ДЕРЖАВНИЙ ЦЕНТР КІБЕРЗАХИСТУ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

2025

РІЧНИЙ ЗВІТ

СИСТЕМА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

TLP: CLEAR

СИСТЕМА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

це сукупність програмних та програмно-апаратних засобів, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об’єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування.

ПІДСИСТЕМА ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

є центральною складовою Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та забезпечує:

- централізоване управління всіма підсистемами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки;
- централізований збір та накопичення інформації про мережеві події інформаційної безпеки;
- проведення моніторингу та оброблення в режимі реального часу кіберзагроз та кіберінцидентів.

Підсистема оперативного центру реагування на кіберінциденти виявляє шкідливу активність, а також системні й мережеві аномалії на об’єктах кіберзахисту шляхом аналізу даних, отриманих з мережевих пристроїв (активні сенсори, міжмережеві екрани, сканери вразливостей), робочих та серверних станцій, систем авторизації, внутрішніх і зовнішніх джерел даних про кіберзагрози.

СТАТИСТИКА МОНІТОРИНГУ

ОПИС ПІДСИСТЕМ, ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ

Протягом 2025 року до підсистеми збору телеметрії інформаційно-комунікаційних систем (NDR) було підключено 24 нових організацій, яким надано комплекти обладнання для моніторингу мережевого трафіку.

Водночас до підсистеми захисту кінцевих точок підключено 97 організацій, у результаті чого в межах СВВ здійснюється моніторинг понад 46,5 тисяч робочих станцій і серверів.

Технології та інструменти

Засоби кіберзахисту

Підсистема збору телеметрії	Підсистема захисту кінцевих точок	Підсистема захисту кінцевих точок
NDR	**EDR**	**MDR**
Підключено організацій: **92**		Підключено організацій: **97 +39**
Встановлено сенсорів: **93 +24**	Захищено хостів (EDR): **~14,5 тис**	Захищено хостів (MDR): **~32 тис**

Основні зусилля були зосереджені на розвитку та масштабуванні функціональних можливостей Системи виявлення вразливостей і реагування на кіберінциденти (СВВ), зокрема на розширенні покриття моніторингу мереж та кінцевих точок, підвищенні якості збору телеметрії та удосконаленні механізмів централізованого аналізу подій інформаційної безпеки.

💡 ПРИМІТКА

Цей звіт ґрунтується на статистичних даних Оперативного центру реагування на кіберінциденти Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки з 1 січня 2025 року по 31 грудня 2025 року включно.

КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ КІБЕРІНЦИДЕНТІВ

Кіберінциденти та кібератаки

17,3 тис
Події безпеки

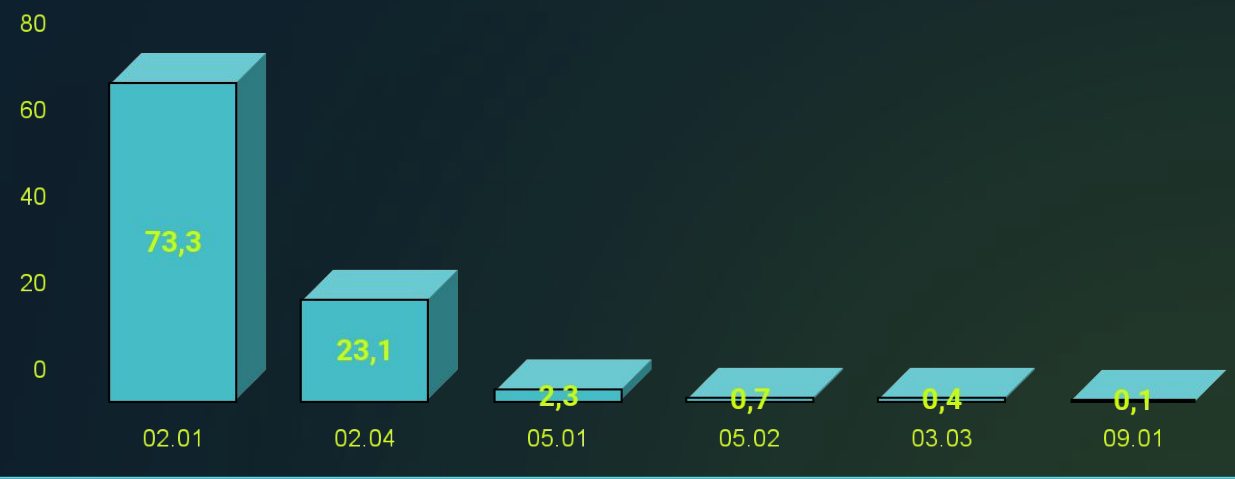
SIEM

730
Кіберінцидентів

Упродовж 2025 року Оперативним центром реагування на кіберінциденти опрацьовано 17,3 тисяч подій безпеки та зафіксовано 730 кіберінцидентів різного рівня складності. Найбільшу частку серед них становили кіберінциденти, пов'язані з використанням шкідливого програмного забезпечення. Аналіз виявлених атак свідчить, що їх ключовою метою було встановлення прихованого контролю над інформаційними системами з подальшим використанням отриманого доступу для кіберрозвідки або незаконного заволодіння фінансовими ресурсами.

! Варто зауважити, що переважна більшість тактик і технік, які зловмисники застосовують як початковий вектор атаки, втрачають ефективність у разі використання непривілейованих облікових записів користувачів та впровадження базових налаштувань безпеки на робочих станціях.

Відсотковий розподіл за типами кіберінцидентів



02.01 - зараження ШПЗ, 02.04 - шкідливе підключення, 05.01 - компрометація облікового запису, 05.02 - компрометація системи, 03.03 - фішинг, 09.01 - вразливість.

КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Кіберінциденти та кібератаки

730
Кіберінцидентів

339
Кібератак

Серед кіберінцидентів і кібератак, зафіксованих Оперативним центром реагування на кіберінциденти, 339 були ідентифіковані як такі, що пов'язані з відомими кластерами кіберзагроз. За результатами аналізу активності у 2025 році найбільш інтенсивну діяльність демонстрували кластери UAC-0010, UAC-0006 та UAC-0050.

UAC-0010

Псевдоніми:
Gamaredon, Primitive Bear, Trident Ursa, Aqua Blizzard

Відслідковується з:
2013 року

Мотивація:
кібершпигунство

Цілі кібератак:
державні органи, сили оборони

UAC-0006

Псевдоніми:
Відсутні

Відслідковується з:
2013 року

Мотивація:
викрадення коштів

Цілі кібератак:
фінансові підрозділи організацій

UAC-0050

Псевдоніми:
Відсутні

Відслідковується з:
2020 року

Мотивація:
кібершпигунство, викрадення коштів, ІПСО

Цілі кібератак:
державні органи, сили оборони, фінансові установи

РЕКОМЕНДАЦІЇ

Для підвищення рівня кіберзахисту ІКС вашої організації пропонуємо скористатися сервісами кіберзахисту, що функціонують в межах Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, щодо виявлення кіберзагроз в реальному часі й управління кіберінцидентами.

NDR	Сервіс передбачає встановлення та налаштування мережевого сенсора для моніторингу мережевого трафіку і виявлення кіберінцидентів та кібератак. Сенсор може бути встановлений як всередині мережі, так і на її периметрі.
EDR	Сервіс передбачає комплексний захист кінцевих точок вашої організації (персональні комп'ютери, сервери, віртуальні машини) за допомогою встановлення та налаштування на них технології EDR.
MDR	Сервіс передбачає централізований збір, кореляцію та аналіз журналів подій із наявних в організації засобів захисту кінцевих точок (EDR/AV) з метою своєчасного виявлення ознак компрометації, реагування на кіберінциденти та підвищення загального рівня захищеності кінцевих точок.

