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

2025

І ПІВРІЧЧЯ

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.

ВСТУП

Звіт за перше півріччя 2025 року є деталізованим описом результатів функціонування Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (далі - СВВ) на виконання Постанови Кабінету Міністрів України від 23 грудня 2020 року № 1295, якою була визначена необхідність створення та функціонування такої системи в рамках захисту країни від кібернетичних загроз.

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки є важливим інструментом для забезпечення безпеки і стабільності інформаційного простору України. Протягом першого півріччя 2025 року, в рамках функціонування СВВ здійснювався постійний моніторинг кіберпростору, як результат – було виявлено низку кіберінцидентів та кібератак, а також було здійснено відповідні заходи щодо реагування на виявлені кіберінциденти та кібератаки фахівцями Оперативного центру реагування на кіберінциденти (далі - ОЦРК).

В рамках звіту будуть представлені статистичні дані та ключові події, які відбулися протягом першого півріччя 2025 року, а також описані кластери кіберзагроз та заходи, що були вжиті для протидії кіберінцидентам та кібератакам.

💡 **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 30 червня 2025 року включно.

КЛЮЧОВІ ВИСНОВКИ

У першій половині 2025 року Система виявлення вразливостей і реагування на кіберінциденти та кібератаки забезпечила обробку мільярдів подій телеметрії та виявлення мільйонів подій інформаційної безпеки.

Таких результатів вдалося досягти завдяки безперервному моніторингу активності в інформаційно-комунікаційних системах із застосуванням засобів мережевого виявлення загроз, аналізу даних із систем захисту кінцевих точок та використання розвідданих про кіберзагрози.

У результаті аналізу виявлених подій було ідентифіковано та опрацьовано 535 кіберінцидентів. Більшість із них були пов’язані з інфікуванням шкідливим програмним забезпеченням. Основною метою таких атак, як правило, було отримання несанкціонованого віддаленого доступу до інформаційних систем для проведення кіберрозвідки або викрадення коштів.

1. Зловмисники дедалі частіше використовують комбіновані вектори атак, поєднуючи соціальну інженерію, фізичний доступ (через флеш-носії) та інфікування неліцензійним програмним забезпеченням, що ускладнює виявлення на ранніх етапах.

2. Електронна пошта залишається найбільш використовуваним каналом для розповсюдження шкідливого програмного забезпечення, підтверджуючи її роль як основного вектора первинного доступу в атаках більшості активних кластерів.

3. Найбільш активними у першій половині 2025 року були кластери кіберзагроз UAC-0010, UAC-0050 та UAC-0202 згідно з класифікацією CERT-UA.

СТАТИСТИКА МОНІТОРИНГУ

ОПИС ПІДСИСТЕМ, ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ

Протягом І півріччя 2025 року до підсистеми збору телеметрії ІКС (NDR) було підключено 11 нових організацій, які отримали 11 комплектів обладнання сенсорів для моніторингу мережі. До підсистеми захисту кінцевих точок (EDR) підключено 11 організацій, таким чином на моніторингу СВВ перебуває понад 40 тисяч робочих станцій і серверів. До сервісу управління поверхнею атаки (ASM) підключено 12 організацій.

Технології та інструменти

Засоби кіберзахисту

Підсистема збору телеметрії	Підсистема захисту кінцевих точок	Управління поверхнею атаки
NDR	**EDR**	**ASM**
Підключено організацій: **78+11**	Підключено організацій: **69+11**	Підключено організацій: **50+12**
Встановлено сенсорів: **80+11**	Захищено хостів: **40 тис.**	Скановано активів: **4 тис.**

Сектори та організації

Об'єкти кіберзахисту

47 Урядові організації	**39** Місцеві органи влади	**9** Стратегічні підприємства
8 Сектор безпеки та оборони	**5** Енергетичний сектор	**3** Фінансовий сектор
4 IT сектор	**3** Медицина	**2** Освіта та наука

КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ КІБЕРІНЦИДЕНТІВ

Загальна інформація

535

Протягом І півріччя 2025 року аналітиками ОЦРК зареєстровано та опрацьовано кіберінцидентів та кібератак

