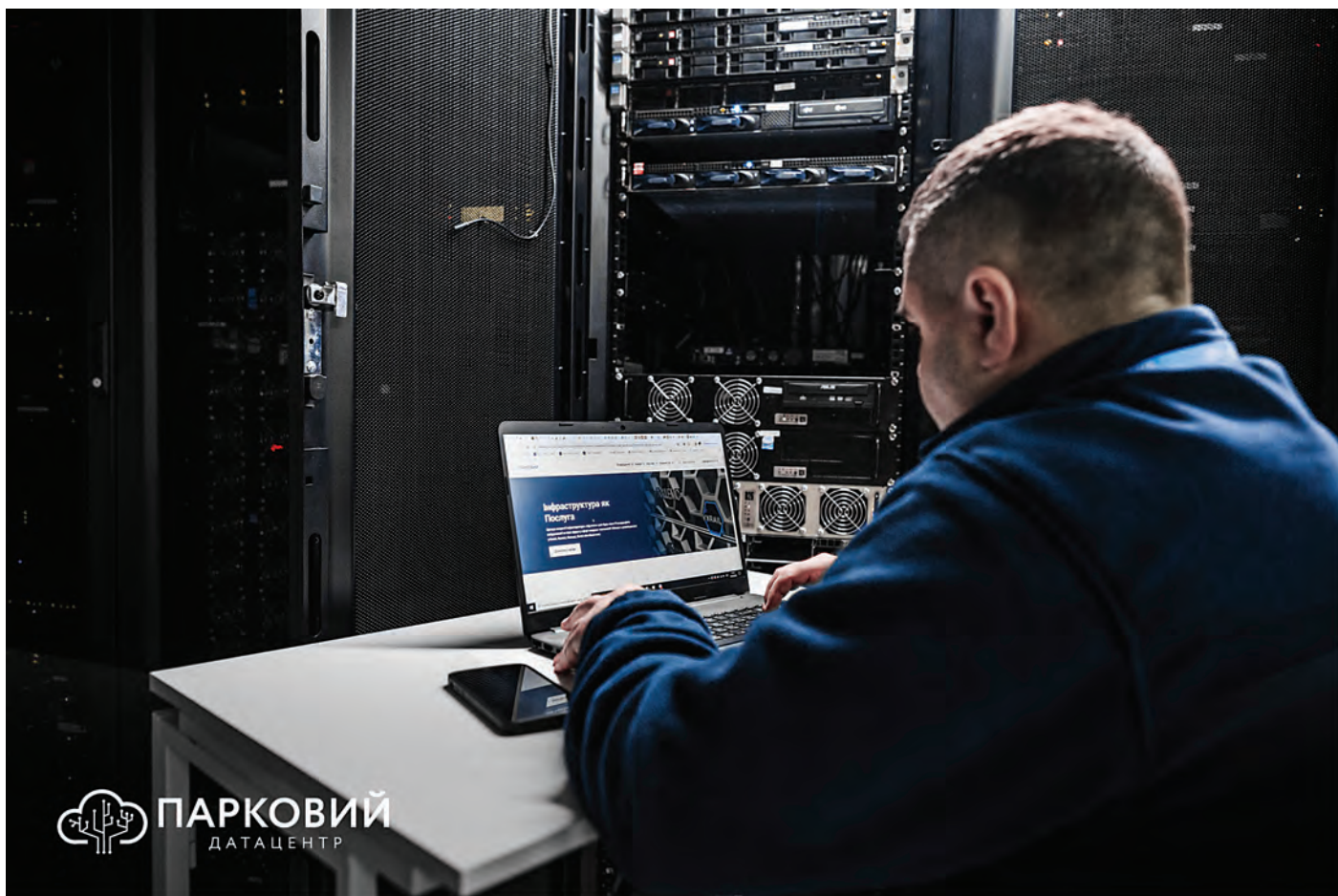


# АКТИВНА ФАЗА

## наймасштабнішої кібервійни 21 століття

Понад 2 роки від початку повномасштабного вторгнення. Ми неухильно продовжуємо виборювати своє право на незалежність, стабільність і безпеку. Сьогодні немає жодного українського міста, яке б не брало безпосередню участь в цій війні, а столиця України – Київ – знаходиться на передовій у наймасштабнішій кібервійні 21 століття.



**ПАРКОВИЙ**  
ДАТАЦЕНТР

Упродовж 2023 року українські аналітики безпеки зафіксували та обробили 1105 кіберінцидентів, повідомляє Держспецзв'язку. Це на 62,5% більше, ніж у 2022 році.

Нещодавно речник Головного управління розвідки Міноборони Андрій Юсов уточнював, що росія на 2024 рік інвестує значні ресурси у кібервійну, аби завдавати шкоди українській економіці. «Ворог спеціально намагається залучити в кібервійська великий ресурс, тому що подібні атаки можуть потенційно завдати більшої шкоди економіці нашої держави, ніж [якщо] інвестувати гроші на лінію фронту... Це більш вигідно для агресора», – зазначив він.

І вже сьогодні ми всі відчуваємо загострення інтенсивності і кількості кібератак на бізнес і критичну інфраструктуру

України. «Київстар», «Монобанк», Держспецзв'язку, «Укрзалізниця», Міносвіти, ресурси Міноборони — загалом мінімум 15 найбільших держустанов та приватних бізнесів зазнали різного виду та інтенсивності кібератак тільки за перші 2 місяці цього року (інформація надана згідно даних із відкритих джерел і ЗМІ за допомогою моніторингу).

