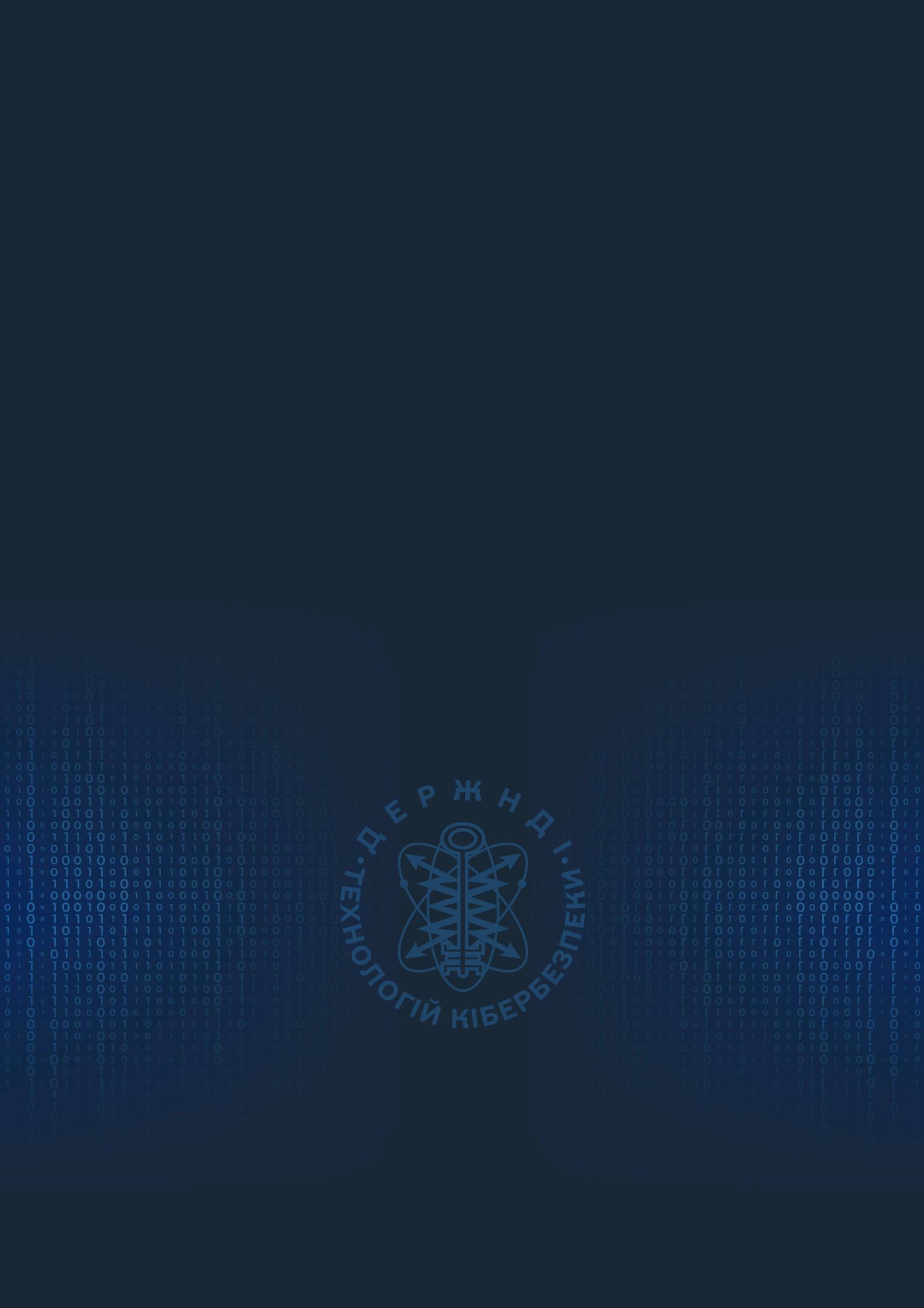
Наклад 50 примірників

Засновник:
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України, 2026 рік

Видавець:
Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації
03142, вул. М. Залізняка 3, корп. 6, м. Київ, Україна
Тел.: 38 (044) 281-85-20, (044) 281-97-11, e-mail: ictip@cip.gov.ua
веб-сайт: csi.cip.gov.ua, Facebook: www.facebook.com/cybersec.sci,
Instagram: www.instagram.com/cybersec.sci

Свідоцтво суб'єкта видавничої справи ДК №8727 від 19 серпня 2026 року
Ідентифікатор медіа R30-07316
Рішення Національної ради України з питань телебачення і радіомовлення
№1652 від 25 червня 2026 року

Матеріали інформаційного бюлетеня можуть бути використані
з посиланням на джерело.


ДЕРЖНДІ
ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