Технічна пропозиція

Архітектура гео-розподіленої інформаційної системи правосуддя в умовах воєнних загроз та високої доступності

2026

Зміст

Зміст

Анотація

У цій технічній пропозиції представлено архітектуру модернізованої гео-розподіленої інформаційної системи судової влади України (ЄСІКС) в умовах високої воєнної загрози (кінетичних та кібернетичних атак). Запропоновано модель взаємодії двох центральних Центрів обробки даних (ЦОД) та регіональних крайових вузлів («зеленої милі»), яка поєднує механізми асинхронної реплікації, пролонгованих транзакцій (Saga Pattern) та динамічного приховування первинних джерел інформації (Moving Target Defense). Також розглянуто варіанти модернізації розподіленого сховища PDF-документів на базі ScyllaDB DHT з перенесенням майстер-реплік на «зелену милю» для забезпечення максимальної живучості системи відповідно до розширених профілів безпеки стандарту NIST SP 800-53.

1. Нормативно-правова база та безпекові стандарти

Розробка архітектури та забезпечення її резистентності здійснюється з урахуванням вимог законодавства України та провідних міжнародних стандартів інформаційної безпеки:

- Постанова КМУ № 712 від 18 червня 2025 року — «Порядок розроблення та затвердження профілів безпеки» та «Порядок авторизації...» для об'єктів критичної інформаційної інфраструктури (КІІ).
- Закон України «Про захист інформації в інформаційно-комунікаційних системах» та нормативні документи технічного захисту інформації (НД ТЗІ).
- NIST Special Publication 800-53 Rev. 5 — каталог контролів безпеки для державних систем високого рівня захисту, зокрема родини контролів:
  - `CP-9 (Information System Backup)` — створення та захист резервних копій;
  - `CP-10 (Information System Recovery)` — плани відновлення після катастроф;
  - `SC-8 (Transmission Confidentiality and Integrity)` — захист даних при передачі;
  - `SC-28 (Protection of Information at Rest)` — шифрування даних у сховищах;
  - `SI-13 (Predictable Execution Behavior)` та концепція Moving Target Defense.
- NIST SP 800-160 (Systems Security Engineering) — інженерія кібербезпеки систем для забезпечення живучості (Resilience).

Умови воєнного стану вимагають мінімізації ризиків фізичного знищення обчислювальних центрів ракетними ударами та нейтралізації кібервпливів ворога, спрямованих на порушення цілісності та доступності судового діловодства.

2. Топологія гео-розподілу та концепція «Зеленої Милі»

Для усунення єдиної точки відмови (Single Point of Failure — SPOF) інформаційна система розподіляється за гібридною топологією:

1. Центральні вузли (ЦОД-1 та ЦОД-2): Двоє територіально рознесених та синхронізованих резервних центрів обробки даних високого класу захисту. Вони виступають довгостроковими репозиторіями та забезпечують глобальну аналітику та взаємодію з іншими державними реєстрами.
2. Периферійні вузли («Зелена миля»): Автономні регіональні сервери в областях (у межах апеляційних округів або великих судових установ). Вони безпосередньо взаємодіють з операторами на місцях (суддями, секретарями, канцелярією).

Така конфігурація забезпечує автономну роботу місцевих судів протягом дня навіть за умов повного зникнення зв'язку з центральними ЦОД.

3. Механізми асинхронної реплікації та пролонгованих транзакцій

Взаємодія між «зеленою милею» та ЦОД будується на двох зустрічних інформаційних потоках.

3.1. Прямий потік: Оператор → «Зелена миля» → ЦОД

Коли оператор на місці створює судову справу або вносить документ, дані спочатку проходять локальну обробку:

- Локальна фіксація: Дані записуються в локальну базу даних периферійного вузла.
- Outbox Pattern: Зміна реєструється в локальній черзі вихідних повідомлень (Outbox) в межах єдиної транзакції бази даних разом з основними даними.
- Асинхронне відправлення: В кінці дня (або під час операційних вікон з низьким навантаженням) фоновий воркер зчитує повідомлення з Outbox і здійснює пакетне передавання до ЦОД. Це мінімізує демаскувальний мережевий трафік у робочий час.

