

GLOBAL ENCRYPTION DAY



2026

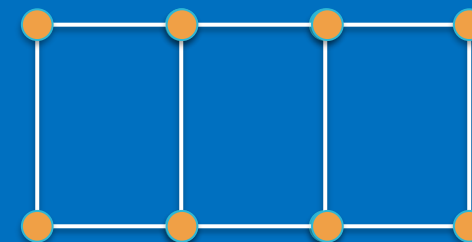
Шифрування як основа цифрової довіри

E2EE • AI • metadata • client-side scanning • post-quantum
cryptography • Internet Governance

21 жовтня 2026

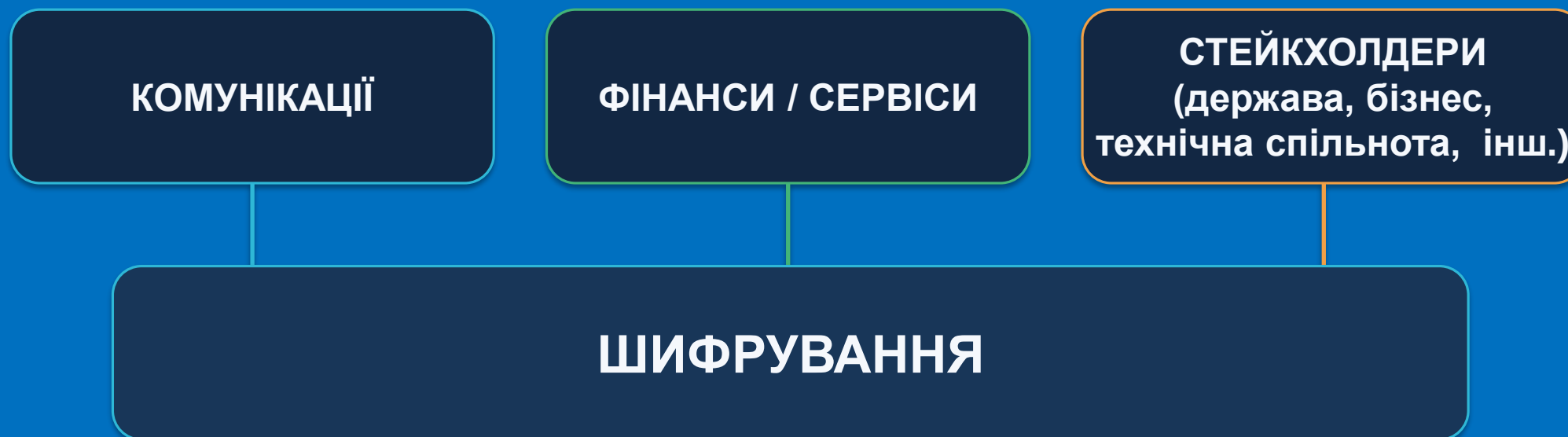


Global
Encryption
Coalition



Чому шифрування стало темою Internet Governance

Від технології захисту даних – до архітектури цифрового довіри



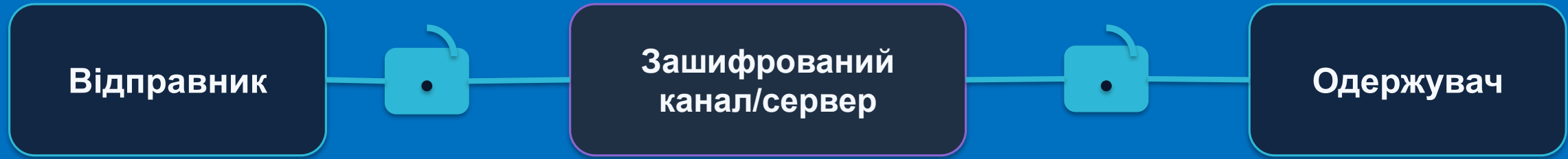
конфіденційність • цілісність • автентифікація • захист від несанкціонованого доступу

Ціль нашого діалогу - не дати «правильну відповідь», а навчитися бачити адміністративні та технічні наслідки рішень по управлінню Інтернет (Internet governance).

ISOC, Global Encryption Day 2026: сильна дискризія є основною частиною статевого захисту online.

Що таке E2EE?