**На передовій у кібервійні з ворогом, у якого на меті тільки одне: тотальне знищення**

В кінці січня на сервіси Датацентру «ПАРКОВИЙ» було здійснено масовану кібератаку. Операція такого рівня підготовки та виконання проводилась проти українського комерційного ЦОД уперше. Об'єктом атаки

стали хмарні сервіси датацентру. У перші ж години ми локалізували загрозу і повернули роботу мережевої інфраструктури. Далі — відновлення з бекапів і удосконалення всієї наявної хмарної інфраструктури. Це був технологічно і процедурно важкий крок, але він може протистояти можливим кібератакам подібного характеру в майбутньому.

Обладнання клієнтів, що зберігалось локально в ЦОД, і вся інженерна екосистема працювали безперебійно та витримали кібератаку без будь-яких наслідків. На прикладі відбитої кібератаки нам всім зрозуміло, наскільки наявні сертифікати ISO 27001 в найновішій редакції 2022 року, а також 9001 та TIER III допомогли нам процедурно та технологічно нівелювати перебіг і результат цієї атаки.

За фактом кіберінциденту триває розслідування, яке здійснюється Департаментом кіберполіції Національної поліції України та департаментом кібербезпеки СБУ з залученням CERT-UA від Держспецзв'язку. Відомості досудового розслідування ми поки не розголошуємо. Але вже зараз можна повідомити, що головною метою атаки було саме знищення всіх даних і їх резервних копій. **Але з цим нападники не впорались. Як результат — нами встановлено, що дані не скомпрометовано і витоку інформації клієнтів не відбулося.**

## Що далі?

Окрім вдосконалення хмарної інфраструктури та впровадження додаткових рішень для унеможливлення подібних атак у майбутньому, ми продовжуємо активно доповнювати й інтегрувати сценарії роботи з обов'язковою двофакторною автентифікацією та навчанням з кібербезпеки. На додачу залучаємо поведінковий аналіз з елементами соціальної інженерії з відстеженням геодоступу для виявлення та своєчасного попередження кіберзагроз.

“ Це все у парі з іншими алгоритмами захисту допоможе клієнту відчувати себе в безпеці, а нам — бути впевненими, що ми нівелюємо вплив зовнішніх факторів та забезпечуємо максимальний рівень кіберзахисту.



**Сергій ЗАБІРКА**, технічний директор Датацентру «ПАРКОВИЙ»

Як додатковий стимул на шляху до посилення кіберзахисту наших клієнтів ми пропонуємо персоналізовані сервіси кібербезпеки «з коробки» від передових гравців цієї галузі — Cisco і Microsoft. Найпопулярніші з них представлені в калькуляторі на нашому сайті, за допомогою якого ви зможете підібрати необхідний сервіс і відразу побачити попередній розрахунок. До того ж при підключенні цих сервісів ми безоплатно додаємо всім клієнтам 1 місяць бекапування засобами Veeam\*.

Щоб додатково посилити кіберстійкість українського бізнесу ми маємо на меті максимально залучити наш досвід відбиття кібератаки подібного рівня для допомоги нашим клієнтам, партнерам та іншим гравцям ринку ЦОД та хмарних сервісів.

“ Ключовий фокус у діяльності нашої компанії на 2024 рік — це підтримка сталого функціонування і розвитку критичної інфраструктури та українського бізнесу. Крім розвитку і посилення кіберстійкості України, ми працюватимемо разом з відповідними державними структурами і поділимося своїм досвідом з відбиття кібератак подібного масштабу. Ми зацікавлені розповісти бізнесу та держустановам про інструменти, які допомогли та допоможуть ефективно протистояти подібного роду операціям у майбутньому.



**Володимир ПОКАТИЛОВ**, директор Датацентру «ПАРКОВИЙ»

## Ключовий індикатор сталості та розвитку під час кризових ситуацій — це єдність

Вся команда датацентру дякує за бездоганну роботу та непохитну підтримку фахівцям Кіберполіції, Національного координаційного центру кібербезпеки Апарату РНБО, Генеральної прокуратури України, співробітникам кібербезпеки СБУ, Держспецзв'язку, Dell, Cisco, Microsoft, CyberLab, Vixen.Uno та інших партнерів і гравців ринку хмарних сервісів.

“ Вся наша команда безмежно вдячна за підтримку і допомогу від усіх без винятку клієнтів за стійкість та максимальну залученість в усі процеси з подолання наслідків кібератаки. Окремо дякуємо нашим клієнтам і колегам, які користуються послугами нашої приватної хмари, за співпрацю та ідеально відпрацьовані алгоритми подолання загроз.



**Алла КИТАЄВА**, комерційна директорка Датацентру «ПАРКОВИЙ»

Більше про сервіси  
Датацентру «ПАРКОВИЙ»  
на сайті [datapark.ua](http://datapark.ua)  
або за телефоном  
+38 (044) 377-77-77.



\* Під безкоштовним бекапом даних засобами Veeam розуміється надання послуги з резервного копіювання даних (BaaS) в Україні або ЄС на 1 місяць з об'ємом даних, який не перевищує 10 Тб. Детальніше — на сайті [datapark.ua](http://datapark.ua)