ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"

РІЧНИЙ ЗВІТ

ОСВІТНЬОЇ КОМАНДИ РЕАГУВАННЯ НА КОМП'ЮТЕРНІ НАДЗВИЧАЙНІ ПОДІЇ
CSIRT-ED

2025

TLP:CLEAR

ЗМІСТ

ВСТУП

Освітня команда реагування на комп'ютерні надзвичайні події CSIRT-ED є позаштатною структурною одиницею Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Діяльність CSIRT-ED спрямована на **підвищення рівня кібербезпеки** підрозділів Інституту та протидії кіберзагрозам. Важливою складовою є **забезпечення ефективної підготовки** майбутніх фахівців у сфері кібербезпеки шляхом залучення науково-педагогічних працівників та здобувачів вищої освіти до виконання практичних завдань в межах її діяльності.

CSIRT-ED розвивається відповідно до рекомендацій **European Union Agency for Cybersecurity (ENISA)**, **Cybersecurity and Infrastructure Security Agency (CISA)**, положень Закону України «Про основні засади забезпечення кібербезпеки України» та постанов Кабінету Міністрів України щодо організаційно-технічної моделі кіберзахисту.

CSIRT-ED поєднує три ключові напрями: **оперативне реагування на кіберінциденти, практичну підготовку спеціалістів та розвиток національної системи кіберзахисту**.

Більше інформації про CSIRT-ED та її діяльність розміщенно на: iscip.kpi.ua/csirt-ed

Місія:

Забезпечення кіберстійкості освітнього простору Інституту та формування професійної еліти через інтеграцію практичного досвіду реагування на кіберзагрози в навчальний процес.

Перший квартал 2025 року став етапом трансформації нормативних положень у діючі механізми захисту. Було проведено комплекс заходів щодо технічного оснащення та кадрового посилення.

Фундаментом діяльності стало розгортання архітектури системи кібербезпеки:
- *впроваджено спеціалізований стек інструментів для моніторингу та реагування;*
- *створено єдиний контур кіберзахисту, що дозволяє виконувати повний цикл робіт – від виявлення аномалій до відновлення систем та криміналістичного аналізу.*

З 1 лютого 2025 року розпочато стратегічний етап залучення людського капіталу:
- *здобувачі вищої освіти інтегровані в процеси CSIRT-ED;*
- *впроваджено систему навчань у вигляді сценаріїв, що моделюють реальні кібератаки (KI/KA). Цим забезпечено стресостійкість та злагодженість дій в складі команд.*

Для стандартизації процесів CSIRT-ED реалізовано:
- *закритий електронний ресурс з методичними рекомендаціями та регламентами функціонування CSIRT-ED;*
- *офіційна вебсторінка CSIRT-ED для інформування спільноти та партнерів.*

Повний мандат доступний за посиланням https://iscip.kpi.ua/csirt/rfc2350.txt

ДІЯЛЬНІСТЬ

Управління подіями інформаційної безпеки:

- моніторинг систем за допомогою автоматизованої системи управління подіями та інформацією про безпеку (SIEM);
- виявлення аномальної, непритаманної системі поведінки за допомогою автоматизованої системи управління подіями та інформацією про безпеку (SIEM), а також систем виявлення та запобігання вторгненням (IDS/IPS);
- аналіз подій та реагування на них.

Управління інцидентами в системі кібербезпеки:

- отримання повідомлень про кіберінциденти від спільноти користувачів;
- аналіз кіберінцидентів;
- аналіз артефактів та даних комп'ютерної криміналістики;
- зменшення негативних наслідків та відновлення сталого функціонування систем;
- координація кіберінцидентів.

Управління вразливостями:

- виявлення вразливостей та їх дослідження;
- аналіз звітів (CVE), надання рекомендацій для усунення застосування вразливостей під час кібератак;
- координація та обмін інформацією про вразливості з суб'єктами кіберзахисту.

Ситуаційна обізнаність:

- збір та аналіз даних про загрози кібербезпеки з використанням мережевих пасток (honeypots);
- моніторинг різних видів джерел, що повідомляють про кіберінциденти;
- моніторинг відкритих джерел інформації щодо можливих загроз кібербезпеки, планування інформаційних операцій, витоку конфіденційної інформації та поповнення бази даних інформаційних ресурсів, які ведуть діяльність в сфері кібербезпеки;
- аналіз та поширення отриманої інформації;
- комунікація зі спільнотою користувачів задля унеможливлення повторних атак.