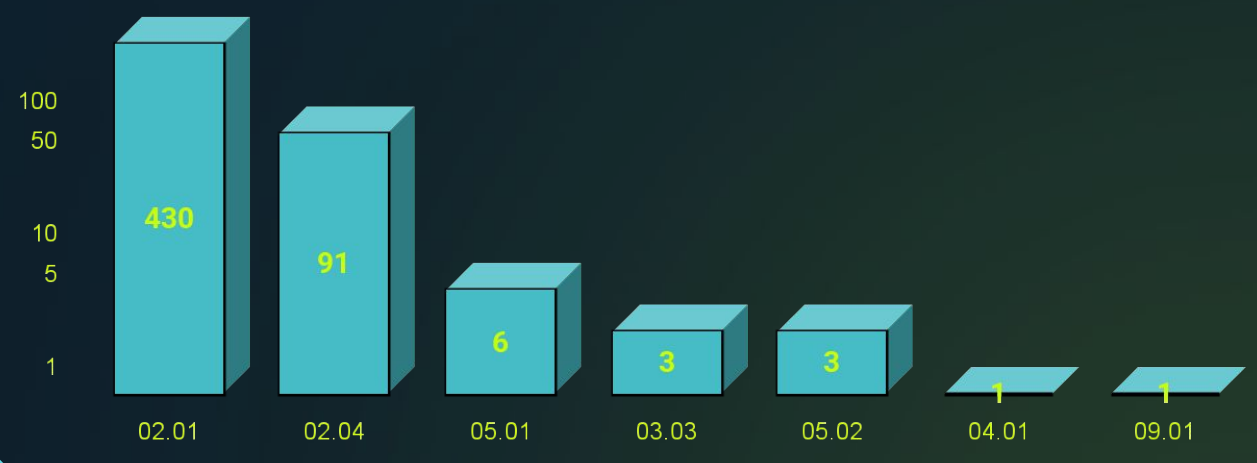
У першому півріччі 2025 року Оперативним центром реагування на кіберінциденти було ідентифіковано та опрацьовано 535 кіберінцидентів та кібератак.

Переважна частина з них стосувалася інфікування шкідливим програмним забезпеченням. Основною метою подібних атак, як правило, було отримання несанкціонованого віддаленого доступу до інформаційних систем для проведення кіберрозвідки або викрадення фінансових ресурсів.

Найпоширенішими типами кіберінцидентів стали:

- зараження шкідливим програмним забезпеченням;
- виявлення шкідливих або аномальних мережевих підключень;
- компрометація облікових записів користувачів.

Розподіл за типами кіберінцидентів

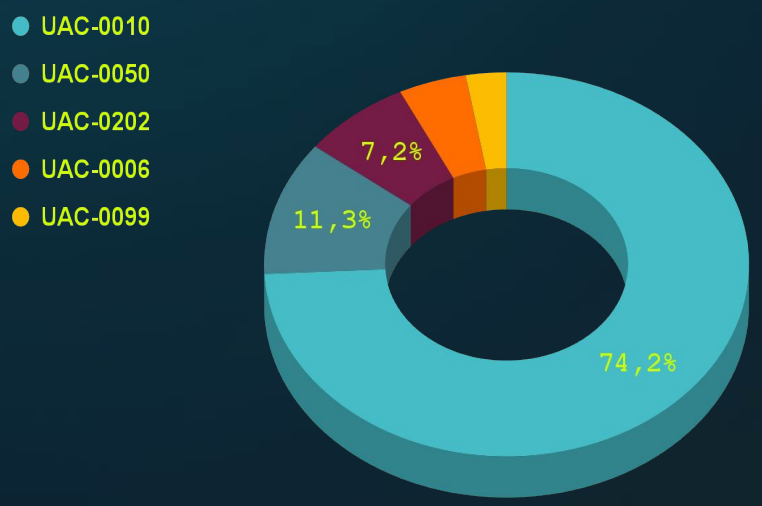


02.01 - зараження ШПЗ, 02.04 - шкідливе підключення, 05.01 - компрометація облікового запису, 03.03 - фішинг, 05.02 - компрометація системи, 04.01 - спроба експлуатації вразливості, 09.01 - вразливість.