End-to-End Encryption

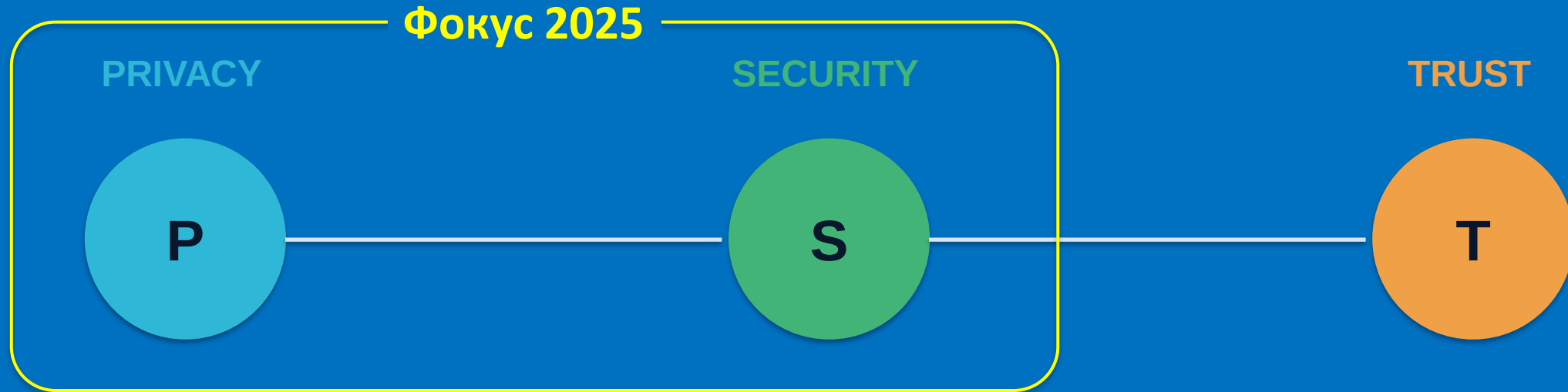


Зміст повідомлення доступний у вигляді тільки кінцевим учасникам комунікації.

- E2EE захищає зміст від доступу посередника до шифрованого повідомлення
- Але E2EE не означає автоматичний захист всіх metadata.
- Безпека залежить також від пристроїв, ключів, додаткової реалізації.

Від Privacy до Digital Trust

Чому 2026 змінює формулювання проблеми

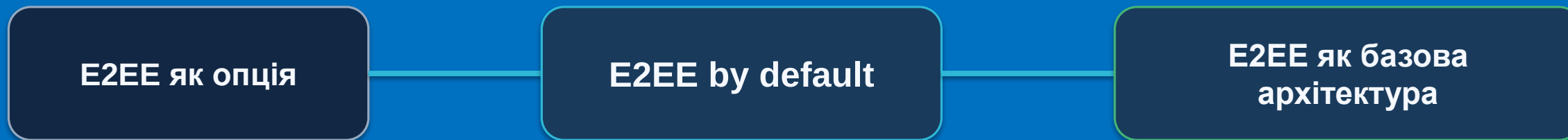


Цифрова довіра означає, що користувач може розраховувати на конфіденційність, цілісність і стійкість цифрової взаємодії.

Encryption → Foundation of Digital Trust

Тренд №1: E2EE стає "by default"

Перехід від «функції» до архітектурних властивостей сервісу



- Discord: E2EE для voice/video дзвінків по замовчуванням.
- Apple + Google: розгортання E2EE для RCS messaging.
- GEC оцінює потенційний охоплення екосистми Android/iPhone приблизно 4 млрд. користувачів.

Наслідок: захист E2EE стає питанням масової інфраструктури, а не вибору «просунутого» користувача.

Але E2EE може і зникати

2026 показує, що архітектурні рішення платформ мають значення

WhatsApp E2EE by default

Messenger E2EE rollout

Instagram Direct E2EE discontinued

GEC критикувала рішення Meta припинити підтримку E2EE у Instagram Direct Messages з травня 2026 року.

- Це показує, що E2EE - не просто checkbox в налаштуваннях.
- Платформи з широким набором функцій, які стикаються з архітектурною та інженерною складністю E2EE.
- Питання 2026року: чи буде privacy protection вбудована по замовчуванням?

Тренд №2: Privacy vs Security → Security vs Security

Як змінюється логіка дискусії про «lawful access»

"Нам потрібен доступ до даних"

Як отримати докази, не створюючи системну вразливість?

