ТЕХНІЧНИЙ ДОКУМЕНТ · ПРОПОНОВАНА АРХІТЕКТУРА · ВЕРСІЯ 1.0

Від виявлення до впровадження заходів реагування

Вимірювана архітектура реагування на DNS Abuse: походження та ланцюг збереження доказів, пропорційні заходи, публічна підзвітність і швидке оскарження—розроблена для перевірки, а не лише для декларування.

Опубліковано 2 серпня 2026 року
PhishDestroy Дослідження
Проект для громадського обговорення
Не пройшло рецензування

PD-WP-2026-01 · Версія 1.0 · Опубліковано 2 серпня 2026 року
Постійна URL-адреса: https://phishdestroy.io/uk/dns-abuse-enforcement-framework

АНОТАЦІЯ

НЕЗАЛЕЖНА ПРОПОЗИЦІЯ · НЕ Є ПРОГРАМОЮ «ICANN»

Прямий висновок. У контрактній екосистемі «gTLD» існує помітний розрив між технічно підтвердженим зловмисним використанням домену та ефективними заходами щодо його нейтралізації. Опубліковані дослідження показують, що багато фішингових кампаній тривають годинами або днями, тоді як процедури забезпечення дотримання договірних зобов'язань можуть розгортатися протягом робочих днів. Оприлюднена модель сценарію демонструє, як затримка збільшує очікувані прибутки від кампанії; діапазон 60–85 % є основною перевіреною оцінкою збитків після отримання повідомлення, наведеною в статті, а не встановленою статистикою для всіх випадків шахрайства у світі. Інженерна оцінка у розмірі 100–150 доларів стосується збору та первинної обробки визначеного корпусу даних про зони, прозорість сертифікатів та публічні канали, а не повної вартості юридичної експертизи чи примусового виконання. У статті пропонується використання підписаних доказів, вимірюваних цілей реагування, автоматичної ескалації підтверджених випадків, пропорційних заходів виправлення, публічної підзвітності та швидкого оскарження. У ній не пропонується надавати особам, які повідомляють про порушення, прямий доступ до засобів управління призупиненням доменів.

● ПЕРШОДЖЕРЕЛО
Підтверджено офіційним документом або опублікованим дослідженням.

● ІЛЮСТРАТИВНА МОДЕЛЬ
Розрахунок, результати якого можна відтворити, а вихідними даними для нього є припущення, а не середні ринкові показники.

● ПРОПОЗИЦІЯ ЩОДО ПОЛІТИКИ
Проект, запропонований для обговорення, тестування та доопрацювання.

01 Дослідницьке питання, сфера дослідження та рівень доказовості

Це питання є більш вузьким, ніж «хто провалився?»: **які з помітних затримок між підтвердженими доказами та пропорційними заходами можна запобігти, і яке втручання зменшує шкоду для**

жертв, не створюючи при цьому неприйнятних помилкових спрацьовувань або побічної шкоди?

Сфера застосування охоплює екосистему gTLD, що діє на договірних засадах: реєстрантів, реселерів, реєстраторів, реєстри та підрозділ ICANN, відповідальний за дотримання договірних зобов'язань. Постачальники послуг хостингу, мережі CDN, браузери, платіжні сервіси, рекламні платформи, національні центри реагування на інциденти (CERT) та органи кримінального правосуддя включаються лише в тих випадках, коли вони впливають на ланцюг доказів або реагування. Домени верхнього рівня з кодом країни мають іншу систему управління і не вважаються такими, що підпадають під дію контрактів ICANN щодо gTLD.

Стан розробки основних тез

- У статті аналізується організація «ICANN» як приватна інституція, що забезпечує управління та дотримання договірних зобов'язань у рамках екосистеми «gTLD». «ICANN» не є державним регуляторним органом чи правоохоронною структурою, проте вона здійснює акредитацію реєстраторів, укладає договори з операторами реєстрів та забезпечує виконання цих угод; такі обмежені повноваження не звільняють організацію від інституційної відповідальності.
- Діапазон 60–85 % є основною кількісною оцінкою в моделі шкоди, представленій у статті. Вона подається як оцінка, що піддається перевірці та виведена на основі чітких припущень і спостережень за конкретними випадками, а не як вже встановлений статистичний показник для всіх випадків шахрайства у світі. Наступним доказовим кроком є оприлюднення набору даних на рівні окремих інцидентів, у якому узгоджені часові мітки виявлення, повідомлення, мінімізації наслідків та заподіяної шкоди.
- Цифра в розмірі 100–150 доларів є перевіреною інженерною оцінкою бюджету для безперервного збору та початкового сортування даних щодо визначеного набору доступних зон, прозорості сертифікатів та даних з публічних каналів про базову інфраструктуру. Це не вартість повної глобальної прозорості, юридичної експертизи, оскаржень, високої доступності чи забезпечення дотримання вимог. Тому в статті ця цифра розглядається як орієнтир, який можна відтворити за допомогою опублікованих даних про робоче навантаження, перелік джерел та журнал витрат, а не як вже перевірена універсальна ціна. Це розмежування звужує масштаб твердження, не скасовуючи при цьому асиметрії витрат, що перевіряється.
- Тритижневе порівняння, наведене в статті, стосується затримки у виконанні вимог, а не універсального SLA щодо вилучення доменів. У статті «ICANN» Часті запитання щодо дотримання умов договору у ньому зазначено, що більшість типів скарг можуть пройти три послідовні періоди реагування тривалістю п'ять робочих днів кожен, перш ніж справа буде офіційно передана на розгляд вищого рівня, тоді як багато зловмисних кампаній тривають годинами або днями. У контрактах окремо передбачено необхідність вжиття оперативних та відповідних заходів щодо мінімізації ризиків після отримання доказів, що дають підстави для дій. [2] [4]
- У випадку підтвердженої зловмисної реєстрації, призначеної виключно для однієї мети, `serverHold` є одним із найбільш руйнівних засобів захисту на рівні DNS, оскільки призводить

до видалення делегування із зони. Цей засіб не є універсальним: він також може порушити роботу пошти, субдоменів та легітимних служб; кешовані відповіді можуть зберігатися до закінчення терміну дії TTL; а для скомпрометованих або спільних служб може знадобитися більш цілеспрямовані заходи з мінімізації ризиків. [4] [7]

ВНЕСОК У НАУКОВІ ДОСЛІДЖЕННЯ

Ця гіпотеза піддається перевірці. У рамках пілотного дослідження можна порівняти експериментальну та контрольну групи за такими показниками: час до сортування, час до вжиття заходів з пом'якшення наслідків, показники, що відображають втрати серед жертв, частоту рецидивів, кількість хибнопозитивних результатів, час відміни ефекту та побічні наслідки.