Передача знань:

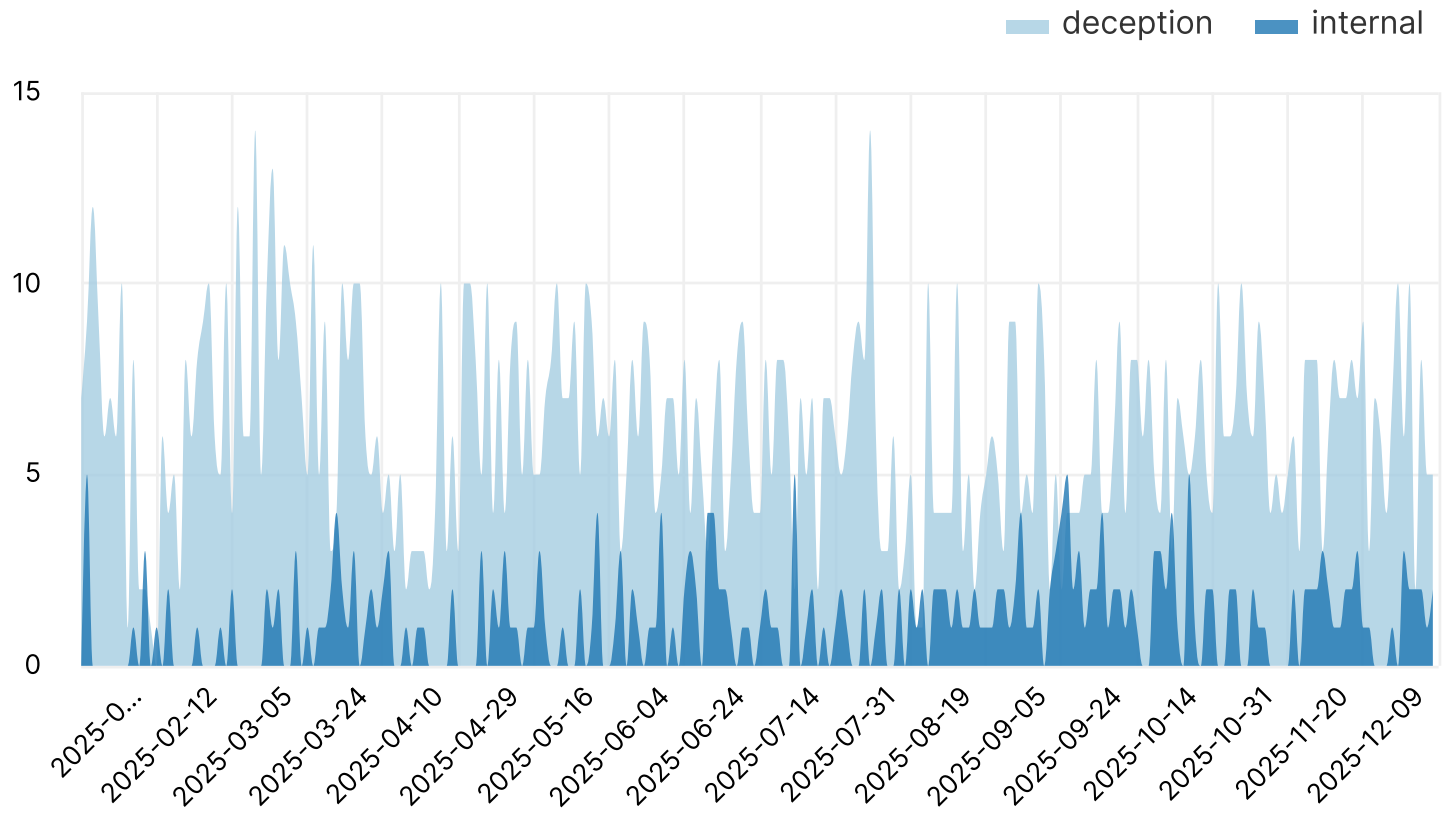
- підвищення обізнаності спільноти користувачів, шляхом поширення інформації про кіберінциденти;
- професійна підготовка складу команди шляхом участі в заходах присвячених кібербезпеці (курси, науково-технічні конференції, змагання CTF, хакатони тощо) та відпрацювання практичних навиків на кіберполігонах;
- розробка, впровадження та тестування сценаріїв для кіберполігону Навчального ситуаційного центру з кібербезпеки Інституту;
- збір інформації про кіберінциденти, які були опрацьовані командою у системі MISP (Malware Information Sharing Platform);
- організація відпрацювання навчальних завдань здобувачами вищої освіти у складі команди.

УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

За звітній період оброблено 1727 події інформаційної безпеки[1], серед яких 280 подій на навчальній інфраструктурі та 1447 – події з мережевих пасток.

Тип	Рівень KI/KA			Кількість
	1, низький	2, середній	3, високий	
deception	221	1163	63	1447
internal	72	185	23	280
Всього				**1727**

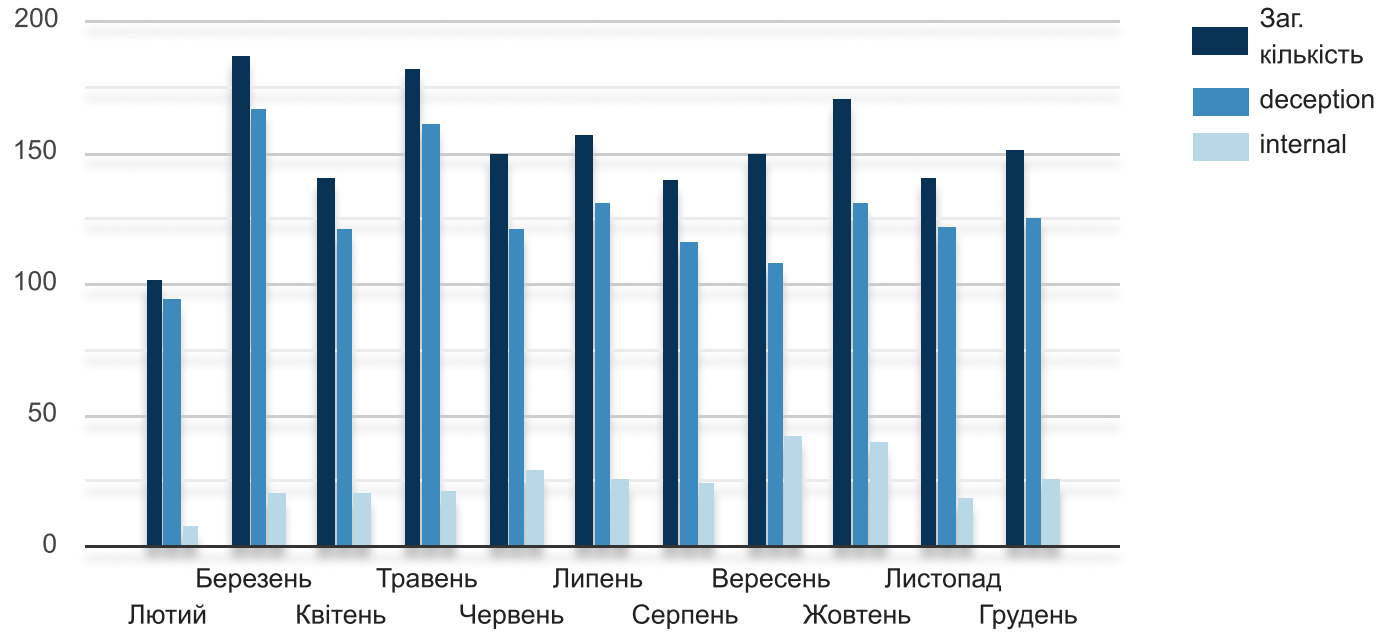
Динаміка виявлення подій інформаційної безпеки