3.2. Зворотний потік: ЦОД → «Зелена миля»

Дані довідників, класифікаторів та судових реєстрів, які оновлюються централізовано, реплікуються на периферію:

- Кешування: Периферійні сервери викачують необхідні масиви інформації асинхронно для локального використання протягом робочого дня.
- Статус кешу: Отримані дані мають статус тимчасових (Cache). Вони можуть автоматично очищатися (за алгоритмом LRU — Least Recently Used) або заміщуватися новими даними при вичерпанні дискового простору локального сервера.
- Консистентність: Оновлення кешу відбувається за подіями (Event-Driven) через захищені веб-сокети або шляхом опитування версійних точок доступу.

3.3. Пролонговані транзакції (Saga Pattern)

Враховуючи нестабільність каналів зв'язку через активну роботу засобів радіоелектронної боротьби (РЕБ) та руйнування інфраструктури, синхронна двофазна фіксація (2PC) є неприйнятною. Для гарантованої доставки застосовується патерн пролонгованих транзакцій (Saga Pattern):

- Кожна операція зміни статусу справи або документа розбивається на послідовність локальних кроків.
- У разі втрати зв'язку транзакція залишається в проміжному стані на локальному вузлі, гарантуючи збереженість змін для оператора.
- При відновленні каналу зв'язку стан автоматично пролонгується до ЦОД. Якщо транзакція відхиляється на центральному рівні (наприклад, через конфлікт версій), виконується компенсуюча транзакція для корекції локального стану на периферії з обов'язковим сповіщенням адміністратора безпеки.

4. Динамічне приховування джерел інформації (Moving Target Defense)

ЄСІКС налічує близько 60 окремих підсистем (компонентів). Постійна фіксація джерел істини (Master Data Sources) у визначених географічних координатах (наприклад, у конкретному ЦОД) робить систему вразливою до цілеспрямованого вогневого (ракетного) або кібернетичного знищення.

Для захисту пропонується концепція Moving Target Defense (MTD):

- План випадкового чергування: Протягом року випадковим чином складається динамічний графік (план), згідно з яким розподіляються ролі компонентів системи.
- Динамічна міграція майстра: Залежно від операційного вікна, первинне джерело істини (Master Database/Write Node) для кожного з 60 компонентів довільно мігрує або в ЦОД-1/ЦОД-2, або на один із захищених периферійних вузлів «зеленої милі».
- Динамічна маршрутизація: Клієнтські додатки та взаємопов'язані сервіси автоматично перенаправляють запити на запис через захищену оверлейну мережу (Service Mesh на базі mTLS), яка визначає актуальний вузол-лідер без розкриття його реальної фізичної IP-адреси для зовнішніх систем.

Це не дозволяє ворогу точно визначити, де саме в конкретний момент часу зберігаються оригінальні дані тієї чи іншої підсистеми, що робить безглуздими як точкові кібератаки, так і кінетичні удари.

5. Модернізація системи зберігання PDF-документів на базі ScyllaDB DHT

Наразі великі обсяги PDF-документів (матеріали справ, судові рішення) зберігаються в розподіленій хеш-таблиці (DHT) на базі ScyllaDB, яка розгорнута виключно в центральних ЦОД. Це створює критичний ризик втрати або недоступності документів.

5.1. Варіанти модернізації сховища

5.1.1. Варіант 1: Повна реплікація DHT на вузли «зеленої милі»

Передбачає повне копіювання всього масиву PDF-документів на всі регіональні сервери.

- Переваги: Максимальна автономність регіонів.
- Недоліки: Величезні витрати на зберігання даних (Storage Overhead); надлишкове споживання смуги пропускання мережі для синхронізації гігабайтних архівів; високі ризики компрометації великих обсягів даних у разі фізичного захоплення регіонального вузла.

5.1.2. Варіант 2: Локальне кешування за запитом (Lazy Caching)

Крайові сервери викачують PDF-документи з ЦОД лише у разі потреби користувача і зберігають їх у локальному тимчасовому кеші.

- Переваги: Економія дискового простору на периферії.

- Недоліки: Нульова працездатність під час мережевої ізоляції; при знищенні ЦОД втрачаються всі документи, які не встигли потрапити в локальні кеші.

5.1.3. Варіант 3: Гібридна ScyllaDB DHT з локальними майстер-репліками (Рекомендований)

Модернізація сховища шляхом розширення ScyllaDB-кластера на регіональні сервери «зеленої милі» з налаштуванням політики реплікації за топологією мережі.