02 Що свідчать першоджерела

$165.1M

ICANN FY27 фінансування операційної діяльності

Затверджено бюджет «FY27». Масштаб залежить від контексту; витрати не відповідають принципу «DNS Abuse». [1]

191,561

Скарги на фішинг та спуфінг у 2025 році (IC3)

Найбільша за кількістю категорія скарг, зареєстрованих у IC3; прямі збитки, визначені на суму 215,8 млн доларів. [10]

24 години

Медіанна тривалість життя за даними одного дослідження 2021 року

Результат, що стосується конкретного набору даних, отриманий на основі аналізу 1 288 фішингових доменів; це не є універсальним показником тривалості існування. [11]

Немає фіксованого SLA

Загальний термін зняття контенту

У поправках 2024 року передбачено «негайні» та «належні» заходи щодо пом'якшення наслідків, а не єдиний загальний термін. [2] [3]

ТЕЗА	СТАТУС	ЩО МОЖНА СКАЗАТИ
Фішинг є DNS Abuse	ПЕРЕВІРЕНО	Фішинг прямо визначено як одну з п’яти категорій, охоплених договірними поправками щодо gTLD 2024 року. [2]
Реєстратори повинні діяти	ПЕРЕВІРЕНО	Реєстратори повинні оперативно діяти, коли мають придатні для реагування докази того, що спонсороване ними доменне ім’я використовується для DNS Abuse. [2]
Оператори реєстрів повинні діяти	ПЕРЕВІРЕНО	Оператори реєстрів повинні оперативно діяти, коли на підставі придатних для реагування доказів вони обґрунтовано визначають, що зареєстроване доменне ім’я використовується для DNS Abuse; належний захід залежить від контексту. [3]
`serverHold` скасовує делегування	ПЕРЕВІРЕНО	Це статус «EPP», встановлений сервером. Відповіді, збережені в кеші за адресою DNS, можуть зберігатися до закінчення терміну дії, і ця дія поширюється на весь зареєстрований домен. [7]
Усі випадки DNS Abuse можна побачити в CZDS або CT	НЕПРАВДА	CZDS і Certificate Transparency є цінними сенсорами, але не дають повного або актуального в реальному часі уявлення про все використання доменів. [8] [9]

У першому піврічному звіті компанії ICANN щодо виконання договірних зобов’язань відповідно до поправок 2024 року зафіксовано 192 розслідування, понад 2 700 призупинених доменів, понад 350 заблокованих фішингових сторінок та два повідомлення про порушення. Ці цифри не доводять, що нинішні заходи контролю є достатніми, але вони спростовують категоричне твердження про те, що система не вживає жодних заходів. [5]

03 Чому затримка відгуку залишається актуальним напрямком досліджень

Деякі фішингові операції тривають від кількох годин до кількох днів. У одному дослідженні 2021 року Бійманс та ін. повідомили, що середня тривалість існування 1 288 фішингових доменів становила 45 годин, а медіана — 24 години. [11] У дослідженні 2026 року, присвяченому нещодавно зареєстрованим фішинговим доменам, було виявлено значний перекіс у розподілі: серед 14 112 доменів із вимірюваним терміном існування середнє значення становило 8,6 дня, а медіана — один день. [12] Жоден із цих прикладів не можна поширювати на всі категорії загроз, але обидва вони демонструють, чому підхід, заснований виключно на підрахунку робочих днів, може не виявити короткочасні шахрайські та фішингові операції.

> **ВИМІРЯНЕ ЧАСОВЕ РОЗХОДЖЕННЯ**
>
> Ці дослідження не визначають частку фінансових збитків, що виникають після отримання повідомлення, але вони виявляють часовий розрив: процес, на початкових етапах якого неформальне дотримання вимог може займати до п’ятнадцяти робочих днів, сам по собі не може слугувати реагуванням на інциденти для кампаній, середня тривалість яких становить близько одного дня. Отже, наведений нижче 21-денний термін є сценарієм затримки у дотриманні вимог, а не позначенням універсального «SLA ICANN».

РИСУНОК 1 · ІЛЮСТРАТИВНИЙ СУКУПНИЙ РЕЗУЛЬТАТ ОПЕРАЦІЇ З ШАХРАЙСТВА ТА ФІШИНГУ

МОДЕЛЬ · ЛОГ-ПОДІБНИЙ ІНТЕРВАЛ ЧАСУ

Ця крива ілюструє сценарій, описаний у розділі 4; це не фактичні ринкові дані. Горизонтальне розташування стискає довгі проміжки часу для зручності сприйняття. Джерело: відтворювана модель з оприлюдненими вхідними даними.

ОБЕРЕЖНІСТЬ ЩОДО ПРИЧИННО-НАСЛІДКОВИХ ЗВ'ЯЗКІВ

Скорочення терміну існування домену не означає автоматичного запобігання фінансовим збиткам. Зловмисники можуть перейти на інші ресурси, використовувати зламані сайти, змінити канали розповсюдження або вивести кошти до того, як їх виявлять. Причинно-наслідковий зв'язок необхідно вимірювати, а не робити висновки лише на основі швидкості блокування.

04 Економіка шахрайської та фішингової операції як відтворюваного сценарію

Економічно значущим активом часто є не реєстраційний внесок, а трафік, креативний потенціал, інфраструктура та довіра, накопичені навколо домену. Таке припущення є цілком ймовірним; його масштаби варіюються залежно від характеру шахрайських та фішингових операцій. Тому наведений нижче калькулятор відображає всі вхідні дані, а не подає гіпотетичний результат у вигляді середнього значення, отриманого на основі спостережень.