КІБЕРЗАГРОЗИ

КІЛЬКІСНІ ПОКАЗНИКИ КІБЕРЗАГРОЗ

Розподіл кіберінцидентів



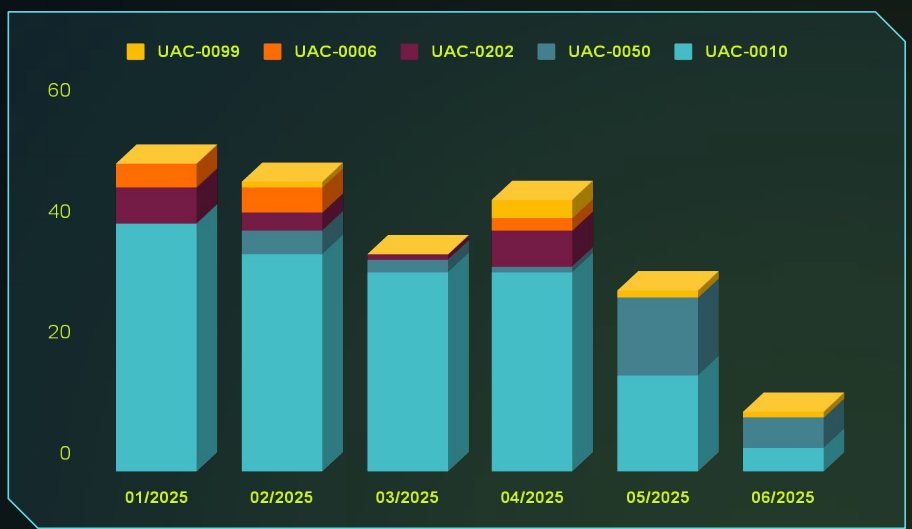
Серед зафіксованих в ОЦРК кіберінцидентів/кібератак **221** було пов'язано з відомими кластерами кіберзагроз. Таким чином, у першій половині 2025 року найактивнішими були UAC-0010, UAC-0050 та UAC-0202.

Основним початковим вектором кібератак було розповсюдження ШПЗ засобами електронної пошти – **T1566.001** Phishing: Spearphishing Attachment (за класифікацією MITRE ATT&CK).

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.

Графік демонструє динаміку виявлених кіберінцидентів протягом першого півріччя 2025 року, зафіксованих Оперативним центром реагування на кіберінциденти.

Спостерігається певне зниження кількості кіберінцидентів, пов'язаних із діяльністю кластеру кіберзагроз UAC-0010.



КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Опис кластеру UAC-0010

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

Відслідковується з:
2013 року

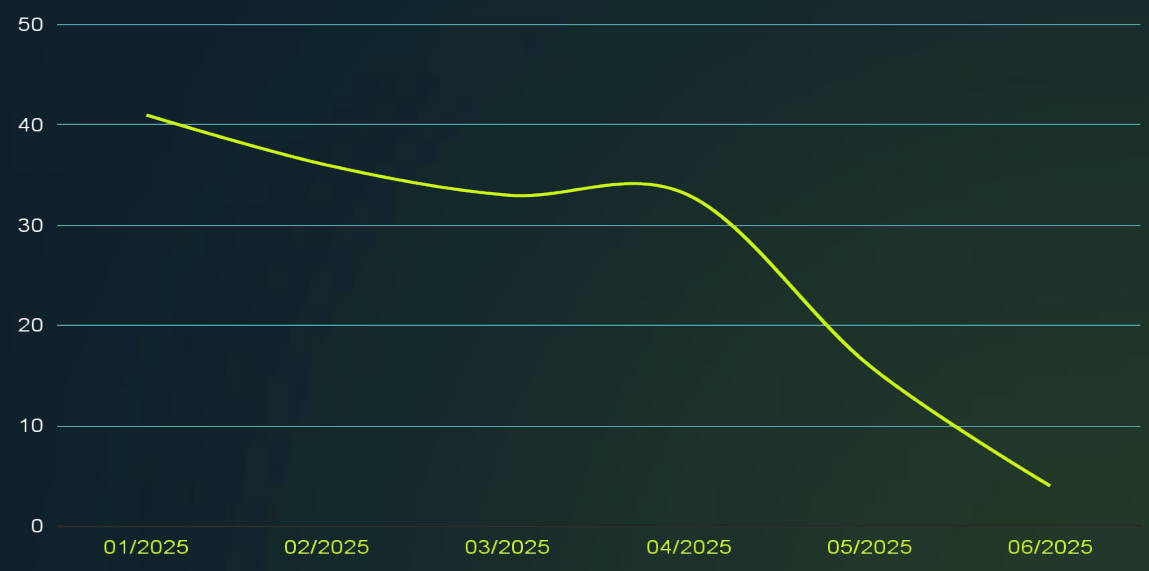
Мотивація:
кібершпигунство

Цілі кібератак:
державні органи, сили оборони

Протягом І півріччя 2025 фахівці ОЦРК виявили 164 кіберінциденти, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0010. Серед досліджених кіберінцидентів первинним вектором ураження було розповсюдження ШПЗ засобами електронної пошти та за допомогою флеш-носіїв.