Security

захист користувачів

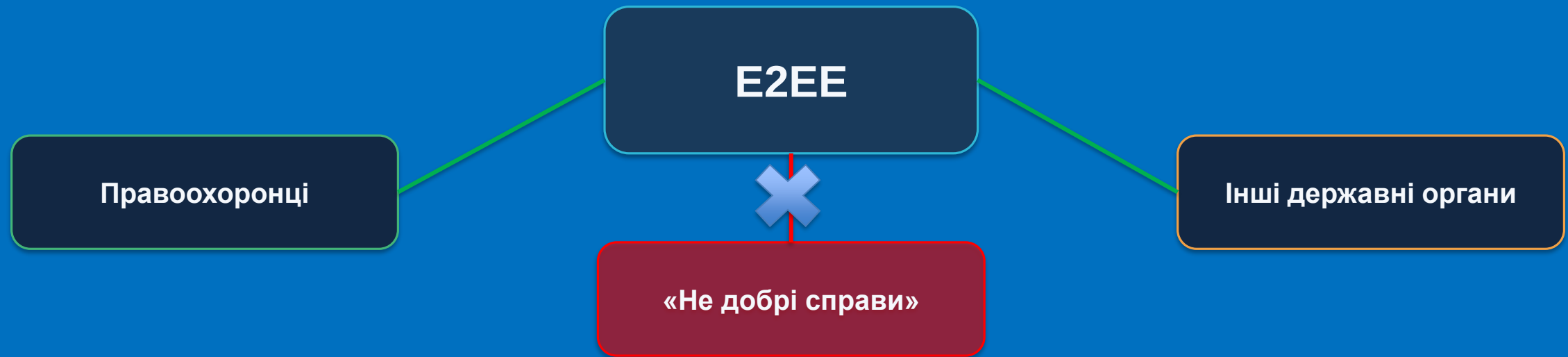
Security

доступ для розслідувань

Центральне питання: як одночасно підтримувати громадську безпеку та охорону інфраструктури?

Backdoor: чому «тільки для добрих справ» не працює

Системна вразливість не знає меж повноважень

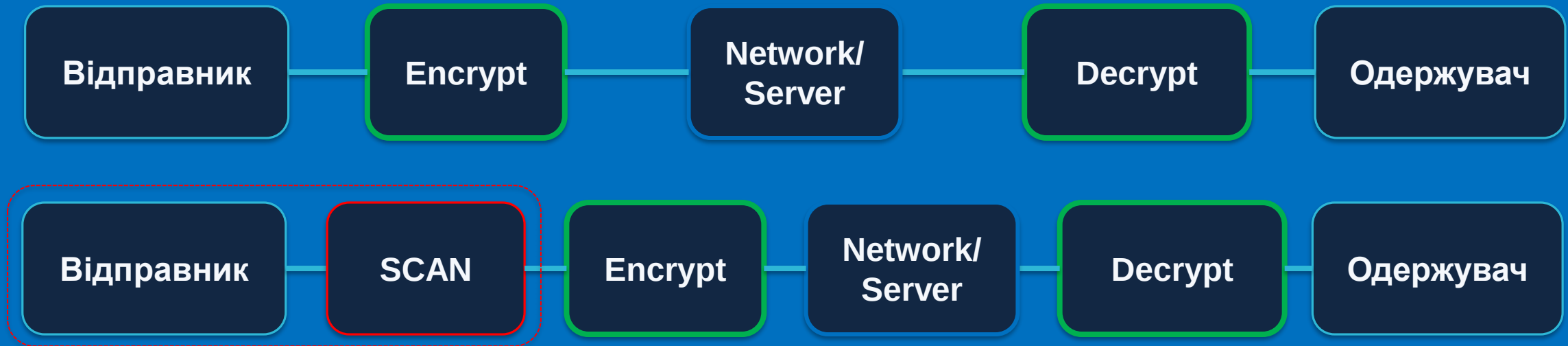


Якщо механізм доступу існує, його наявність стає частиною сукупності всіх уразливостей, точок входу та методів, які зловмисник може використовувати для проникнення в комп'ютерну систему, мережу чи компанію (attack surface)

Питання не тільки «хто отримає ключ?», але і «яка нова вразливість з'являється?»

Client-Side Scanning: шифрування до або після перевірки?

Чому CSS змінює trust model E2EE



CSS технічно не зламує самі криптографічні ключі, але повністю знищує філософію Zero Trust (нульової довіри до посередників), перетворюючи кінцеві пристрої на інструмент превентивного моніторингу.

Формально шифрування не «зламано» – але вміст перевіряється до того, як стає E2EE-захищеним.

