

22 зі 100: що показала перевірка понад 800 українських сайтів

Безпека, платформи й що з цим робити



Ветеранський кластер України · дані 31.08 – 06.10.2026

Корпоративний сайт зазвичай роблять один раз: замовляють у студії, приймають, платять і забувають. Згадують тоді, коли він «ліг», коли хостер надіслав попередження про спам або клієнт повідомив, що зі сторінки відкривається щось дивне. Ми вирішили подивитися, у якому стані сайти насправді.

ЯК МИ РАХУВАЛИ

Smart Audit працює пасивно: читає лише публічні сторінки, нічого не змінює й не підбирає паролі. Оцінка складається з безпеки, пошукової видимості, швидкості та готовності до ШІ-агентів. Взято **832 унікальні домени**, для кожного остання завершена перевірка. Це не опитування всього бізнесу, а вибірка сайтів, що пройшли через наш сервіс: 671 сайт послуг і B2B, 126 магазинів, 35 медіа. Для середнього корпоративного сайту зріз показовий, для великих компаній із власними ІТ-командами ні.

832

унікальних сайтів у вибірці

22/100

середня оцінка сайту

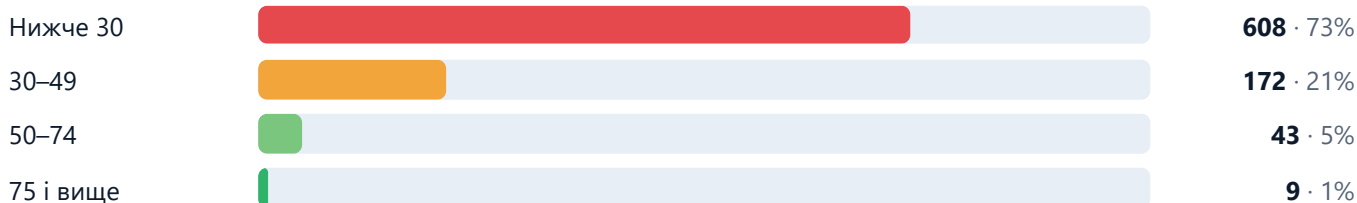
86%

сайтів мають оцінку безпеки нижче 50

1%

набрали 75 балів і більше (9 сайтів)

01 Загальна картина



02 Оцінки за напрямками

НАПРЯМ	СЕРЕДНІЙ БАЛ
Безпека	19
Пошукова видимість	17
Швидкість	18
Готовність до ШІ	57

ПРО ГОТОВНІСТЬ ДО ШІ

Найвищий бал не означає, що сайти готові: перевірка охоплює лише базове. Найчастіше бракує файлу `11ms.txt`, який підказує ШІ-агентам, що є на сайті. Його немає на **89%** сайтів.

03 Безпека: захист, який можна ввімкнути безкоштовно

Найпоширеніші проблеми не потребують складних атак. Це налаштування, які браузер застосовував би сам, якби сервер про них повідомив. Частка сайтів без захисту або зі слабким налаштуванням:

Permissions-Policy: камера, мікрофон, геолокація	93%
Content-Security-Policy: захист від підміни скриптів	90%
Referrer-Policy: що потрапляє в адресу при переході	87%
Захист від вбудовування у чужі сторінки	73%
Заборона вгадування типу файлів (nosniff)	71%
HSTS: примусове HTTPS	62%

Форми й дані відвідувачів

61%

сайтів збирають особисті дані у формах без згоди на обробку

60%

сайтів із формами без захисту від автоматичного спаму

55%

сайтів із формами без захисту від підроблених запитів

Коли сайт сам допомагає атакувальнику

ЗНАХІДКА	САЙТІВ
Cookie встановлюються без захисних прапорців	37%
Сервер видає свою версію програмного забезпечення	28%
Відкриті службові адреси, які не мають бути доступні відвідувачам	19%
Сайт повідомляє точну версію платформи	16%
Форма надсилає особисті дані через адресний рядок	9%
Сертифікат відсутній, недійсний або ось-ось закінчиться	4% + 5%

04 Платформи: де найгірше

ПЛАТФОРМА	САЙТІВ	СЕРЕДНЯ ОЦІНКА
WordPress	201	19
OpenCart	86	11
Бітрікс	18	12
Next.js	28	33
Drupal	7	30
Решта, зокрема власні розробки	474	25

За типом сайту: магазини **14** балів, сайти послуг **23**, медіа **30**. Для магазину ризик подвійний: тут оброблюються замовлення й персональні дані покупців. Вибірка по Drupal, Joomla, Tilda чи Wix нечисленна, тож порівнювати їх із WordPress треба обережно: дані показують, де проблеми поширені, а не «яка платформа гірша».