[Схема реплікації: Локальний запис на «Зеленій милі» → Асинхронна передача в ЦОД]

Деталі реалізації рекомендованого варіанту:

- Локальний Master: Створюваний у суді документ (PDF) підписується КЕП судді і записується безпосередньо у локальний сегмент ScyllaDB DHT на «зеленій милі». Для цього документа локальний вузол стає основним (Master Replica).
- Гео-реплікація: ScyllaDB конфігурується за допомогою `NetworkTopologyStrategy`, де кожен регіональний вузол і ЦОД виступають окремими Data Centers у розумінні СКБД.
- Асинхронна синхронізація: Запис негайно завершується успіхом на локальному рівні (Consistency Level: `LOCAL_QUORUM` або `ONE`), а реплікація до ЦОД-1, ЦОД-2 та одного з сусідніх регіонів відбувається асинхронно у фоновому режимі.

5.2. Аналіз безпеки та живучості відповідно до NIST SP 800-53

Рекомендований Варіант 3 безпосередньо відповідає вимогам розширених профілів безпеки:

- SC-28 (Protection of Information at Rest): Кожен PDF-документ перед записом у DHT шифрується на рівні прикладного ПЗ за допомогою симетричного ключа (AES-GCM-256), який пов'язаний з ідентифікатором справи. Ключі зберігаються в апаратному модулі безпеки (HSM / Гряда) або захищеному сховищі ключів. Навіть при компрометації дисків ScyllaDB на периферії, зловмисник не отримає доступу до змісту документів.
- SC-8 (Transmission Confidentiality and Integrity): Весь міжвузловий трафік реплікації ScyllaDB захищений двостороннім TLS (mTLS) з використанням сертифікатів внутрішнього ЦСК судової системи.
- CP-9 (Information System Backup) & CP-10 (System Recovery): Система не потребує класичного «холодного» бекапу для відновлення працездатності. При повному знищенні одного або обох ЦОД, первинні дані PDF-документів залишаються збереженими на периферійних вузлах «зеленої милі», які їх створили. Новий ЦОД може бути розгорнутий і наповнений даними шляхом ініціалізації процедури відновлення кластера (Node Recovery) з периферійних джерел.

6. Порівняльний аналіз варіантів модернізації сховища PDF

У таблиці ?? наведено порівняння трьох розглянутих архітектурних варіантів модернізації системи зберігання документів.

Табл. 1: Порівняльний аналіз варіантів зберігання PDF-документів

Критерій порівняння	Варіант 1 (Повна)	Варіант 2 (Кеш)	Варіант 3 (Гібрид)
Накладні витрати сховища	Критично високі	Мінімальні	Помірні (оптимальні)
Мережевий трафік вдень	Критично високий	Низький	Низький
Автономність при ізоляції	Повна	Відсутня	Повна для локальних справ
Живучість при руйнуванні ЦОД	Повна	Низька	Абсолютна (за рахунок регіонів)
Шифрування (NIST SC-28)	Підтримується	Підтримується	Децентралізоване (AES-GCM)
mTLS шифрування (NIST SC-8)	Складне керування	Стандартне	Вбудоване в кільце ScyllaDB

7. Висновки

Впровадження запропонованої гео-розподіленої архітектури ЄСІКС на базі топології «Зеленої милі», асинхронної реплікації через Outbox/Saga та концепції Moving Target Defense дозволяє створити високонадійну систему правосуддя, стійку до загроз воєнного часу.

Модернізація сховища PDF-документів за Варіантом 3 (гібридний DHT на базі ScyllaDB з локальними майстер-репліками) є оптимальним інженерним рішенням, яке гарантує збереженість критичних даних судочинства при фізичній ліквідації основних ЦОД та повністю відповідає вимогам безпекових профілів класу Assurance L2 і стандарту NIST SP 800-53.

Література

[1] NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.

[2] NIST Special Publication 800-160 Vol. 2 Rev. 1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.

[3] Постанова Кабінету Міністрів України № 712 від 18 червня 2025 року. Про затвердження Порядку розроблення та затвердження профілів безпеки.

[4] ScyllaDB Enterprise Documentation. Advanced Replication Strategies: Datacenter-Aware Configuration (NetworkTopologyStrategy).

[5] Chris Richardson. Microservices Patterns: With examples in Java (Saga Pattern and Outbox Pattern implementations).

[6] Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats (Advances in Information Security).