ВИЗНАЧЕННЯ МОДЕЛІ

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Калькулятор сценаріїв

Змініть будь-яке припущення. Наведені значення є ілюстративними і не є оцінками типового ринку фішингу.

ІЛЮСТРАТИВНА МОДЕЛЬ

Бюджет шахрайської та фішингової операції (USD)

5000

Щоденні відвідування

2000

Коефіцієнт конверсії у жертву (%)

1.5

Середній розмір збитків на одну жертву (USD)

2400

Втрати під час виведення коштів (%)

25

Час до застосування заходу (години)

24

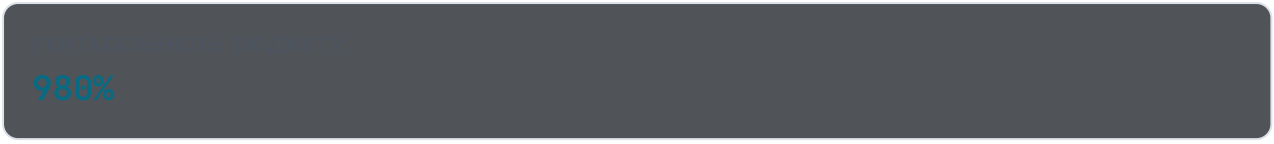
2,000

30

$54,000

$49,000

2.2 h



Оскільки модель відображає очікуване значення, прогнозована кількість жертв може бути дробовою. Вона не враховує спад трафіку, зміну поведінки після виявлення, перенесення кампанії, повторний підрахунок жертв і розподіли невизначеності.

▶ Переглянути таблицю джерел моделі

05 Оцінка запобіжної шкоди без вигадування точності

«Втрата після виявлення» може стати корисним результатом лише за умови послідовного визначення понять «виявлення», «передача» та «завдання шкоди». Час внесення до чорного списку не є доказом того, що реєстратор отримав докази, на підставі яких можна вжити заходів. Транзакцію з гаманця не можна автоматично пов’язати з одним конкретним доменом. Те, що домен стає недоступним, не дозволяє встановити, який суб’єкт спричинив цю зміну.

Мінімальна схема події

ПОДІЯ	НЕОБХІДНА МІТКА ЧАСУ	МІНІМАЛЬНИЙ ДОКАЗ
Перше спостереження	`t_obs`	Датчик, хеш запиту/відповіді, метод зчитування, джерело тактової частоти.
Технічна валідація	`t_valid`	Повторюваний показник, особистість рецензента, категорія загрози та рівень впевненості.
Повідомлення вручено	`t_повідомлення`	Версія з підтвердженою квитанцією про доставку та пакетом доказів.
Відповідальна сторона визнає, що	`t_ack`	Ідентифікатор справи та роль адресата: хост, реєстратор, реєстр, платформа або уповноважений орган.
Спостерігається пом'якшення наслідків	`t_mitigate`	DNS, HTTP, стан платежів або платформи, що вимірюються з різних точок спостереження.
оскарження / відновлення	`t_restore`	Підстави для прийняття рішення, зміна доказів та перевірка відновлення.
Подія, що завдає шкоди	`t_harm`	Звіт про потерпілого без ідентифікаційних даних, відповідна транзакція або інший задокументований показник.

ПРОПОНОВАНИЙ ПОКАЗНИК РЕЗУЛЬТАТИВНОСТІ

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

У чисельнику та знаменнику має застосовуватися одне й те саме правило віднесення. У результатах слід вказати когорту, довірчий інтервал, праве цензурування, відсутні джерела, обробку дублікатів жертв та чутливість до вікна спостереження. Термін «попереджуваний» слід застосовувати лише у випадку причинно-наслідкового дизайну або, як мінімум, порівняння за парностями — а не до кожної події після повідомлення.

СЕРЕДНЯ МОДЕЛЬОВАНА ОЦІНКА · 60–85 %

У статті як основна оцінка частки шкоди, що може бути пов’язана з інцидентом і яка виникає після його виявлення та повідомлення, у класі модельованих інцидентів зберігається значення 60–85 %. Це оцінка сценарію, отримана на основі оприлюднених припущень та спостережень за конкретними випадками, а не виміряна статистична величина, що охоплює всі випадки шахрайства у світі. Її слід використовувати для аналізу чутливості доти, доки набір даних на рівні окремих інцидентів не узгодить спостереження, підтверджені докази, терміни виявлення, запобігання та заподіяння шкоди. Оприлюднення цього набору даних є доказовою перевіркою тези, а не приводом для її відхилення.

06 Інституційна схема: потенціал розподілений

Жоден окремий учасник не бачить і не контролює весь процес у цілому. Реєстратор знає про відносини між реєстрантами; реєстр контролює стан доменів, що знаходяться в його віданні; хост-провайдер та CDN контролюють доставку контенту; браузери та постачальники засобів безпеки контролюють попередження; постачальники платіжних послуг та електронних гаманців можуть переривати перекази; органи влади можуть вимагати збереження або вилучення даних. ICANN розробляє та забезпечує виконання договорів в екосистемі gTLD, але не керує універсальною площиною управління EPP.

01 · СИГНАЛ

Дослідники та датчики

Спостерігати за індикаторами контенту, інфраструктури та жертв; зберігати походження та ланцюг збереження доказів.

02 · ОБСЛУГОВУВАННЯ

Ведучий / CDN / платформа

Може швидко видаляти вміст або блокувати доступ, часто без зміни домену.

03 · СПОНСОР

Реєстратор

Перевіряє наявність зловмисного технічного використання, зв'язується з власником домену та може встановлювати статус на стороні клієнта.

04 · ЗОНА

Оператор реєстру

Керує налаштуваннями реєстру, що визначають статус «EPP», а також делегуванням зони «TLD».

05 · ДОГОВІР

ICANN Дотримання вимог

Перевіряє дотримання вимог контрагентами; не розглядає кожен випадок шахрайства.

06 · ПРАВО

CERT / органи влади

Координувати заходи реагування та використовувати повноваження, передбачені законодавством конкретної юрисдикції.