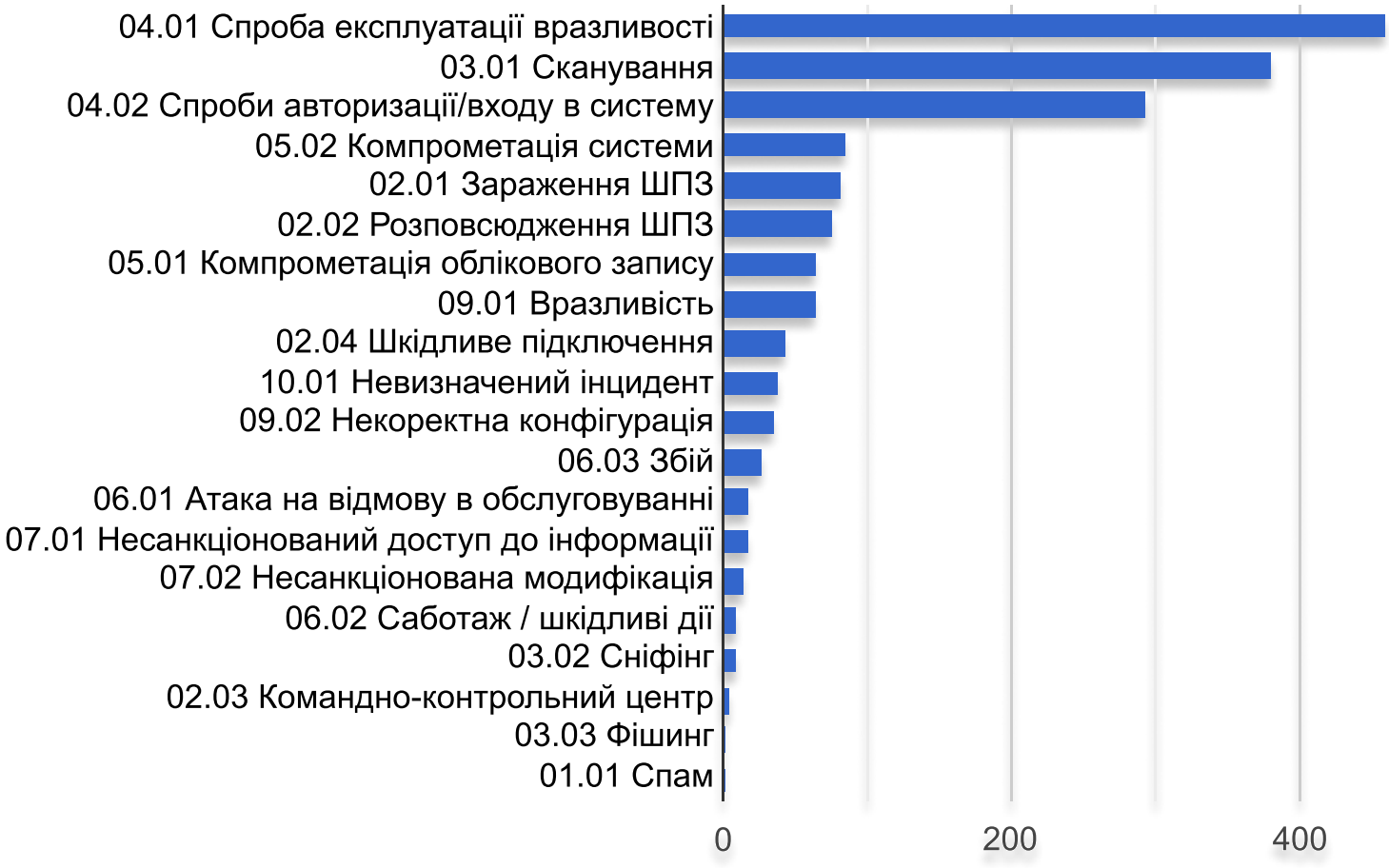
1. Подія інформаційної безпеки (*в контектсі даного документу*) – подія кібербезпеки з навчальної інфраструктури або мережевої пастки, що розглядається як кіберінцидент, та не є ним.

ТЕНДЕНЦІЇ

Зафіксовано сплески активностей на навчальній інфраструктурі навесні та восени.



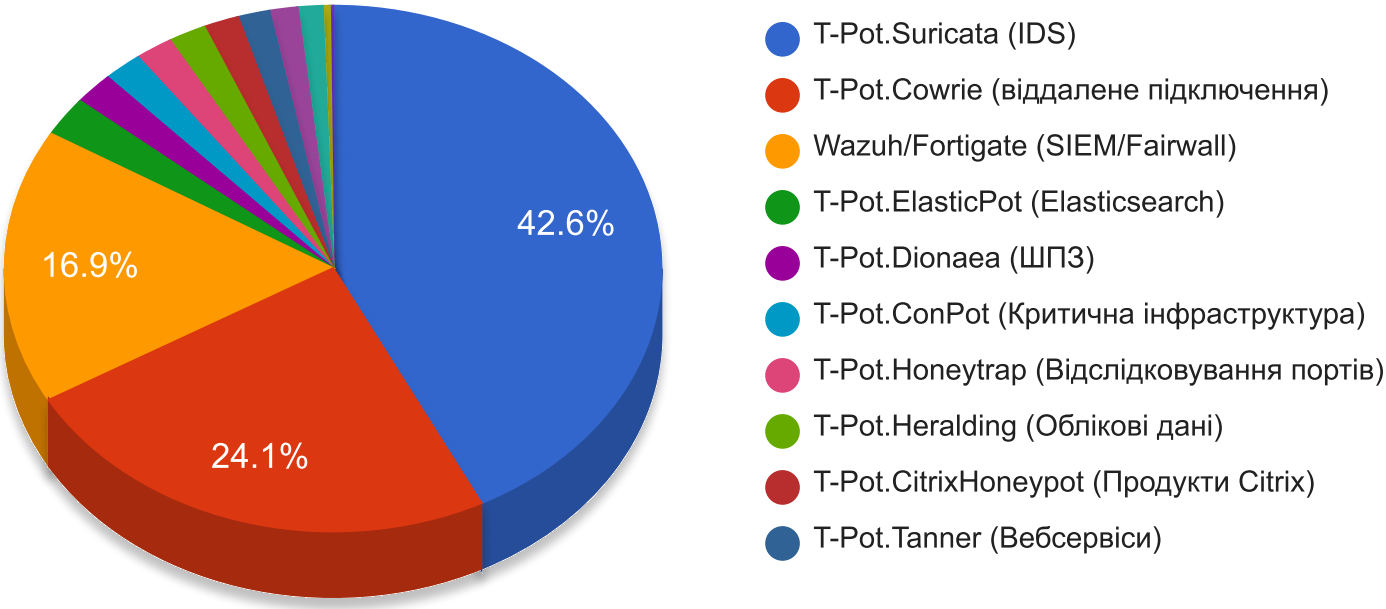
Якщо брати до уваги типи подій[2], то можемо констатувати факт, що більшість подій пов'язані зі спробами експлуатації вразливостей навчальної інфраструктури.



