

Кібератаки на державні структури України

Від викликів до незламності

Як Україна перетворила кібервійну на урок для всього світу

Made with GAMMA



КОНТЕКСТ

Україна як полігон кібервійни

З 2014 року

Україна стала ідеальним майданчиком для випробування нових видів кіберзброї – першою в світі зазнала масштабних державних кібератак.

Тисячі атак щомісяця

Від енергетичного сектору до державних реєстрів – жодна критична система не залишилась поза увагою агресора.

Стратегічна мета

Дестабілізація через руйнування даних та дискредитацію влади – кібератаки як інструмент гібридної агресії.

Made with GAMMA

КЕЙС

Січень 2022: Масштабна атака на держресурси



70 сайтів за одну ніч

Сайти органів влади виведено з ладу в результаті скоординованої атаки на державну інфраструктуру.

Ключові цілі

Постраждали Дія, Кабінет Міністрів, МЗС та інші ключові відомства – атака мала демонстративний характер.

Метод атаки

Використано вразливість **October CMS** для дефейсу та приховування шкідливого ПЗ, що знищує дані.

Made with GAMMA

АНАЛІЗ ЗАГРОЗ

Еволюція кіберзагроз

Кібератаки пройшли шлях від хаотичних спроб до високоорганізованих операцій державного рівня.

1

Випадкові атаки

Поодинокі спроби злому без чіткої стратегії та координації

2

Цілеспрямовані операції

Скоординовані багатовекторні атаки для обходу сигнатурних систем захисту

3

Зброя масового знищення

Складне ПЗ, створене для систематичного знищення критичної інформації

Made with GAMMA

ЗАХИСТ

Національна система захисту: Хто стоїть на варті



Єдина система реагування

Синергія міжвідомчої взаємодії забезпечує комплексний захист державного цифрового простору.

- **РНБО** – стратегічне управління національною кібербезпекою
- **Держспецзв'язку та CERT-UA** – оперативне реагування на інциденти
- **СБУ, Нацполіція, Міноборони** – протидія кіберзагрозам на всіх рівнях