Розподілені повноваження не означають зняття відповідальності. Реєстратор-спонсор не звільняється від своїх договірних зобов'язань, делегуючи розгляд випадків зловживань реселлеру; реєстр контролює стан EPP, встановлений на серверах; організація «ICANN» забезпечує дотримання договірних зобов'язань. У журналі аудиту має фіксуватися не лише те, хто вчинив дію, а й те, хто отримав докази, що дають підстави для вжиття заходів, перенаправив справу, не надав відповіді або не виконав покладене на нього обов'язок. Юридичні повноваження залишаються за особою, уповноваженою застосовувати заходи; відповідальність також поширюється на задокументовані випадки невиконання обов'язків.

Концентрація фінансування та гіпотеза про конфлікт стимулів, що піддається перевірці

$165.1M

Фінансовий рік 27: Фінансування діяльності організації «ICANN»

Затверджено базовий варіант бюджету на 27-й фінансовий рік. [1]

≈98.1%

джерела доходів від реєстрації та послуг реєстратора

Приблизно 162,0 млн доларів із загального обсягу фінансування в розмірі 165,1 млн доларів. [1]

70.7%

лише комісії за транзакції

$116.8M tied to billable domain transactions. [1]

Отже, структура фінансування значною мірою зосереджена на платежах від сторін, з якими укладено договори, виконання яких забезпечує організація «ICANN», а значна її частина залежить від кількості реєстраційних операцій, що підлягають оплаті. Це створює структурну залежність і викликає обґрунтовані сумніви щодо конфлікту інтересів. Це *не*, самі по собі не є доказом навмисного недотримання законодавства або повного «захоплення регуляторних органів». Гіпотезу про захоплення слід перевіряти з урахуванням часу реагування на конкретні випадки, результатів правозастосування, санкцій, повторних зловживань та ролі зацікавлених сторін, що отримують фінансування, у прийнятті рішень щодо політики та її реалізації.

07 Базовий рівень за договором на 2024 рік — і те, що в ньому не зазначено

Глобальні поправки, внесені у квітні 2024 року до Угоди про акредитацію реєстраторів та Базової угоди про реєстр, запровадили чіткі зобов'язання щодо пом'якшення DNS Abuse. Реєстратори повинні оперативно діяти, коли мають придатні для реагування докази того, що спонсороване ними доменне ім'я використовується для DNS Abuse. Оператори реєстрів повинні оперативно діяти, коли на підставі придатних для реагування доказів вони обґрунтовано визначають, що зареєстроване доменне ім'я використовується для DNS Abuse. В обох випадках належний захід залежить від контексту, серйозності та супутньої шкоди. [2] [3]

Три часові лінії, які часто плутають між собою

ХРОНОЛОГІЯ ПОДІЙ	ДО ЧОГО ЦЕ СТОСУЄТЬСЯ	ЩО ЦЕ НЕ ОЗНАЧАЄ
24 години	Розгляд відповідно до RAA §3.18.3 належно обґрунтованих повідомлень про незаконну діяльність, поданих до спеціальної контактної особи правоохоронними органами, органами захисту прав споживачів, квазіурядовими або подібними органами.	Це не є універсальним 24-годинним терміном для призупинення дії.
«Негайно»	Вжиття відповідних заходів щодо пом'якшення наслідків після досягнення встановленого порогу доказовості, що дає підстави для вжиття заходів.	Це не фіксована кількість годин, і не в кожному випадку потрібні однакові заходи.
21 день	Може розглядатися як строк для виправлення ситуації після офіційного повідомлення про порушення умов договору.	Це не звичайний термін дії, який надається кожному повідомленому шкідливому домену.

Така гнучкість має свої переваги: з компрометованим університетським доменом не слід поводитися так само, як із щойно зареєстрованим одноцільовим фішинговим доменом. Проблема підзвітності полягає в тому, що без опублікованих часових міток, категорій випадків та кодів результатів важко порівняти поняття «оперативно» та «належним чином». Наведена нижче пропозиція передбачає введення механізмів оцінки та перегляду, не стверджуючи при цьому, що один термін підходить для всіх випадків.

08 Проблема розмежування: фішинг враховується; деякі види фінансового шахрайства можуть не враховуватися

Фішинг прямо входить до договірного визначення DNS Abuse. Складніша межа стосується сайтів, які вводять користувачів в оману під власною назвою, а не видають себе за конкретну третю сторону: деяких фальшивих інвестиційних платформ, шахрайських магазинів, схем повернення коштів і підпису гаманців. Залежно від обставин такі випадки можуть розглядатися як порушення на рівні контенту сайту, споживче шахрайство або інша правова категорія, а не договірне DNS Abuse.

> ПРОПОНОВАНА НАЗВА ДОСЛІДЖЕННЯ
>
> **Підтверджене зловживання, що спричиняє фінансову шкоду (VFHA)**: задокументоване використання домену для отримання шляхом обману коштів, платіжних даних, приватних ключів або seed-фраз незалежно від імітації бренду. VFHA не є чинним терміном ICANN і саме по собі не створює договірних повноважень.

Політична консультація може визначити, чи має вузька, доказова категорія на кшталт VFHA належати до майбутніх договорів, міжсекторальної системи перенаправлення або національного

законодавства. Розширення має вимагати точного критерію шкоди, надійних доказів, пропорційних засобів, перевірки юрисдикції та оскарження. Розмитого ярлика «шахрайство» недостатньо.