2. Відповідно Переліку категорій і типів кіберінцидентів Наказу Адміністрації Держспецзв'язку від 03 липня 2023 року №570 "Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі".

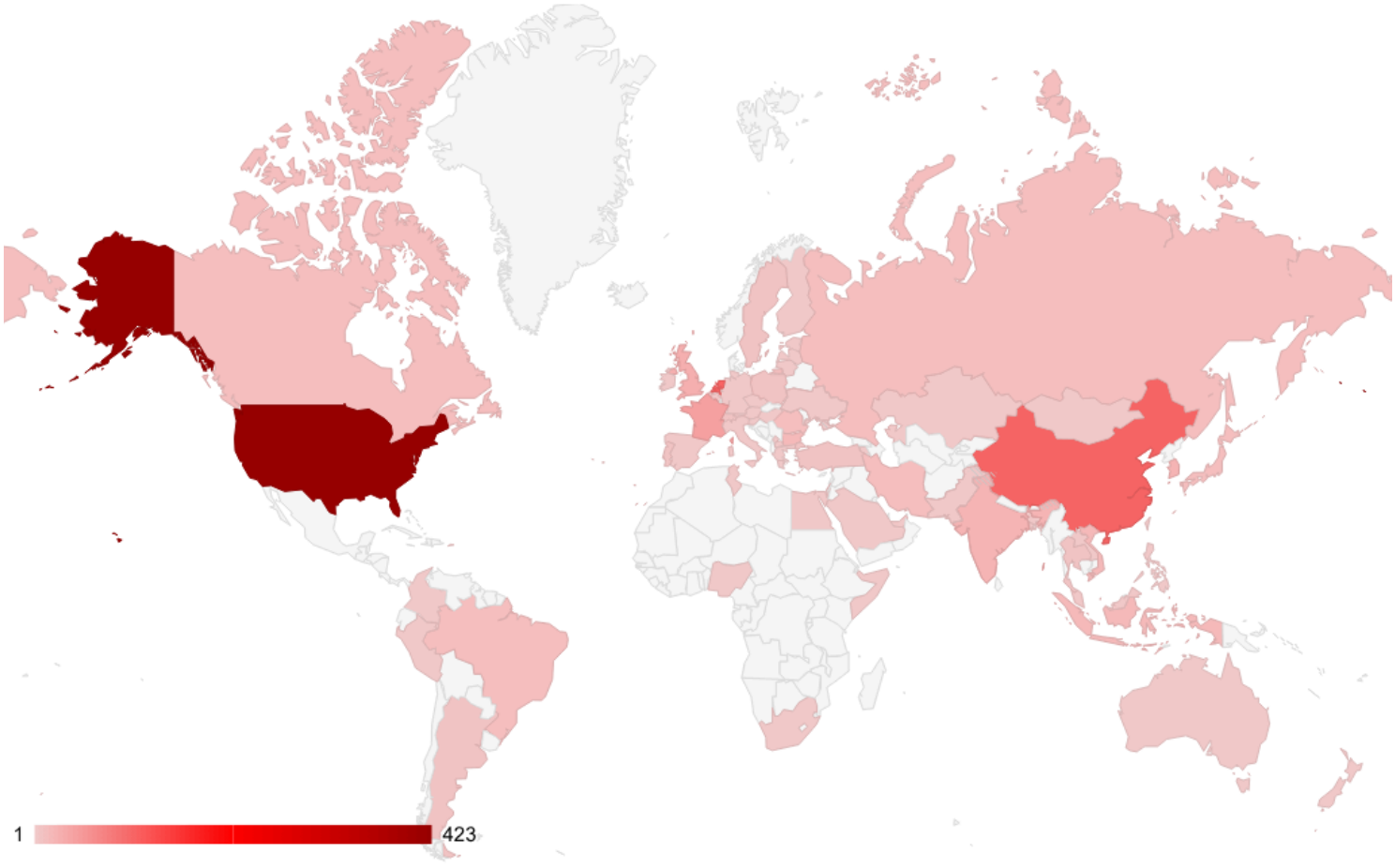
ТЕНДЕНЦІЇ

Основиними джерелами виявлення подій інформаційної безпеки були IDS Suricata разом з системою мережевих пасток T-Pot, SIEM Wazuh та фаєрволом нового покоління Fortigate.



Протягом 2025 року відпрацювання теоретичних та практичних навиків під керівництвом постійних експертів Інституту пройшло **48** здобувачів вищої освіти.

Найбільшу кількість подій інформаційної безпеки зафіксовано з IP-адрес, розташованих у США, Королівстві Нідерланди та Китаї.