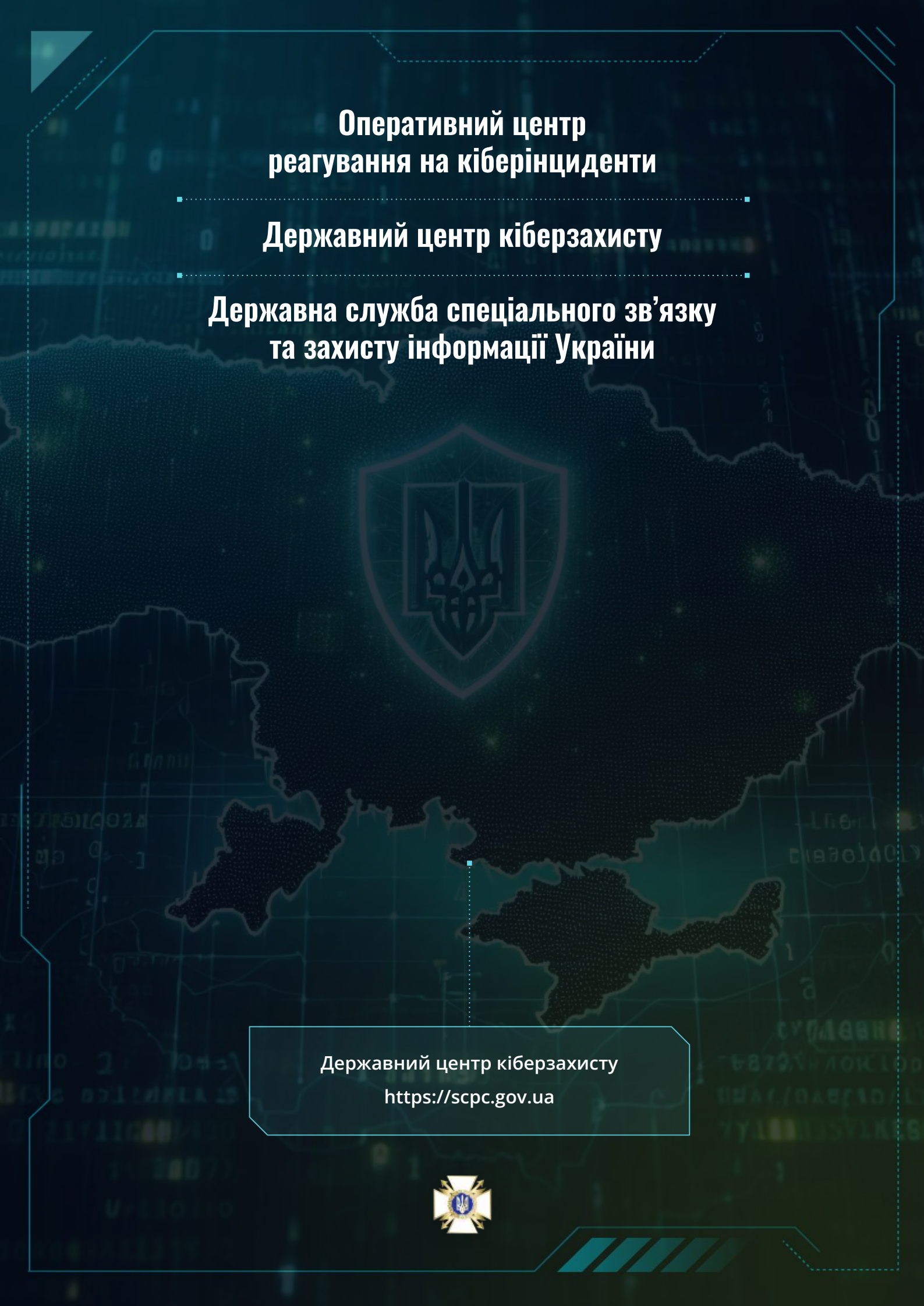
Для зв'язку з Державним центром кіберзахисту щодо підключення вищезгаданих сервісів:

Email: `info_scpc@cip.gov.ua`

Оперативний центр реагування на кіберінциденти

Державний центр кіберзахисту

Державна служба спеціального зв'язку та захисту інформації України



Державний центр кіберзахисту

https://scpc.gov.ua