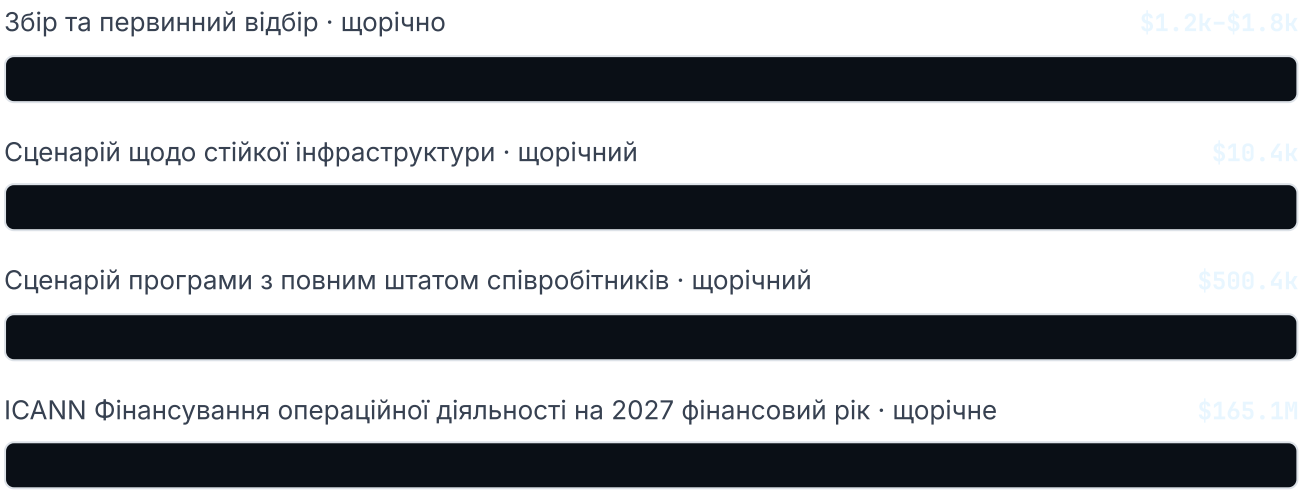
09 Що має довести твердження про моніторинг вартістю 100–150 доларів на місяць — і чого воно довести не може

Стандартний сервер може завантажувати загальнодоступні знімки файлів зон, що беруть участь у програмі «Прозорість сертифікатів» (gTLD), та обчислювати зміни локально, отримувати вибрані події «Прозорості сертифікатів» та відкриті канали даних, нормалізувати рядки, обчислювати хеші та визначати пріоритетність кандидатів. Це корисний, підданий тестуванню інженерний тест — а не «повний моніторинг Інтернету». У другому кварталі 2026 року компанія Verisign повідомила про 401,6 мільйона реєстрацій у всіх доменах верхнього рівня (TLD); система CZDS охоплює файли зон gTLD, що беруть участь у програмі, а не всі домени верхнього рівня, а система CT реєструє публічно зафіксовані сертифікати або попередні сертифікати, а не кожен активний або шкідливий домен. [8] [9] [17]

МОЖЛИВІСТЬ	ЗВИЧАЙНИЙ ПРОТОТИП	ВИРОБНИЧА СЛУЖБА СУСПІЛЬНОГО ІНТЕРЕСУ
Збір зон/CT/каналів	Можливий для визначеного набору джерел	Резервні збирачі, договори з джерелами, моніторинг прогалин
Сортування рядків/хешів	Можливо	Порівняльне тестування, виявлення дрейфу, дослідження хибнонегативних результатів
Відтворення в браузері	Невелика вибіркова підмножина	Ізольований кластер, регіональні точки спостереження, стримування шкідливого ПЗ
Правове визначення	Не включено	Кваліфіковані рецензенти, зіставлення юрисдикції та повноважень
Висока доступність / збереження доказів	Зазвичай відсутнє	Підписи на основі HSM, журнали аудиту, резервні копії та реагування на інциденти
Оскарження та відновлення	Не включено	Робота 24/7, незалежна ескалація та цільові показники сервісу

РИСУНОК 2 · КОНТЕКСТ ПОРЯДКУ ВЕЛИЧИН

ЛОГАРИФМІЧНА ШИРИНА · ВИТРАТИ, ЩО НЕ МОЖНА ПОРІВНЮВАТИ НА ОДНІЙ ОСНОВІ



Завдяки логарифмічному масштабуванню навіть найменші значення залишаються видимими. Перші три цифри є оприлюдненими інженерними або програмними припущеннями, які потребують опублікованого еталонного показника, і не є ціновими пропозиціями постачальників. ICANN Фінансування операційної діяльності — це перевірена цифра на інституційному рівні. Ці бюджети навмисно нерівнозначні: порівняння перевіряє, чи є базовий збір та сортування даних за своєю суттю надмірно високими витратами, а не те, чи коштує повна програма забезпечення дотримання вимог 100 доларів на місяць.

10 Пропонована система реагування на підтверджені випадки DNS Abuse

Запропонована система є еталонною архітектурою, а не автоматичним глобальним механізмом відключення. Вона стандартизує формат справи, протокол прийняття рішення та часові мітки, водночас надаючи уповноваженому оператору можливість обрати найменш руйнівний ефективний захід.

01 · ІНГЕСТ

Придбати та зберегти

Збирати звіти та спостереження; обробляти необроблені артефакти; синхронізувати годинники.

02 · походження та ланцюг зберігання доказів

Узагальнити докази

Зафіксуйте походження, метод, історію обробки та залежності від джерел.

03 · ПЕРЕВІРИТИ

Підтвердити

Відтворіть шкідливу поведінку та виділіть незалежні докази.

04 · ОЦІНКА

Ризик та забезпечення

Класифікуйте випадки зловмисної реєстрації, скомпрометованих сервісів, спільного хостингу та ступеня критичності.

05 · ВІДПОВІДЬ

Повідомляти та вживати заходів щодо мінімізації наслідків

Призначте відповідальну особу, встановте терміни виконання та оберіть найменш руйнівний ефективний захід.

06 · ОГЛЯД

Аудит та оскарження

Оприлюднювати метадані про результати, оцінювати вплив та сприяти швидкому виправленню ситуації.

Рівні доказовості

E1 **Неперевірений сигнал**

Один звіт, лексична збіжність або заява щодо репутації. Підходить для спостереження, але сам по собі ніколи не є достатньою підставою для відсторонення.

E2 **Відтворена поведінка**

Запис із позначкою часу, що демонструє викрадення облікових даних, доставку шкідливого програмного забезпечення або шахрайський маршрут транзакції.

E3 **Незалежне підтвердження**

Щонайменше два справді незалежні джерела або одне відтворюване технічне підтвердження, а також перевірка авторства та контексту.

E4 **Кваліфіковане підтвердження**

Компетентний орган, служба, що зазнала впливу, власник бренду або підтверджені докази потерпілого, із дотриманням ланцюга відповідальності, що забезпечує захист конфіденційності.

