**Перелік категорій кіберінцидентів**

1. Перелік категорій кіберінцидентів (далі – Перелік) розроблений з використанням та відповідає рекомендації Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy[[1]](#footnote-1), січень 2018 року), а також спільному документу ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs[[2]](#footnote-2)).

2. Перелік призначений для впровадження єдиної таксономії як інструменту для обміну інформацією щодо кіберінцидентів.

3. Перелік може застосовуватись суб’єктами забезпечення кібербезпеки для формування за необхідності власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням кодування категорій кіберінцидентів, наведених у цьому документі.

4. Перелік має регулярно переглядатися з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від суб’єктів забезпечення кібербезпеки.

5. Суб’єкти забезпечення кібербезпеки при обміні та поширенні інформації про кіберінциденти, підготовці звітів і публічних повідомлень про кіберінциденти застосовують Перелік.

6. Цей перелік є обов'язковим для основних суб’єктів забезпечення кібербезпеки при реєстрації, обліку та обміні інформацією про кіберінциденти, передачі звітів до НКЦК, зокрема із використанням автоматизованих платформ обміну інформацією про кіберзагрози.

7. У випадку, коли на початковій стадії реагування кіберінцидент може бути віднесений до декількох категорій, вибирається категорія із більшим рівнем загрози.

|  |  |  |  |
| --- | --- | --- | --- |
| **Код** | **Категорія інциденту** | **Назва інциденту** | **Назва інциденту в MISP** |
| 01. | Шкідливий (образливий) вміст (Abusive content) | Спам | Spam |
| Образливий контент | Harmful Speech[[3]](#footnote-3) |
| Шкідливий контент | Child/Sexual/Violence/...[[4]](#footnote-4) |
| 02. | Шкідливий програмний код (Malicious Code) | Вірус | Virus |
| Хробак | Worm |
| Троян | Trojan |
| Шпигунське програмне забезпечення | Spyware |
| Діалер | Dialer |
| Руткіт | Rootkit |
| Шкідливе програмне забезпечення | Malware |
| Управління ботами | Botnet drone |
| Програма-здирник | Ransomware |
| Конфігурація шкідливого програмного забезпечення | Malware configuration |
| Командно-контрольний центр | C&C |
| 03. | Збір інформації зловмисником (Information Gathering) | Сканування | Scanning |
| Перехоплення і аналіз мережевого трафіку | Sniffing |
| Соціальна інженерія | Social Engineering |
| 04. | Спроби втручання (Intrusion Attempts) | Експлуатація відомих вразливостей | Exploiting of known Vulnerabilities[[5]](#footnote-5) |
| Спроби авторизації | Login attempts[[6]](#footnote-6) |
| Експлуатація раніше невідомих вразливостей | New attack signature (exploit)[[7]](#footnote-7) |
| 05. | Втручання (Intrusion) | Компрометація привілейованого облікового запису | Privileged Account Compromise |
| Компрометація непривілейованого облікового запису | Unprivileged account compromise |
| Компрометація застосунку | Application compromise |
| Бот | Bot |
| Дефейс | Defacement |
| Компрометація системи | Compromised |
| Бекдор | Backdoor |
| 06. | Порушення доступності (Availability) | Атака на відмову в обслуговуванні | DoS |
| Розподілена атака на відмову в обслуговуванні | DDoS |
| Саботаж, диверсія | Sabotage |
| Збій без участі зловмисника | Outage, no malice |

|  |  |  |  |
| --- | --- | --- | --- |
| 07. | Порушення властивостей інформації (Information Content Security) | Несанкціонований доступ до інформації | Unauthorised access to information |
| Несанкціоноване внесення змін до інформації | Unauthorised modification of information |
| Сервер з публічними правами на запис | Dropzone [[8]](#footnote-8) |
| 08. | Шахрайство (Fraud) | Несанкціоноване використання ресурсів | Unauthorized use of resources |
| Порушення авторських прав | Copyright |
| Маскарадинг | Masquerade[[9]](#footnote-9) |
|  |  | Фішинг | Phishing |
| 09. | Відома вразливість (Vulnerable) | Вразливості, відкриті для експлуатації | Open for abuse |
| 10. | Інше (Other) | Чорний список | Blacklist |
| Недостатньо даних | Unknown |
| Інше | Other [[10]](#footnote-10) |

Приклад представлення інформації, яка надається при обміні про кіберінциденти.

Приклад повідомлення щодо обміну інформацією про кіберінциденти.

TLP: КОЛІР

Поле для зазначення суб’єкта інформування

Поле для повідомлення про кіберінцидент

Категорія кіберінциденту

Назва кіберінциденту

Опис кіберінциденту

TLP: КОЛІР

1. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy [↑](#footnote-ref-1)
2. https://www.europol.europa.eu/sites/default/files/documents/common\_taxonomy\_for\_law\_enforcement\_and\_csirts\_v1.3.pdf [↑](#footnote-ref-2)
3. Небажаний контент, в тому числі расистський чи ксенофобний матеріал, погрози особі чи групі осіб [↑](#footnote-ref-3)
4. Шкідливий контент, в тому числі дитяча порнографія, насильство, пропаганда [↑](#footnote-ref-4)
5. Спроба компрометації чи пошкодження функціонування системи або сервісу шляхом експлуатації вразливостей, які мають стандартизований ідентифікатор (наприклад, CVE) [↑](#footnote-ref-5)
6. Численні спроби авторизації: підбір паролів, злам паролів і т.п. [↑](#footnote-ref-6)
7. Використання раніше невідомих вразливостей і експлойтів [↑](#footnote-ref-7)
8. Зловмисники використовують сервери з правами на запис для тимчасового збереження викраденої із скомпрометованих систем інформації, в тому числі даних кейлогерів, скомпрометованих облікових даних і т.ін. [↑](#footnote-ref-8)
9. Використання копії ідентифікаторів суб'єкта або системи, в тому числі крадіжка особистості [↑](#footnote-ref-9)
10. Інциденти, які не відносяться до будь-якого вищезазначеної категорії [↑](#footnote-ref-10)