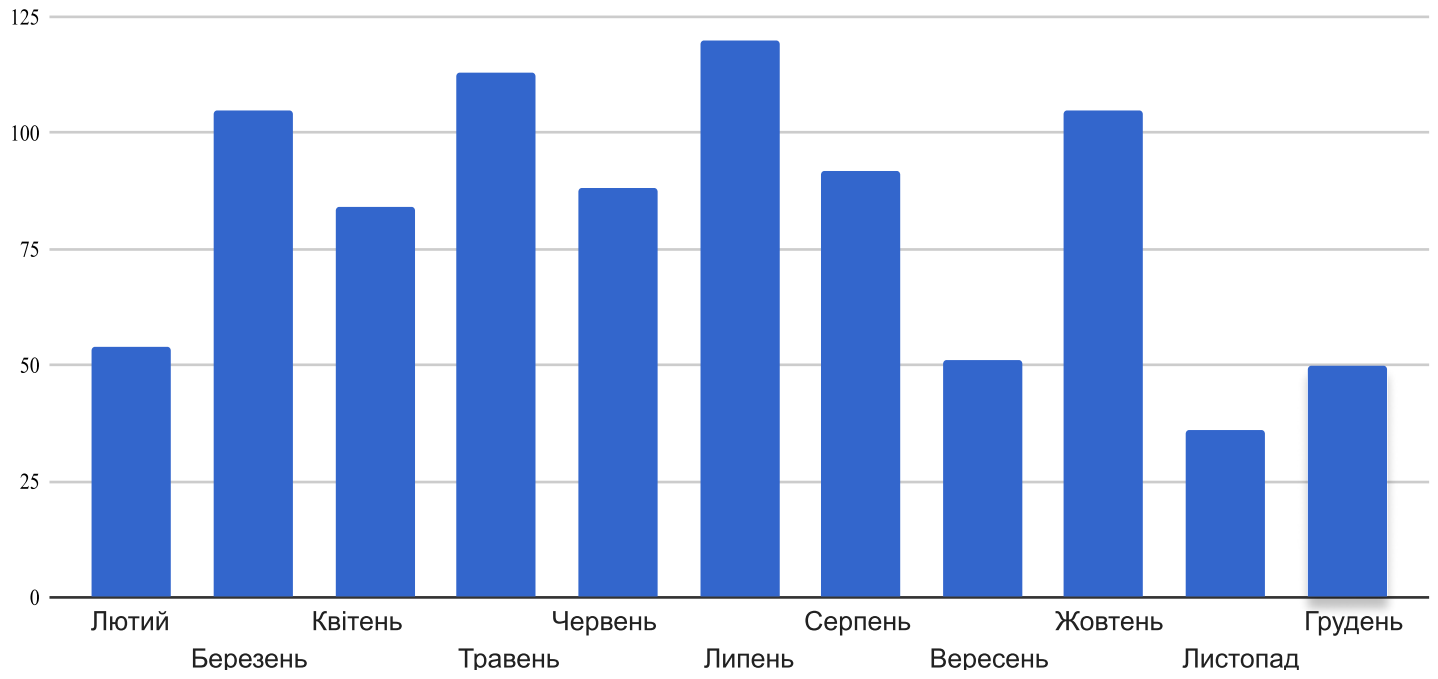


СИТУАЦІЙНА ОБІЗНАНІСТЬ

Протягом звітного періоду поповнювався список джерел відкритої інформації з числа соціальних мереж, новинних сайтів, форумів, які напряму чи опосередковано здійснюють/висвітлюють інформацію про кібератаки/кіберінциденти, витоки даних. Отже, було ідентифіковано **240** нових джерел інформації, що відповідають заданим критеріям. Для кожного з них зібрано та систематизовано відомості щодо типу джерела, характеру діяльності та виду інформаційних матеріалів.

Джерело	Кібератаки	Компрометація	Новин	Всього
Telegram	30	20	48	98
X	11	3	10	24
VK			9	9
YouTube	1		4	5
Facebook	1		3	4
WhatsApp			3	3
Instagram			2	2
Discord			1	1
OK			1	1
Інші веб-ресурси			93	93
Сума	43	23	174	240

Крім цього здійснено пошук та накопичення новин, щодо кібератак та витоку даних, що відбулись в Україні та за кордоном. Загалом накопичено 898 новин, що відповідає заданому критерію.



ПЕРЕДАЧА ЗНАНЬ

З метою вдосконалення практичних навиків реагування на кіберінциденти, було проведено спеціалізовані навчання для здобувачів вищої освіти. Навчання базувалося на реалістичних сценаріїв, розроблених постійними експертами CSIRT-ED.

Під час тренувань здобувачі вищої освіти відпрацювали повний цикл Incident Response: від отримання сповіщень про витік даних у Dark Web до локалізації загрози в гетерогенній інфраструктурі.

Сценарій: «Кіберінцидент: Втрачена Формула»

Цей сценарій симулює складну атаку на критичну інфраструктуру, що дозволяє відпрацювати повний цикл реагування на кіберінциденти у гібридному середовищі. Він вимагає від аналітика не лише технічних навиків форензики, а й розуміння контексту загрози.

Основна користь полягає у поєднанні мережевого аналізу, дослідження хостів (Windows, Linux) та Threat Intelligence для побудови цілісної картини атаки.

З метою підвищення якості практичної підготовки здобувачів вищої освіти, функціонал розробленого кіберполігону «CyberEdge» було масштабовано шляхом впровадження **понад 50** тренувальних сценаріїв.