ПРАВИЛО НЕЗАЛЕЖНОСТІ

Три канали, що копіюють той самий висхідний блок-лист, є одним джерелом, а не трьома. Граф походження та ланцюга збереження доказів має показувати спільне походження, синхронізацію та повторну публікацію постачальником.

11

Мінімальний пакет доказів і сумісний API

Функція «API» повинна створювати перевірену справу та запускати таймер реагування, який підлягає аудиту; репортер не повинен мати можливості безпосередньо видавати команду призупинення. Якщо справа категорії E3/E4 стосується зловмисної реєстрації з єдиною метою і термін її розгляду закінчується без обґрунтованого рішення або ефективних заходів щодо усунення проблеми, система автоматично передає її на розгляд оператору реєстру або іншому суб'єкту, що має договірні чи юридичні повноваження. A `serverHold` Команда може надходити лише від уповноваженого суб'єкта. Автоматичне підвищення рівня доступу та повноваження реєстру щодо дій після закінчення терміну дії є запропонованими змінами до політики, а не твердженнями щодо існуючих повноважень. Кожен перехід між станами підписується та додається до журналу аудиту.

POST /V1/CASES · ПРИКЛАД

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

У разі успішного виконання запиту повертаються ідентифікатор справи, суб'єкт-одержувач, рівень доказів, помилки щодо повноти даних, орієнтовний термін розгляду та публічна URL-адреса для забезпечення прозорості. У відповіді не слід обіцяти конкретні заходи до того, як компетентний суб'єкт оцінить повноваження та побічні наслідки.

12 Пропоновані терміни реагування, а не загальні терміни видалення контенту

Цілі щодо рівня обслуговування повинні бути розділені *подяка*, *сортування*, *рішення* та *ефективне пом'якшення наслідків*. Це дозволяє оцінити ефективність, не виходячи з припущення, що відстрочка завжди є правильним результатом.

ОПИС СПРАВИ	ПІДТВЕРДИТИ	ЦІЛЬ СОРТУВАННЯ	ЦІЛЬ РІШЕННЯ	ТИПОВІ ВАРІАНТИ ВІДПОВІДЕЙ
Крадіжка платіжних облікових даних E3/E4 або початкової фрази під час реєстрації на шкідливому ресурсі, призначеному для однієї мети	15 хв	1 год	4 години	Блок вмісту; блокування реєстратором/реєстром у випадках, коли це дозволено; попередження браузера та щодо оплати.
Фішинг під брендом E3 або розповсюдження шкідливого програмного забезпечення	30 хв	2 години	6 годин	Видалення хоста/CDN, обмеження доступу до домену, перенаправлення на «синкхол» або попередження відповідно до контрольного пункту.
Зламаний легітимний домен або спільний обліковий запис користувача SaaS	1 год	4 години	12 годин	Ізоляція шляху/облікового запису та відновлення доступу власника; за можливості слід уникати блокування зареєстрованого домену.
Фінансове шахрайство з оскаржуваною класифікацією	4 години	12 годин	24 години	Збереження, втручання на рівні платформи/платежів, направлення до компетентного органу та обґрунтоване рішення.
Сигнал E1 або неповний звіт	Авто	24 години	Немає, доки не буде підтверджено	Відстежуйте, доповнюйте та запитуйте докази.

Це орієнтовні показники. Правильні значення слід визначати на основі даних про тривалість існування загроз, чисельність персоналу, вартість помилок та законодавчі обмеження, а потім оприлюднювати у вигляді розподілів досягнутих значень, а не у вигляді одного середнього значення.

13 Безпека, дотримання належних процедур, конфіденційність та варіанти відмови

Швидке реагування без відповідних запобіжних заходів може призвести до того, що недостовірні дані спричинять цензуру, комерційний саботаж або збій у роботі інфраструктури. Тому в належній архітектурі помилкові спрацьовування та побічна шкода розглядаються як серйозні порушення безпеки.

РЕЖИМ ВІДМОВИ	НЕОБХІДНИЙ КОНТРОЛЬ	ПОКАЗНИК, ЩО ПІДЛЯГАЄ АУДИТУ
Недобросовісна скарга на конкурента	Аутентифікація репортерів, репутація джерел, незалежне відтворення інформації та санкції за зловмисне використання технічних засобів	Частота відхилення звітів за авторами; підтверджені випадки маніпуляцій
Циркулярність кормів, що видається за консенсус	Граф походження доказів і усунення дублікатів висхідних джерел	Підрахунок незалежних джерел до та після корекції генеалогічного дерева
Заблоковано легітимний домен, що зазнав злом, у повному обсязі	Класифікація намірів реєстрації та пріоритети заходів щодо пом'якшення ризиків на рівні шляхів	Частка скомпрометованих доменів; легітимні сервіси, що зазнали впливу
Дані про жертв або подробиці експлойтів стали загальнодоступними	Багаторівневе розкриття інформації, вилучення даних, засекречені докази та строки зберігання	Випадки порушення конфіденційності; результати перевірки редагування
Неправомірні дії тривають	Прийом оскаржень 24/7, незалежний рецензент і автентифікований шлях відновлення	Медіана та час розвороту на рівні 95-го процентиля
Блокування в реєстрі спричиняє перебої в роботі електронної пошти/піддоменів	Перелік забезпечення, пропорційність заходів правового захисту та моніторинг після завершення судового розгляду	Кількість порушених послуг на одну дію; коефіцієнт відкату

Мінімальні гарантії дотримання належного процесу

1. Для кожного обмежувального заходу фіксуються код причини, рівень доказовості та особа, яка прийняла рішення.
2. Реєстрант може отримати обґрунтування, що відповідає вимогам щодо захисту персональних даних, та подати протилежні докази.
3. Справи категорії «оскарження» розглядаються особою, яка не приймала початкове рішення.
4. Скасування поширюється тим самим каналом із тим самим знаком, що й початкова дія.
5. Зведені статистичні дані щодо помилок та відновлення є загальнодоступними; доступ до конфіденційних доказів залишається обмеженим.

14 Від «оцінки токсичності» до обґрунтованого індексу якості реагування

Публічний рейтинг реєстратора може сприяти підвищенню підзвітності, проте наївні рейтинги спотворюються через розмір портфеля, охоплення каналів, структуру клієнтської бази, а також через те, чи були домени зареєстровані зловмисно або згодом скомпрометовані. Рейтинг ні в якому разі не може слугувати підставою для колективного блокування всіх клієнтів реєстратора.