Made with GAMMA

СТАТИСТИКА 2024

Масштаб операційної діяльності у 2024 році

сотні млрд

Подій телеметрії

Опрацьовано аналітиками ОЦРК для виявлення аномалій та загроз

·3 млн

Подій ІБ

Зафіксовано подій інформаційної безпеки за рік

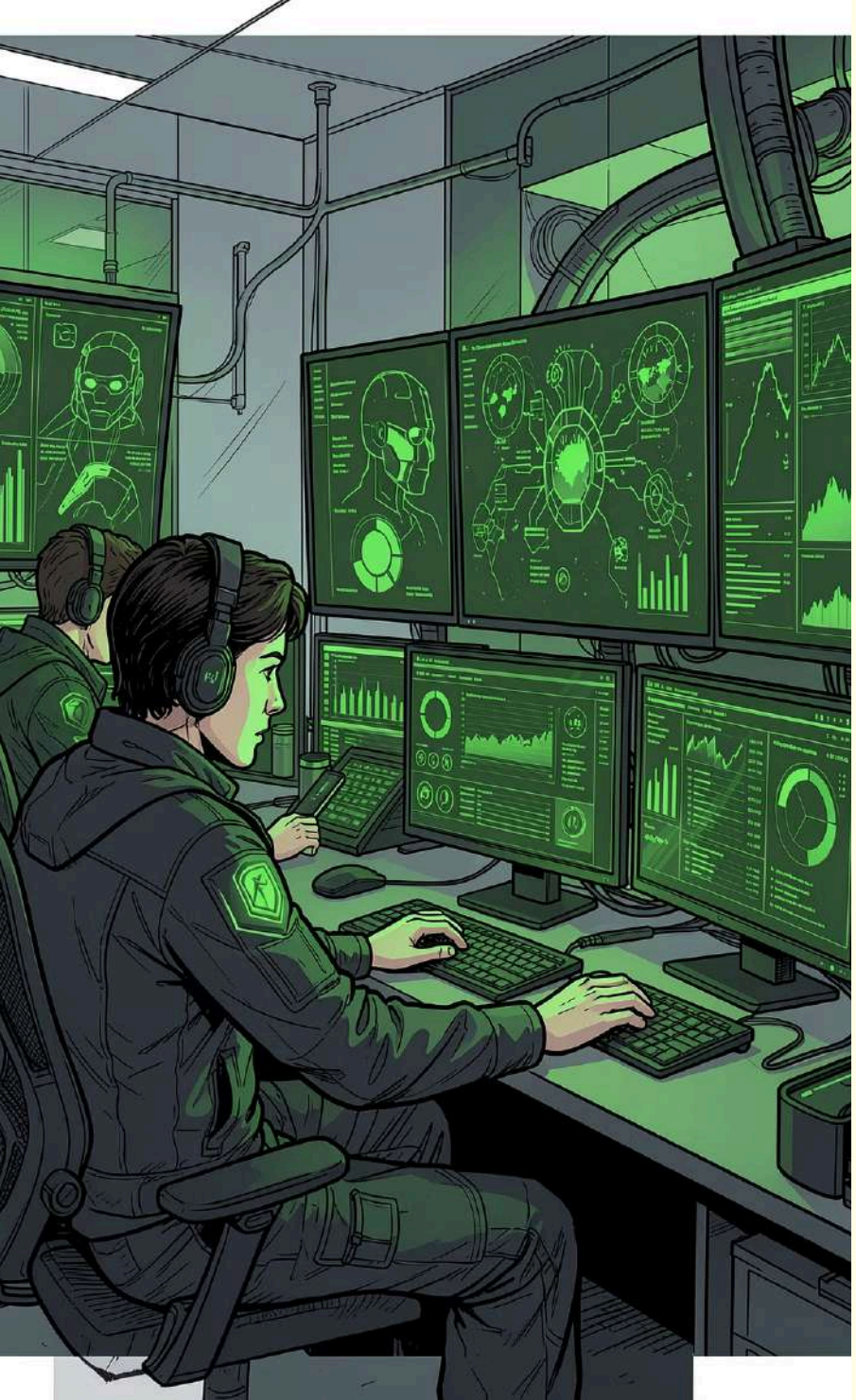
28 000

Критичних інцидентів

Аналітики ОЦРК оперативно втрутились у кожну критичну загрозу

Операційний центр реагування на кібератаки (ОЦРК) забезпечує цілодобовий моніторинг та миттєве реагування на загрози державного рівня.

Made with GAMMA



РЕЗУЛЬТАТИ

Успіхи систем реагування

Швидкість реагування

Значне скорочення часу на виявлення та нейтралізацію загроз у 2025 році завдяки автоматизації та AI.

Прозорість

Підвищення довіри через публікацію звітів про стан кібербезпеки державних реєстрів.

Цілісність систем

Посилення контролю над цілісністю державних інформаційних систем та реєстрів населення.

Made with GAMMA

УРОКИ

Уроки кібервійни: Чому захист став пріоритетом



1 Периметр безпеки — там, де користувач

Переосмислення підходу: захист має слідувати за даними, а не обмежуватися корпоративною мережею.

2 Гармонізація законодавства

Важливість міжнародної співпраці та узгодження стандартів кібербезпеки з нормами ЄС та НАТО.

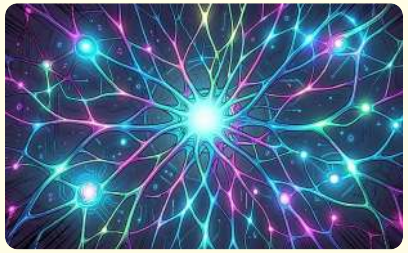
3 Кадровий резерв

Формування професійної спільноти фахівців з кіберзахисту — стратегічний ресурс держави.

Made with GAMMA

ПОГЛЯД У МАЙБУТНЄ

Виклики майбутнього



Протидія невідомим атакам

Загрози постійно змінюють поведінкові шаблони — традиційні сигнатурні методи вже недостатні.



Захист критичної інфраструктури

Об'єкти енергетики, транспорту та зв'язку потребують гіпердинамічного захисту від цілеспрямованих атак.



Штучний інтелект у захисті

Інтеграція AI в системи виявлення вразливостей дозволить реагувати на загрози швидше за агресора.

Made with GAMMA

ВИСНОВОК

Кіберстійкість як наш новий стандарт

> Україна перетворює болючий досвід кібератак на глобальний стандарт захисту – урок для всього демократичного світу.

🔍 Моніторинг

Постійне відстеження загроз у реальному часі

💡 Інновації

Розвиток передових технологій захисту

📋 Підзвітність

Прозорість і довіра як основа цифрової безпеки

