ПЕРЕЛІК
категорій кіберінцидентів

1.Перелік категорій кіберінцидентів (далі – Перелік) розроблений на основі Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21дск)).

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

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

Код xx	Категорія інциденту	Код xx	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
01.	Шкідливий (образливий) вміст (Abusive content)	01	Спам	Spam	Надсилання небажаних повідомлень або великої кількості повідомлень (флуд)
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містятять вкладення з шпз або посилання на його завантаження.
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами.

		04	Шкідливе підключення	Malicious connection	Спроби з’єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов’язаних із активністю певної бот-мережі.
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі.
		02	Снiфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку.
		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи

					використання раніше скомпрометованих вже не актуальних даних.
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromise	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу.
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS	Вплив на нормальне функціонування системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів.
		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо.
		03	Збій	Outage, no malice	Збій в роботі системи

					чи її компоненту без зловмисного втручання.
07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації.
		02	Несанкціонована модифікація	Unauthorised modification of info	Несанкціонована зміна або видалення певного набору інформації.
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних.
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfiguration	Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту

ПРИКЛАД 1: Код інциденту: 01.01; Тип інциденту: Spam (Спам).
ПРИКЛАД 2: Код інциденту: 02.04; Тип інциденту: Malicious connection (Шкідливе підключення).
Якщо інцидент віднесено до певної категорії, проте не визначено його тип, використовується код 00.
ПРИКЛАД 3: Код інциденту: 01.00; Тип інциденту: не визначено. Категорія: Abusive content.

ПРАВИЛА обміну інформацією про кіберінциденти

1.Ці Правила розроблені на основі Загальних правил обміну інформацією про кіберінциденти (Протокол TLP), схвалених Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21дск)).

2.Ці Правила застосовуються в ДЦКЗ Держспецзв'язку при наданні звітів за результатами проведення аналізу даних про кіберінциденти; взаємодії з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; передачі інформації про кіберінциденти від громадян щодо об'єктів кіберзахисту.

3.Особовий склад ДЦКЗ Держспецзв'язку, який працює зінформацією про кіберінциденти, відповідає за виконання обмежень визначених стороною, яка поширює інформацію та встановила відповідне маркування.

4.У випадку необхідності поширення інформації більш широко, ніж передбачено маркуванням згідно з протоколом TLP, необхідно отримати відповідний дозвіл від сторони, яка поширює інформацію.

5.ДЦКЗ Держспецзв'язку, як сторона інформаційного обміну, маркує повідомлення мітками TLP у таких значеннях:

Мітка (колір)	Значення	Приклад
TLP:RED (червоний)	Не для поширення, тільки для кінцевого одержувача. Мітка TLP:RED використовується у випадках, коли інформація не може поширюватись для третьої сторони, і її несанкціоноване поширення може вплинути на репутацію або функціонування установи сторони. Застосовується виключно для обмеженого кола учасників інформаційного обміну та їх працівників, що визначається стороною, яка поширює інформацію.	Одержувачі не можуть поширювати інформацію з міткою TLP:RED іншим сторонам за межами конкретного кола осіб, зустрічі або розмови, в яких вона була спочатку розкрита. Зазвичай використовується при поширенні інформації при особистій зустрічі або прямим електронним листом одержувачу. Мітка TLP:RED може застосовуватись для передачі повідомлень про кіберінцидент представникам основних суб'єктів національної системи кібербезпеки.
TLP:AMBER (жовтий)	Обмежене поширення, доступне тільки серед представників організації-одержувача. Мітка TLP:AMBER використовується, коли для підвищення ефективності обробки інформації необхідна стороння підтримка або допомога, і в той же час	Мітка TLP:AMBER може застосовуватись для передачі індикаторів компрометації з метою інформування інших організацій про потенційні загрози.

	її несанкціоноване поширення створює репутаційні ризики або загрози для функціонування установи, якщо вона поширюється за межі залучених організацій. Застосовується для обмеженого кола учасників інформаційного обміну, одержувач може поширювати таку інформацію тільки серед представників своєї організації, а також передавати клієнтам або замовникам, яким необхідно знати цю інформацію, щоб захистити себе чи запобігти подальшій шкоді.	
TLP:GREEN (зелений)	Обмежене поширення, доступне тільки для представників спільноти або сектору. Мітка TLP:GREEN використовується, коли інформація може підвищити обізнаність усіх учасників інформаційного обміну, а також представників інших організацій або секторів. Застосовується для поширення інформації з організаціями-партнерами у своєму секторі або у спільноті учасників інформаційного обміну, але без поширення через засоби масової інформації, мережу інтернет, соціальні мережі. Інформація з міткою TLP:GREEN не може поширюватись за межами спільноти.	Мітка TLP:GREEN використовується для підвищення колективної безпеки, може застосовуватись для обміну аналітичною інформацією та рекомендаціями щодо шкідливого програмного забезпечення або фішингових атак відносно певного сектору.
TLP:WHITE (білий)	Необмежене поширення. Мітка TLP:WHITE використовується, коли інформація несе мінімальний або нульовий прогнозований ризик неправильного використання, з урахуванням загальноприйнятних правил публічного оприлюднення.	Інформація з міткою TLP:WHITE може поширюватись без обмежень, з урахуванням вимог законодавства про авторське право.

6.У електронних листах мітка TLP вказується у темі повідомлення та в тілі листа безпосередньо перед інформацією, якою здійснюється обмін.

У паперових документах мітка TLP вказується у верхньому і нижньому колонтитулах кожної друкованої сторінки з урахуванням кольору мітки.

Мітка TLP позначається великими літерами: TLP:RED, TLP:AMBER, TLP:GREEN або TLP:WHITE, шрифтом 12pt або більше.

Кольори TLP у палітрі RGB:

TLP:RED : R=255, G=0, B=51;

TLP:AMBER : R=255, G=192, B=0;

TLP:GREEN : R=51, G=255, B=0;

TLP:WHITE : R=255, G=255, B=255.

7. Ці Правила не призначені для позначення інформації, що становить державну, банківську таємницю, та службову інформацію. Передавання такої інформації здійснюється відповідно до законодавства України.