ПРОПОНОВАНИЙ ВЕКТОР ЯКОСТІ

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Якщо для управління необхідний зведений показник, перед оцінкою слід встановити вагові коефіцієнти, провести тестування на чутливість та ретроспективне тестування на вибірці, що не брала участі в оцінці. Результати слід розбивати за категоріями «TLD», розміром реєстру, класом загрози та джерелом доказів. Кінцевим результатом є сигнал про відповідальність — а не автоматичний висновок щодо домену.

15 Багаторівнева публічна база даних прозорості DNS Abuse

Реєстр прозорості може усунути суперечки щодо того, чи існувало повідомлення, коли воно було надіслано та які дії було вжито після цього. Однак оприлюднення всіх матеріалів може призвести до розкриття особи жертв, їхніх персональних даних, методів розслідування та активних шляхів експлуатації вразливостей. Виходом із ситуації є багаторівневий доступ.

P

Публічний реєстр

Ідентифікатор справи, індикатор, загальна категорія, ключові часові мітки, рівень доказовості, ролі учасників, код результату, стан «оскарження» та хеші запечатаних артефактів.

C

Перегляд даних контрагента

Докази технічного характеру, що піддаються відтворенню, канал зв’язку, супутній контекст та інструкції щодо збереження.

R

Перегляд з обмеженими повноваженнями

Дані про потерпілих, фінансова атрибуція, матеріали поточних розслідувань та неотредагований ланцюг зберігання доказів.

Кожне оновлення додається лише у кінці запису, має мітку часу та підпис. Виправлення не стирають історію; вони додають новий запис, що замінює попередній. Публічний пошук повинен дотримуватися правил зберігання даних, запобігати масовому виявленню потерпілих та надавати можливість виправлення неточних персональних даних.

16 Шестимісячний пілотний проект із попередньо зареєстрованою оцінкою

Ефективний пілотний проект повинен бути достатньо невеликим, щоб його можна було контролювати, і достатньо великим, щоб перевірити причинно-наслідковий ланцюг. Рекомендований обсяг: три реєстратори-добровольці, два оператори реєстру, один партнер з хостингу/CDN, два незалежних джерела даних для дослідження та кваліфікована група експертів оскарження. Протокол дослідження та визначення результатів слід зареєструвати до розподілу випадків.

1-й МІСЯЦЬ

Протокол та правове відображення

Визначте категорії, уповноважені органи, рівні доказовості, оцінку впливу на конфіденційність та умови припинення.

МІСЯЦЬ 2

Впровадити існуючий процес

Вимірюйте базові часові мітки та результати, не змінюючи поведінку респондентів.

3-й МІСЯЦЬ

Запустити пакет доказів

Запровадити підписане походження доказів, усунення дублікатів і класифікацію супутнього впливу.

4-й МІСЯЦЬ

Цілі для тестових відповідей

Проведіть рандомізацію відповідних випадків або застосуйте поетапне впровадження; щодня відстежуйте помилки.

5-й МІСЯЦЬ

Вправа «оскарження» та невдачі

Проводити навчання з відновлення систем, імітаційні атаки «червоної команди» та аудит засобів контролю доступу.

6-й МІСЯЦЬ

Незалежна оцінка

Опублікуйте величини ефекту, довірчі інтервали, дані про відсутні спостереження, побічні ефекти, витрати та матеріали для відтворення результатів.

Основні результати пілотного проєкту

- Медіана та 90-й процентиль часу від отримання підтверджених даних до вжиття ефективних заходів щодо пом'якшення наслідків.
- Різниця у шкоді, що може бути пов'язана з подією після отримання повідомлення, або заздалегідь визначений показник, що відображає ступінь впливу на потерпілих.
- Частота хибнопозитивних результатів, ступінь тяжкості помилкових дій та медіанний час відновлення.
- Повторення на рівні того самого реєстранта, кластера інфраструктури та шахрайської/фішингової операції.
- Прямі операційні витрати на кожен підтверджений випадок та на кожен ефективний захід щодо пом'якшення наслідків.

ПРАВИЛО ПРИЙНЯТТЯ РІШЕННЯ

Розширювати масштаби слід лише в тому випадку, якщо пілотний проект продемонструє істотно швидше ефективне зменшення ризиків без перевищення заздалегідь встановлених обмежень щодо помилкових спрацьовувань, інцидентів, пов'язаних із порушенням конфіденційності, затримки «оскарження» або побічних перебоїв у роботі сервісів.

17 Висновки та рекомендації, що піддаються перевірці

Реагування на DNS Abuse не є ані суто технічним фільтром, ані проблемою, яку одна установа може розв'язати самостійно. Договірні зміни 2024 року встановили змістовні обов'язки щодо пом'якшення, але залишили значну свободу розсуду стосовно доказів, строків і засобів реагування. Такий розсуд необхідний для пропорційності; без порівнянних записів він водночас ускладнює оцінювання результативності.

1. **Стандартизувати пакет доказів.** Використовувати спільні поля походження доказів, часових міток і результатів для заявників, реєстраторів, реєстрів та інфраструктурних провайдерів.
2. **Вимірюйте етапи окремо.** Публікуйте час підтвердження отримання, сортування, ухвалення рішення, пом'якшення та оскарження за класом загрози й рівнем доказовості.
3. **Відрізняйте зловмисну реєстрацію від компрометації.** Віддавайте перевагу виправленню шляхів доступу/облікових записів у разі порушення безпеки законних сервісів, а заходи на рівні домену застосовуйте лише в тих випадках, коли вони є пропорційними.
4. **Пілотуйте цільові показники реагування.** Перевіряйте погодинні цілі для високонадійно виявлених одноцільових зловмисних реєстрацій замість проголошення універсального строку.
5. **Опублікуйте дані про підзвітність, що забезпечують захист персональних даних.** Використовуйте багаторівневий реєстр прозорості з підписаними історіями та обмеженим доступом до доказів.
6. **Оцініть причинно-наслідковий вплив.** Не ототожнюйте швидше призупинення зі збереженими коштами, доки попередньо зареєстроване дослідження не виміряє наслідки для потерпілих і переміщення загрози на інші канали чи інфраструктуру.

