Десятиліття в окопах кібервійни

Кібератаки на Україну 2016–2026: хроніка цифрового фронту, де кожен день — нова загроза, а кожна атака — урок стійкості.

2016–2026 | КІБЕРБЕЗПЕКА | НАЦІОНАЛЬНА СТІЙКІСТЬ



2016–2021: Ера системних викликів

Перші масовані атаки

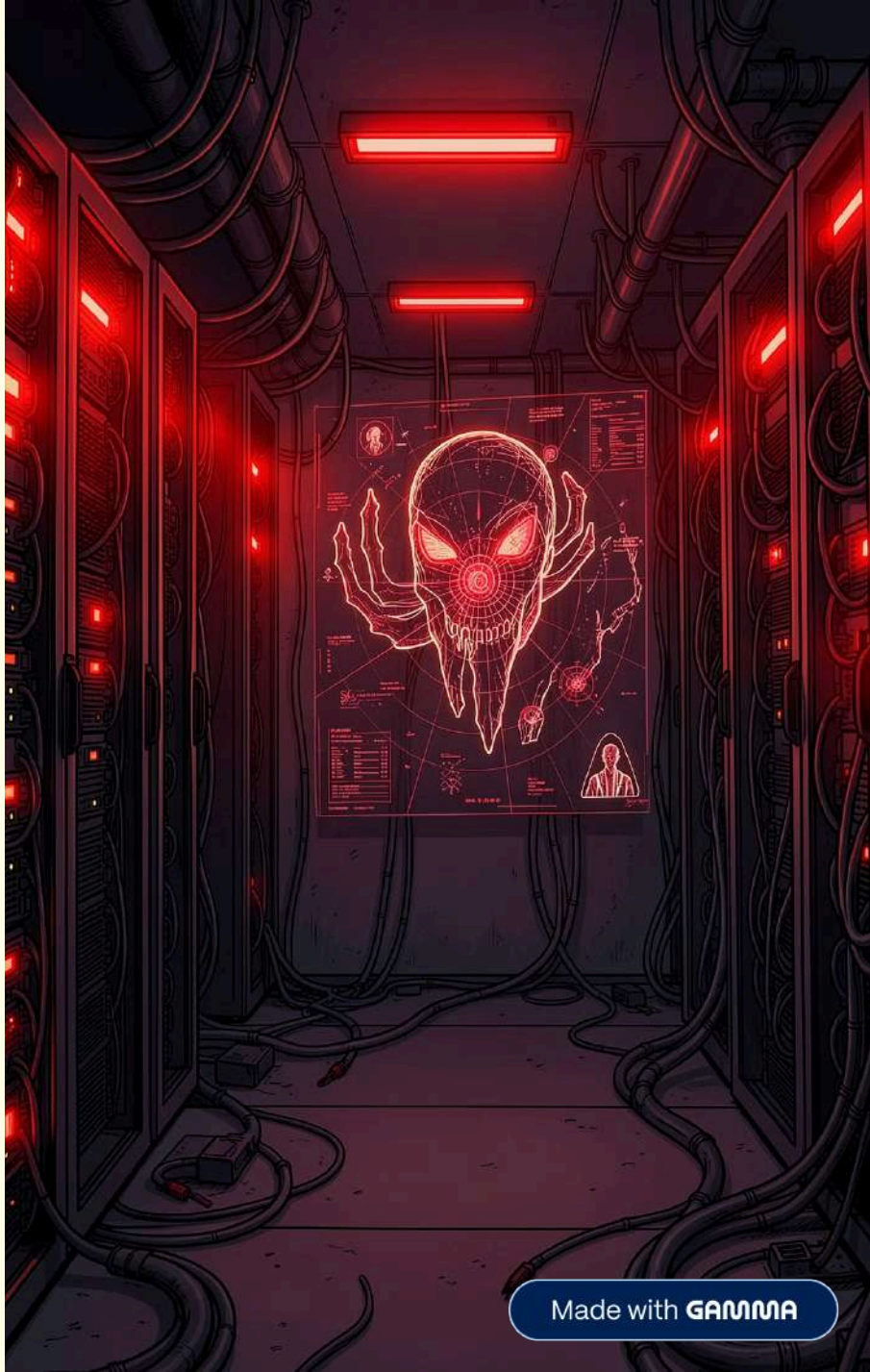
Системні удари по державних ресурсах та об'єктах критичної інфраструктури – від енергетики до банківської системи.