- CSS змінює межі довіри: пристрій стає точкою контролю вмісту.
- З'являється нова поверхня атаки і нове джерело false positives/misuse.
- ISOC зазначає, що CSS підриває очікувану конфіденційність E2EE.

Чи можна розслідувати злочини без послаблення E2EE?

ISOC 2026: розширювати слідчі можливості, а не створювати системні недоліки

Інструменти, які можуть працювати в рамках існуючої архітектури Інтернет

User reporting

Undercover

Voluntary
cooperation

Metadata

Device forensics

TARGETED INVESTIGATION + DUE PROCESS + PROPORTIONALITY
ЦІЛЬОВЕ РОЗСЛІДУВАННЯ + НАЛЕЖНА ПРОЦЕДУРА + ПРОПОРЦІЙНІСТЬ

ISOC підкреслює: проблема часто не у відсутності даних, а в здібності законно і ефективно отримувати цікаві дані з вже доступних джерел.

Тренд №3: metadata стає стратегічною сутністю

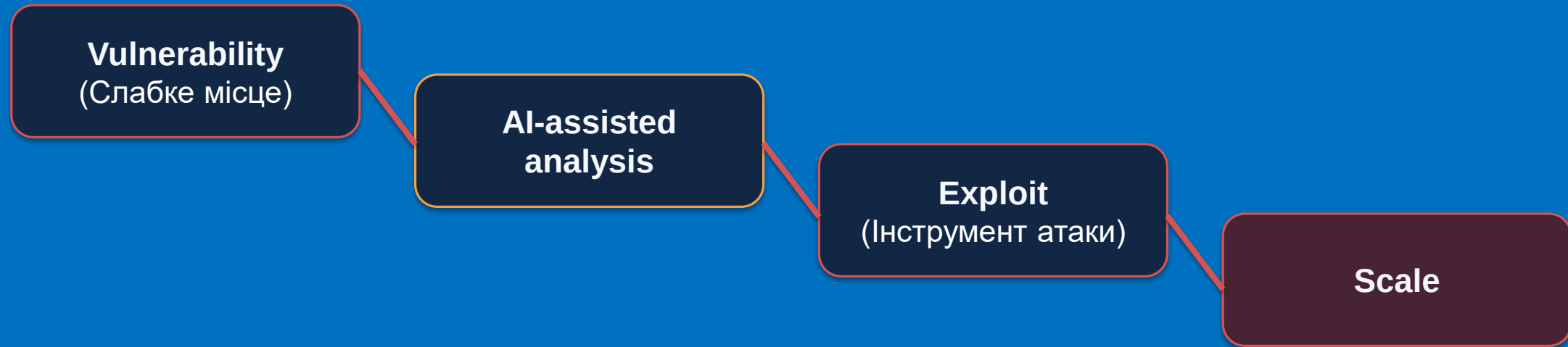
Коли зміст захищений, зростає відносна цінність контексту



Наслідок для Internet Governance: потрібно окремо обговорювати content governance і metadata governance.

Тренд №4: AI змінює модель погроз

Системна вразливість стає не безпечніше, коли пошук і експлуатація вразливостей прискорюються



AI не створює проблему **backdoor** - він змінює економіку атаки

- Чим більше користувачів залежить від одного криптографічного механізму, тим вищий системний ефект компрометації
- У 2026 році до ризиків необхідно додавати швидкість автоматизованого пошуку та експлуатації

Тренд №5: Post-Quantum Cryptography: готуємось заздалегідь

Від RSA/ECC до квантово-стійких механізмів

Класична криптографія

RSA • ECC

Вразливість до алгоритму Шора

Post-Quantum Cryptography
ML-KEM • ML-DSA

Нові математичні основи

«Harvest now, decrypt later»

Дані, що перехоплені сьогодні можуть мати цінність для розшифрування в майбутньому

PQC- це не тільки шифрування, а також authentication / key establishment

Post-Quantum Cryptography: готуємось заздалегідь

Від RSA/ECC до квантово-стійких механізмів

ML-KEM та ML-DSA – це перші офіційні світові стандарти постквантової криптографії, затверджені американським інститутом стандартів та технологій [NIST у серпні 2024 року](#)

ML-KEM (Обмін ключами)

При доступі до ресурсу клієнтському агенту потрібно узгодити із сервером секретний ключ, щоб зашифрувати подальше листування. Клієнт бере відкритий постквантовий ключ сервера, генерує випадковий секрет, «упаковує» його за допомогою ML-KEM шифротекста відправляє серверу. Сервер розпаковує його своїм закритим ключем. Тепер обидва мають спільний ключ, захищений від квантового перехоплення.