Конструктивний висновок полягає не в тому, що початкова проблема зникає після уточнення її тверджень. Він полягає в тому, що тепер можна перевірити основні твердження: діапазон шкоди після виявлення у 60–85 % є чіткою кількісною гіпотезою; $100–150 — це перевірюване припущення щодо інженерного бюджету для визначеного рівня сенсорів та сортування; а цільові показники реагування в межах години можна випробувати на прикладі високодостовірних, одноцільових зловмисних реєстрацій. Опублікуйте обсяг роботи, витрати, часові мітки та результати, порівняйте їх із базовим рівнем та виміряйте відхилення й похибки. Підтвердження виправдало б зміни в контрактах та політиці; відхилення дозволило б визначити, яке припущення виявилося хибним.

Інформація про редакцію та методи дослідження. PhishDestroy — це незалежний некомерційний проєкт з аналізу загроз. Ця публікація є пропозицією щодо політики та технічних рішень, а не юридичною консультацією, програмою «ICANN» чи рецензованою науковою статтею. Діапазони бюджетів, позначені як «моделі», є плановими припущеннями. Посилання на першоджерела наведено нижче. Поправки можна надсилати через канали зв'язку та відповідального розкриття інформації, зазначені на сайті.

ПОЗИЦІЯ «ВІД ПЕРШОЇ ОСОБИ» · ВІДПОВІДАЛЬНІСТЬ МАЄ ОБМЕЖУВАТИ ЯК БЕЗДІЯЛЬНІСТЬ, ТАК І ПЕРЕВИЩЕННЯ ПОВНОВАЖЕНЬ

Особисті обмеження повноважень щодо забезпечення виконання

Я не прошу — і не хочу — отримати прямий доступ до інструменту блокування доменів. Такі повноваження вимагають незалежного контролю, публічних журналів аудиту, можливості оперативного оскарження та можливості скасування рішень.

Я вважаю, що існує чимало компетентних і відповідальних компаній, яким можна довірити виконання частини цієї роботи. Виходячи зі свого досвіду та опублікованих мною матеріалів, я не відношу компанію «NameSilo» до цієї групи.

Я б не радив легальним американським компаніям доручати відповідальні функції, пов'язані з боротьбою зі зловживаннями або забезпеченням безпеки, конкретним підрядникам, чиї конфлікти інтересів, компетенція чи поведінка не витримують незалежної перевірки. Мова йде про задокументовані дії, а не про громадянство: російське походження саме по собі нічого не доводить, так само як і адреса американської компанії нічого не доводить.

Я хочу справедливості та реальної відповідальності щодо реєстраторів, які отримували дохід від реєстрації та поновлення доменів, задокументованих у рамках неодноразових шахрайських кампаній. У випадках, коли докази вказують не лише на недбалість, а й на можливе свідоме сприяння — чи то у вигляді безпосередньої оперативної участі, чи то у ролі обізнаного посередника, функцією якого було збереження реєстрації та доступності шкідливого домену в мережі попри неодноразові попередження, — така поведінка має бути предметом незалежного розслідування, а в разі підтвердження — тягнути за собою відповідні наслідки. Я не подаю підозри як доведений факт; однак статус посередника не повинен надавати імунітету від перевірки.

Ознайомтеся з матеріалами попереднього розслідування ↗

A

Посилання та примітки щодо джерел

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Джерело даних про 165,1 млн доларів фінансування операцій FY27 і структуру джерел фінансування.

[2] **ICANN, 2024 Global Amendment to the Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Основне договірне джерело щодо обов'язків реєстраторів стосовно DNS Abuse.

[3] **ICANN, 2024 Global Amendment to the Base gTLD Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Основне договірне джерело щодо обов'язків операторів реєстрів із пом'якшення наслідків.

[4] **ICANN Contractual Compliance, DNS Abuse Obligations Advisory (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

Операційне тлумачення, вимоги до повідомлень і приклади належного пом'якшення.

[5] **ICANN, Enforcement of DNS Abuse Mitigation Requirements (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf

Шестимісячний звіт про впровадження, кількість розслідувань і заходів із пом'якшення.

[6] **ICANN SSAC, SAC115: Report on an Interoperable Approach to Addressing Abuse Handling (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf

Відомості про сумісність повідомлень щодо DNS Abuse та якість доказів.

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html

Технічне визначення значень статусу домену EPP, включаючи статус, встановлений сервером.

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html

Офіційна специфікація протоколу та обмеження роботи пристрою «CT» як датчика.

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service

Область дії та модель доступу для файлів зон, що беруть участь у програмі «gTLD».

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Дані щодо скарг та заявлених збитків, включаючи кількість випадків фішингу та спуфінгу.

[11] **Bijmans et al., Catching Phishers By Their Bait (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf

Вимірювання фішингової інфраструктури та тривалості її існування, отримані на основі конкретних наборів даних.

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020

Останні емпіричні дані щодо нещодавно зареєстрованих фішингових доменів та розподілу їхнього терміну існування.

[13] **Inferential Analysis of Maliciously Registered Domains — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

ICANN -фінансований аналіз випадків зловмисних реєстрацій та факторів екосистеми; відповідні обмеження щодо тверджень про причинно-наслідкові зв'язки.

[14] **Chainalysis, 2026 Crypto Scam Trends** · https://www.chainalysis.com/blog/crypto-scams-2026/

Оцінка постачальника щодо обсягів коштів, отриманих в результаті шахрайських операцій в ланцюжку блоків у 2025 році; не враховується в загальному обсязі фішингу доменів.

[15] **APWG, Phishing Activity Trends Report, Q1 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Виявлені фішингові атаки/URL-адреси; ці показники не відповідають кількості унікальних зареєстрованих доменів.

[16] **Cybercrime Information Center / Interisle, Phishing Landscape 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Розрізняє зафіксовані атаки, унікальні домени та домени, зареєстровані з зловмисною метою.

[17] **Verisign, Domain Name Industry Brief, Q2 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Джерело даних про 401,6 млн реєстрацій у всіх доменних зонах.