05 Чому так відбувається



Сайт із чужих деталей

Готова тема, десяток плагінів від різних авторів і адмінка з нечітким розмежуванням прав. Кожен плагін оновлюється в свій час, а одне пропущене відкриває двері всьому сайту.



Ніхто не відповідає

Студія здала проєкт і пішла, хостер дає сервер, але не чіпає код, власник не знає, що оновлювати. Сайт ніби нічий.



Злам непомітний

Рідко ламають заради гучного ефекту. Підкладають приховані посилання, розсилають спам, збирають дані форм. Дізнаються, коли пошуковик уже знизив довіру до домену.

06 Що з цим можна зробити

1

Закрити прості речі. Левова частка знахідок виправляється кількома рядками налаштувань сервера: захисні заголовки, опис сторінок, розміри зображень, згода у формах. Це години, а не місяці.

2

Визначити відповідального. Хтось має знати, на якій версії працює сайт, коли був останній бекап і хто закриє вразливість, якщо вона з'явиться завтра.

3

Переглянути платформу. Якщо сайт тримається на десятках плагінів, захист залежить від дисципліни всіх їхніх авторів. Альтернатива: цілісна система, де безпека закладена в основу й оновлюється одним випуском для всіх.

ВІДПОВІДЬ КЛАСТЕРА

Smart CMS: безпека за замовчуванням

Саме такий шлях ми обрали в кластері. Коли виявили масштаб проблеми на чужих сайтах, постало питання, що пропонуємо партнерам ми самі. Відповіддю стала **Smart CMS**: власна система керування сайтами, яку SmartGT розвиває разом із ветеранами та іншими партнерами кластера й надає клієнтам та учасникам інкубатора.

Найчастіші знахідки нашого аналізу в ній закриті з коробки: політика безпеки вмісту, унікальна для кожного запиту, обмеження браузерних можливостей, примусове HTTPS, заборона вбудовування та вгадування типів файлів. Форми мають згоду на обробку даних, а вхідний текст очищується від шкідливого коду.

Content-Security-Policy	✓	Permissions-Policy	✓
Referrer-Policy	✓	HSTS, nosniff, захист від вбудовування	✓
Згода на обробку даних у формах	✓	Очищення вхідного HTML	✓
Опис, canonical, структурована розмітка	✓	lms.txt для ШІ-агентів	✓

Це не гарантія недоторканності: так не обіцяє жоден чесний інженер. Але це різниця між сайтом, де кожен захист треба налаштовувати й пам'ятати, і сайтом, де вони ввімкнені за замовчуванням. Платформа підходить не лише для візитівок: на ній працюють корпоративні сайти, інтернет-магазини з кошиком і онлайн-оплатою, особисті кабінети, новинні видання та ШІ-консультант. Усе оновлюється централізовано, тож нова вразливість закривається для всіх сайтів одночасно. Сайти кластера, зокрема veterano.media та veterano.info, працюють саме на ній.

07 Як перевірити свій сайт

Найпростіше почати зі звіту. Smart Audit безкоштовний, не потребує доступу до сайту й нічого на ньому не змінює: введіть адресу й за кілька хвилин отримаєте перелік проблем за пріоритетом. Низька оцінка не вирок, а типовий стан сайту без нагляду. Питання лише в тому, дізнаєтесь ви про це зі звіту чи з листа від клієнта.



„Ми почали перевіряти чужі сайти, щоб зрозуміти, з чим працюємо самі, і вийшло, що проблема системна. Сайт перестали сприймати як те, що потребує догляду, і ставляться до нього як до візитки, зробленої раз і назавжди. А це інфраструктура, через яку клієнти залишають заявки й платять. Ми будували Smart CMS разом із партнерами кластера так, щоб безпека була вимогою за замовчуванням, а не опцією, яку треба пам'ятати вмикати. Але головне не в нашій платформі. Перевірте свій сайт сьогодні, поки це зробили ви, а не зловмисник.

Михайло Васянович

CEO SmartGT, координатор AI-інкубатора Ветеранського кластера України, тренер із застосування штучного інтелекту для державних службовців. Спеціалізується на автоматизації бізнес-процесів, інтеграції ШІ та впровадженні Microsoft 365.