Зведена інформація щодо діяльності угрупування UAC-0010 за посиланням: **https://cert.gov.ua/article/5160737**.

Таймлайн кібератак UAC-0010



КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Опис кластеру UAC-0050

Псевдоніми:
Відсутні

Відслідковується з:
2020 року

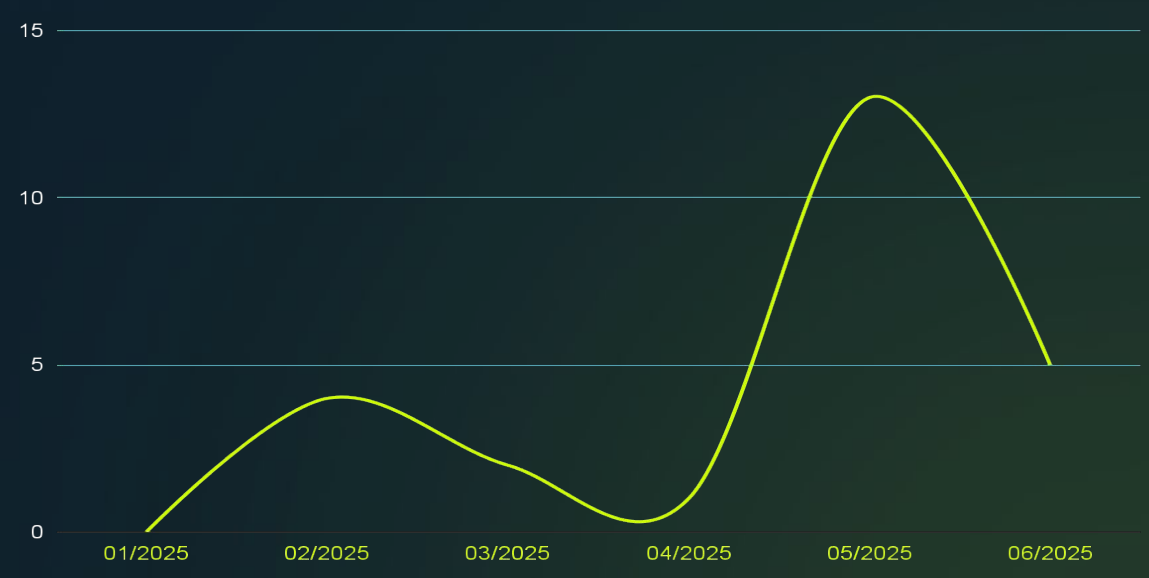
Мотивація:
кібершпигунство, викрадення коштів, ІПСО

Цілі кібератак:
державні органи, сили оборони, фінансові установи

Упродовж І півріччя 2025 фахівці ОЦРК виявили 25 кіберінцидентів, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0050. Серед досліджених кіберінцидентів первинним вектором ураження було розповсюдження ШПЗ засобами електронної пошти.

Зведена інформація щодо діяльності угрупування UAC-0050 за посиланням: **https://cert.gov.ua/article/6281009**.

Таймлайн кібератак UAC-0050



КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Опис кластеру UAC-0202

Псевдоніми:
Відсутні

Відслідковується з:
щонайменше з 2013 року

Мотивація:
Майнинг криптовалют, шпигунство

Цілі кібератак:
Не визначено

Упродовж І півріччя 2025 року фахівці ОЦРК виявили 16 кіберінцидентів, пов'язаних з активністю, яку CERT-UA відстежує під ідентифікатором UAC-0202.

У більшості випадків первинним вектором ураження було використання неліцензійного програмного забезпечення, до складу якого було вбудовано шкідливе програмне забезпечення. Такий підхід дозволяв зловмисникам здійснювати приховане зараження систем під час встановлення "піратського" ПЗ.

Таймлайн кібератак UAC-0202

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.
ASM	Сервіс передбачає сканування публічних інформаційних ресурсів, та охоплює перевірку наявних вразливостей, ідентифікацію потенційних ризиків та векторів атак, надання детальних звітів з описом вразливостей тощо.

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

Email: info_scpc@cip.gov.ua

Телефон: +38 (044) 281 87 37

Оперативний центр реагування на кіберінциденти

Державний центр кіберзахисту

Державна служба спеціального зв'язку та захисту інформації України

e-mail: soc@cip.gov.ua

тел.: +38 (044) 281 87 37