NotPetya (2017)

Найруйнівніший кібератак в історії: вірус-вимагач, що завдав збитків на **$10 млрд** по всьому світу. Створений для України – вдарив по всій планеті.

Атаки на виборчі системи

ЦВК та виборча інфраструктура стали мішенню для спроб впливу на демократичні процеси через DDoS та втручання в бази даних.



2022: Кіберфронт повномасштабного вторгнення



🎯 Синхронізація ударів

Кібератаки координувалися з ракетними обстрілами – цифровий та фізичний фронти діяли як єдиний механізм.

🕵️ Шпигунська експансія

Масовані операції проти Сил оборони: спроби викрадення даних, дезінформація, компрометація каналів зв'язку.

⚡ Енергосистема під ударом

Кіберпростір використано для дестабілізації енергетичної інфраструктури в поєднанні з фізичними атаками.

Made with GAMMA

Еволюція тактики: від шпигунства до хактивізму

За десятиліття ворог змінив не лише інструменти, а й саму філософію кібернаступу.



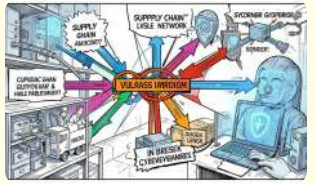
APT-групи

APT28, Gamaredon – професійні підрозділи спецслужб РФ. Цілеспрямовані, терплячі, добре фінансовані. Діють роками, непомітно.



Масовий хактивізм

Група **NoName057(16)** – тисячі атак на день. Дешевий, але ефективний інструмент тиску через масовість.



Supply Chain атаки

Удар через партнерів та постачальників ПЗ. Один компрометований ланцюг – сотні жертв одночасно.

Made with GAMMA

Масштаб загрози: 2023–2024 роки

10+

Атак на день

За словами голови СБУ Василя Малюка — мінімальна щоденна інтенсивність кібератак

1,042

Підтверджених інцидентів

Лише через систему CIROC за один рік — реальна картина кіберзагроз

100B+

Подій телеметрії

Сотні мільярдів телеметричних подій оброблено для захисту інфраструктури у 2024 році

Ці цифри відображають лише **виявлені та підтверджені** інциденти. Реальна кількість атак може бути значно вищою.

Made with GAMMA

Економічний та соціальний вимір



Фінансові втрати

Атаки на банківську систему призвели до прямих збитків. Відомий кейс – спроба викрадення **1,5 млн грн** через компрометацію платіжних систем.

Крадіжка даних

Supply chain-атака на інтернет-магазин НБУ – масова компрометація персональних даних клієнтів через стороннього постачальника.

Фішинг як зброя

Маскування під **Ощадбанк** та **Укренерго**: фальшиві повідомлення про виплати використовувалися для викрадення облікових даних.

Made with GAMMA

2025–2026: Нова реальність

📊 1,651 інцидент

Кіберінцидентів зафіксовано проти України лише за останній рік — рекордна інтенсивність загроз.