ML-DSA (цифровий підпис)

Використовується, коли потрібно довести авторство. Сервер використовує свій закритий ключ, щоб підписати пакет даних алгоритмом ML-DSA. Будь-який користувач з відкритим ключем сервера може миттєво верифікувати цей підпис і переконатися, що файл або сайт не були підроблені хакерами. Що примітно, створення підпису в ML-DSA відбувається майже в 10 разів швидше, ніж у старому RSA-2048

Новий регуляторний фронт: Age Assurance × E2EE

Чи можна обмежити privacy tools тільки для неповнолітніх, не торкнувшись інших?



Парадокс:

щоб обмежити доступ до інструменту забезпечення конфіденційності (privacy-preserving tool) для частини користувачів, може потрібно перевіряти вік всіх користувачів.

- GEC у 2026 виступила проти age-assurance mandates, що торкаються E2EE та VPN.
- Це з'єднує три домени governance: (1) сферу забезпечення безпеки дитинства, (2) конфіденційність та (3) кібербезпеку

Новий регуляторний фронт: Age Assurance × E2EE

Чи можна обмежити privacy tools тільки для неповнолітніх, не торкнувшись інших?

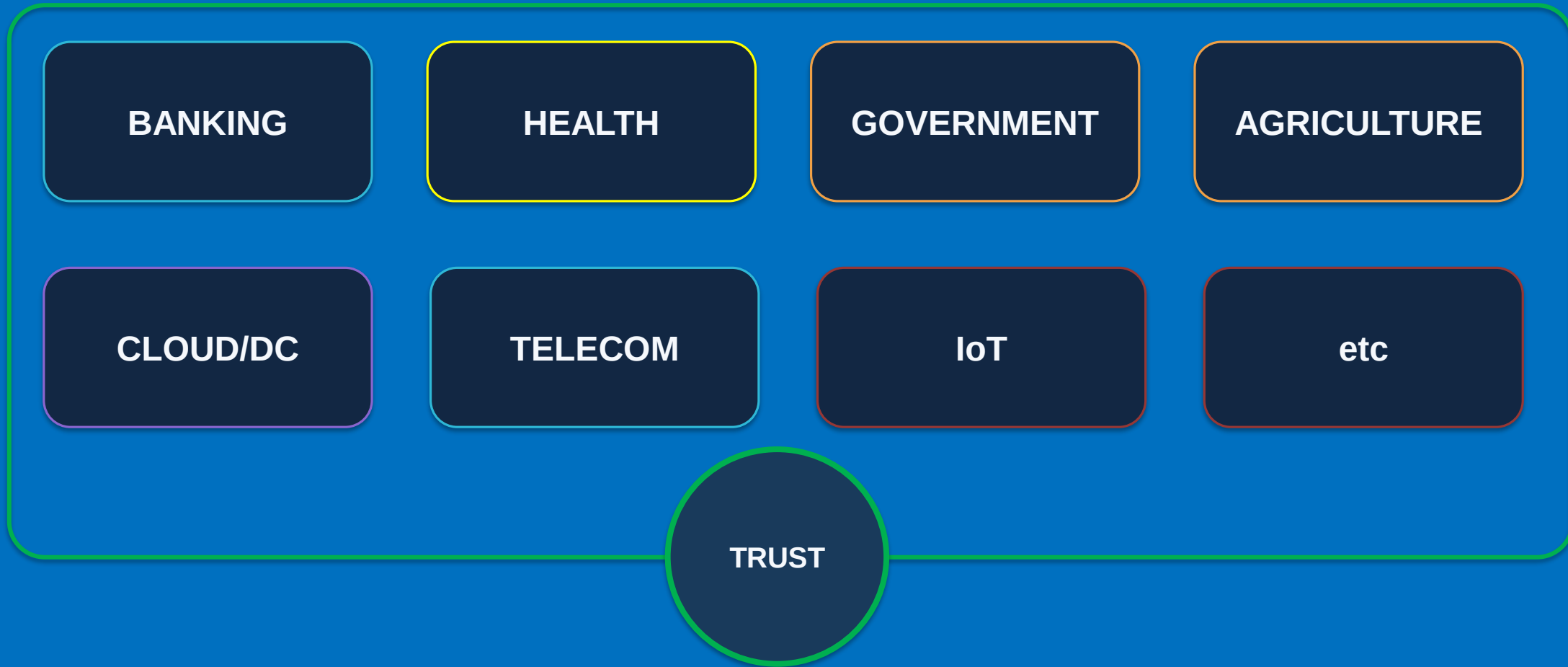
У Великій Британії гостра дискусія навколо Age Assurance (підтвердження віку) та E2EE (наскрізного шифрування) – Закон [Online Safety Act \(OSA\)](#) вимагає впровадження Highly Effective Age Assurance (високоєфективного підтвердження віку) через перевірку документів, сканування особи нейромережею чи за допомогою механізмів перевірки кредитних карток