Інтеграція цих сценаріїв дозволила створити варіативне навчальне середовище, яке забезпечує формування стійких професійних компетентностей у здобувачів вищої освіти. Сценарії варіюються за рівнем складності та охоплюють критичні аспекти кібербезпеки у **форматі CTF (Capture The Flag)**, що дозволяє адаптувати освітній процес під індивідуальний рівень підготовки здобувачів вищої освіти.

Важливою складовою діяльності команди є регулярна участь у профільних змаганнях з кібербезпеки та розробки програмного забезпечення. Це дозволяє здійснювати незалежну оцінку рівня кваліфікації учасників та відслідковувати актуальні тренди у методах кібератак та кіберзахисту.

Команда демонструє стабільні результати у змаганнях формату CTF на національному та міжнародному рівнях, за звітній період прийнято участь у понад 60 заходах.

Окремим вектором розвитку є участь у змаганнях формату Attack&Defence, які максимально наближені до реальних умов кіберпротистояння. Команда отримала унікальний досвід захисту власної інфраструктури в режимі реального часу, оперативного патчингу сервісів та моніторингу мережевої активності під постійним тиском атак опонентів. Отримані навики активно імплементуються у сценарії навчального кіберполігону «CyberEdge».

У рамках технічних хакатонів команда фокусується на створенні інноваційних рішень для автоматизації процесів забезпечення кібербезпеки. Участь у таких заходах дозволила пройти шлях від ідеї до MVP (Minimum Viable Product) для низки проєктів, зокрема систем моніторингу та аналізу кіберзагроз.

ВЛАСНІ РОЗРОБКИ

CSIRT-ED використовує як готові рішення, так і створює власні продукти для навчання та захисту.

AIS "Hacker Groups"

Інформаційно-аналітична система:

- база знань про APT-угруповання (TTPs);
- профілі ворога: інструменти та методи проникнення;
- інтеграція даних для проактивного захисту.

CyberAggregator

Система раннього виявлення загроз:

- OSINT-інструмент для цілодобового аналізу соцмереж та форумів;
- раннє виявлення підготовки до DDoS та кібератак;
- пошук злитих даних.