🛡️ Кіберстрахування

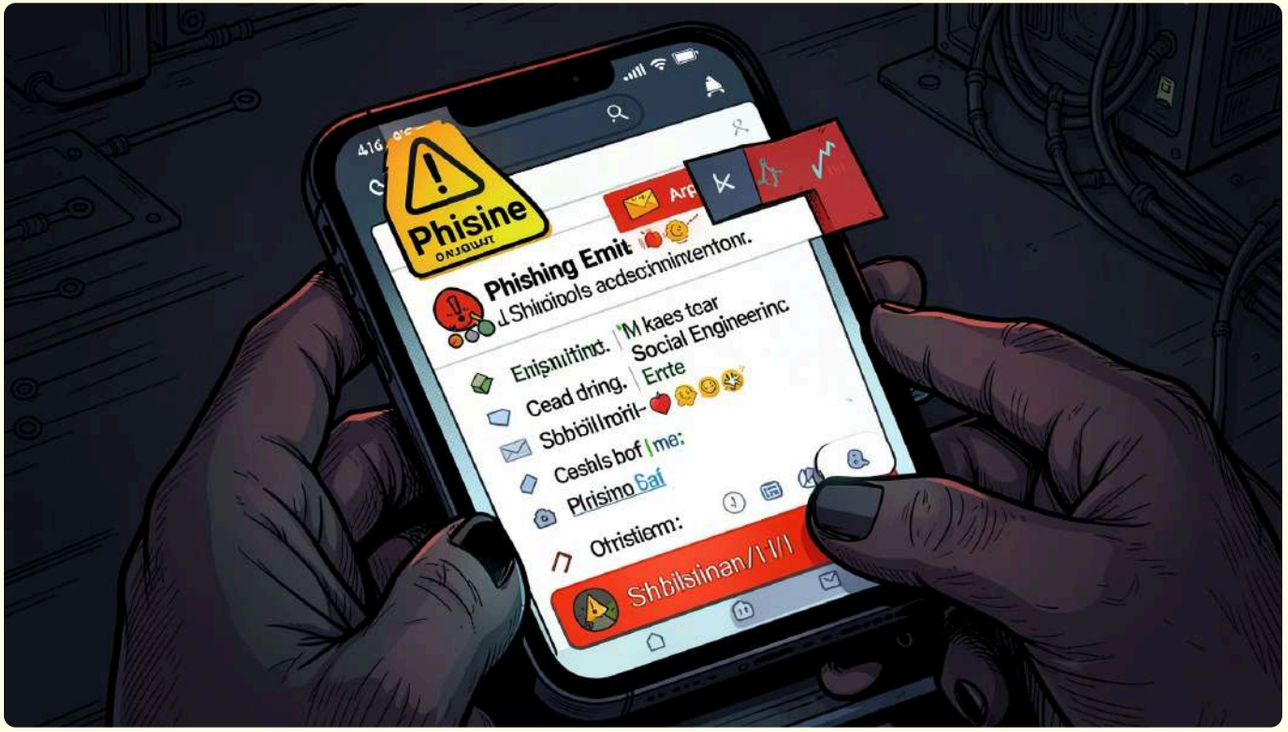
Зростання ролі кіберстрахування та системного захисту приватного сектору як критичної інфраструктури.

⚔️ Асиметрична відповідь

Успішні хак-інфільтрації в **Міноборони РФ** та доксинг офіцерів ФСБ — Україна перейшла в активний кібернаступ.



Анатомія сучасного фішингу



1 Маскування під довірені джерела

Зловмисники видають себе за **НАБУ, МВС, благодійні фонди** – організації, яким жертви довіряють беззаперечно.

2 Психологічний тиск через месенджери

Соціальна інженерія в Telegram та Viber: терміновість, страх, авторитет – тригери для миттєвої реакції без роздумів.

3 Приховані шкідливі архіви

Нова тактика: ZIP-файли під паролем, що **обходять автоматичний сканінг** поштових систем безпеки.

Made with GAMMA

Уроки десятиліття

Кібербезпека = національна стійкість

Захист цифрового простору став невід'ємною частиною оборонної доктрини держави.

Threat Intelligence — основа випередження

Аналіз тактик, технік і процедур ворога дозволяє передбачати атаки до їх реалізації.

Від захисту до активної оборони

Міжнародна співпраця, спільні операції та обмін розвідданими — ключ до протидії загрозам.

Made with GAMMA



Стійкість як наша відповідь

Десятиліття кібервійни не зламало Україну — воно загартувало її.

🔧 Технологічна адаптація

Багаторівневі системи виявлення інцидентів, AI-аналітика та автоматизоване реагування.

🌐 Готовність до майбутнього

Захист інформаційного простору — обов'язок кожного: від держави до кожного громадянина.

🏆 Глобальний центр експертизи

Україна стала світовим полігоном реальної кібервійни — і лідером у виробленні практичних рішень.

> «Той, хто вижив у десяти роках кібервійни, знає: найкращий захист — це знання, готовність і єдність.»

Made with GAMMA