Закон вимагає від платформ (WhatsApp, Signal, Viber, Telegram, Discord etc.) використання «акредитованих технологій» для пошуку матеріалів, пов'язаних із насильством над дітьми (CSAM) та тероризмом, навіть у зашифрованих чатах

Єдиний спосіб зробити це без формального злому ключів шифрування – впровадити Client-Side Scanning (CSS), що призведе до появи за своєю суттю прихованого бекдора, який перетворює особисті смартфони громадян на інструменти масового державного стеження, повністю зводячи нанівець математичні гарантії E2EE

Encryption та критична цифрова інфраструктура

Чому питання шифрування виходить далеко за межі месенджерів



ISOC 2026: шифрування захищає дані, зв'язок, пристрої та послуги є основою безпечного та надійного Інтернету

Internet Governance: чотири рівні рішення

Encryption - одночасно технічні, і та політичні питання



Головне питання 2026: як узгодити громадську безпеку, кібербезпеку, недоторканність приватного життя та права людини без руйнування базової архітектури Інтернет?

Що це означає для України?

Практичний контекст для студентів та майбутніх фахівців

Телеком & Інтернет

Державні цифрові послуги

Критична інфраструктура

- Українська цифрова інфраструктура працює в умовах підвищеного середовища загроз.
- Encryption - частина стійкості (resilience): захищає комунікації, доступ, дані і довіру до сервісів.
- Для фахівців важливо розуміти не тільки алгоритм, а також governance модель навколо нього
- Європейська інтеграція означає участь України в загальноєвропейських дискусіях про шифрування, конфіденційність та законного доступу (encryption, privacy та lawful access).

10 тенденцій Global Encryption Day 2026

Що варто запам'ятати

Encryption → Digital Trust

E2EE by default

Mainstream adoption

Security vs Security

AI × Encryption

Metadata becomes strategic

Client-side scanning

Age Assurance × E2EE

Post-Quantum transition

Encryption as infrastructure

Головна думка: захист сильного шифрування - це питання не тільки приватності, але і безпеки, довіри і стійкості цифрового ком'юніті

Питання до дискусії

Три питання, на які немає суто технічної відповіді

1. Чи має держава мати доступ до зашифрованих повідомлень, якщо йдеться про (1) намір до злочину, (2) злочин, (3) тяжкий злочин?

2. Чи можна забезпечити безпеку дітей (child safety) не послаблюючи E2EE?

3. Хто повинен визначати межу допустимого втручання до периметру захисту: (1) інженери, (2) держава, (3) платформи, (4) спільнота мультістейкхолдерів або (5) хтось інший?

Джерела і матеріали для подальшого вивчення

Офіційні матеріали Internet Society та Global Encryption Coalition

Internet Society-Global Encryption Day 2026

<https://www.internetsociety.org/events/global-encryption-day-2026/>

GEC-Global Encryption Day Summit 2026

<https://www.globalencryption.org/2026/09/global-encryption-day-summit-2026/>

ISOC-Solving Crime Without Breaking Encryption

<https://www.internetsociety.org/resources/policybriefs/2026/solving-crime-without-breaking-encryption/>

GEC-E2EE by Default, July 2026

<https://www.globalencryption.org/2026/07/global-encryption-coalition-welcomes-growing-adoption-of-end-to-end-encryption-by-default/>

GEC-Age Assurance and E2EE/VPNs

<https://www.globalencryption.org/2026/06/gec-steering-committee-response-to-uk-dsit-consultation-on-age-based-restrictions/>

GEC-Meta/Instagram E2EE

<https://www.globalencryption.org/2026/04/global-encryption-coalition-steering-committee-statement-on-metas-removal-of-end-to-end-encryption-from-instagram-direct-messages/>

ISOC-Client-Side Scanning

<https://www.internetsociety.org/resources/doc/2023/client-side-scanning/>

Презентація - Global Encryption Day 2025

https://isoc-ua.org/wp-content/uploads/2025/10/isoc-global-encryption-day_new.pdf