CyberEdge

Кіберполігон:

- віртуальне середовище для симуляції кібератак на критичну інфраструктуру;
- безпечне тренування Red/Blue Teams;
- сценарії кібер захисту без ризику для реальної мережі;
- впроваджено більше 50 сценаріїв.

КОМУНІКАЦІЯ ТА СПІВПРАЦЯ

Основними завданнями CSIRT-ED є сприяння підрозділам Інституту у вирішенні питань щодо кіберзахисту та протидії кіберзагрозам, а також підвищення ефективності підготовки кадрів у сфері кібербезпеки шляхом залучення науково-педагогічних, наукових працівників та здобувачів вищої освіти Інституту до виконання завдань в межах діяльності команди реагування на комп'ютерні надзвичайні події.

Забезпечено комунікації із суб'єктом кіберзахисту та фахівцями відділів інформаційно-комунікаційних систем та кіберзахисту Інституту щодо виявленого КІ/КА.

Діяльність CSIRT-ED тісно інтегрована в національну систему кібербезпеки шляхом взаємодії з структурними підрозділами Держспецзв'язку, такими як Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) та Державний центр кіберзахисту (ДЦКЗ), реалізується за такими напрямами:

- Оперативна взаємодія: CSIRT-ED у межах своєї компетенції офіційно взаємодіє зі структурними підрозділами Адміністрації Держспецзв'язку.
- Реагування на інциденти: Команда здійснює опрацювання інформації про кіберінциденти та забезпечує взаємодію з іншими українськими командами реагування на комп'ютерні надзвичайні події (до яких відноситься CERT-UA).
- Координація та обмін даними: CSIRT-ED здійснює координацію та обмін інформацією про вразливості із суб'єктами кіберзахисту, а також використовує методичні рекомендації Держспецзв'язку щодо реагування на події у кіберпросторі.

Ця співпраця дозволяє CSIRT-ED ефективно виконувати завдання з моніторингу кіберзагроз, накопичення даних про кіберінциденти та надання допомоги у їх усуненні.

РЕКОМЕНДАЦІЇ

CSIRT-ED здійснює моніторинг кіберзагроз та надає методичну допомогу підрозділам Інституту для запобігання кіберінцидентам. Нижче наведено базові рекомендації для користувачів та технічних адміністраторів.

Парольна політика:

- використовуйте унікальні паролі для кожного ресурсу;
- налаштуйте двофакторну автентифікацію всюди, де це можливо (корпоративна пошта, хмарні сервіси).

Протидія фішингу:

- не відкривайте вкладення та не переходьте за посиланнями у листах від невідомих відправників;
- перевіряйте адресу відправника: зловмисники часто маскують адреси під офіційні (наприклад, admin-kpi@gmail.com замість офіційного домену).

Робота з даними:

- не зберігайте конфіденційні службові документи на особистих файлообмінниках;
- регулярно робіть резервні копії важливих даних.

Управління вразливостями:

- забезпечте своєчасне оновлення операційних систем та програмного забезпечення;
- регулярно перевіряйте системи на наявність відомих вразливостей, використовуючи інформацію від CSIRT-ED, CERT-UA, ДЦК3 Держспецзв'язку.

Якщо ви помітили підозрілу активність (зникнення файлів, блокування екрана, повідомлення про викуп, аномальна робота комп'ютера):

1. Не вимикайте живлення комп'ютера (це може знищити докази в оперативній пам'яті), але від'єднайте його від мережі (витягніть кабель LAN або вимкніть Wi-Fi).
2. Зафіксуйте час виявлення кіберінциденту та видимі ознаки (зробіть фото екрана пристрою, якщо скріншот неможливий).
3. Терміново повідомте підрозділ кібербезпеки. Команда забезпечує управління кіберінцидентами та координацію реагування.

CSIRT-ED у своїй діяльності керується нормативною базою та методичними рекомендаціями державних суб'єктів забезпечення кібербезпеки. Для отримання детальної технічної інформації, індикаторів компрометації та спеціалізованих інструкцій рекомендуємо звертатися до офіційних ресурсів наших партнерів:

- Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA)

Вебсайт: cert.gov.ua

- Державний центр кіберзахисту (ДЦК3) Держспецзв'язку

Вебсайт: scpc.gov.ua

Освітня команда реагування на комп’ютерні надзвичайні події CSIRT-ED

Інститут спеціального зв’язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Офіційний сайт: https://iscip.kpi.ua/csirt-ed
Контактна адреса: csirt-ed@iscip.kpi.ua