



ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Державний центр кіберзахисту

НАКАЗ

м. Київ

07.04.2023

№ 34

Про впровадження протоколу
TLR версії 2.0 та переліку
категорій кіберінцидентів

Відповідно до Положення про Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, затвердженого наказом Адміністрації Держспецзв'язку від 30.08.2018 № 528 (у редакції наказу Адміністрації Держспецзв'язку від 06 жовтня 2022 року № 590), рішень Національного координаційного центру кібербезпеки при Раді національної безпеки та оборони України (Протоколи № 18 від 25.10.2021 (від 28.10.2021 № 16/320/21дск), № 21 від 09.02.2023 (від 15.02.2023 № 16/47/23дск)), з метою впровадження в діяльності структурних підрозділів ДЦКЗ Держспецзв'язку

НАКАЗУЮ:

1. Затвердити такі, що додаються:

- 1.1 Правила обміну інформацією про кіберінциденти;
- 1.2 Перелік категорій кіберінцидентів.

2. Наказ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України від 10.11.2021 року № 79 «Про впровадження протоколу TLR та переліку категорій кіберінцидентів» визнати таким, що втратив чинність.

3. Начальникам 2-8 управлінь, 9-10 відділам, СІК ДЦКЗ Держспецзв'язку забезпечити застосування документів, затверджених цим наказом, в діяльності підрозділів, а також привести категоріювання інцидентів та звітність у відповідність з ними.

4. Контроль за виконанням цього наказу покласти на заступника начальника ДЦКЗ Держспецзв'язку відповідно до розподілу обов'язків.

Начальник Центру
майор

Валерій БУШКОВ

ЗАТВЕРДЖЕНО

Наказ Державного центру
кіберзахисту Державної служби
спеціального зв'язку та захисту
інформації України

04 квітня 2023 року № 34

ПРАВИЛА обміну інформацією про кіберінциденти

1. Ці Правила розроблені на основі Загальних правил обміну інформацією про кіберінциденти (Протокол TLP версії 2.0), схвалених Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 21 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 09.02.2023 (від 15.02.2023 № 16/47/23дск)).

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 з інформацією 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
1	2	2
TLP:RED	Не для поширення, тільки для кінцевого одержувача.	Одержувачі не можуть поширювати інформацію з міткою TLP:RED

(ЧЕРВОНИЙ)	<p>Мітка TLP:RED використовується у випадках, коли інформація не може поширюватись для третьої сторони, і її несанкціоноване поширення може вплинути на репутацію або функціонування сторони, яка поширює інформацію.</p> <p>Застосовується виключно для обмеженого кола учасників інформаційного обміну та їх працівників, що визначається стороною, яка поширює інформацію.</p>	<p>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 кінцевому одержувачу.</p> <p>Мітка TLP:RED може застосовуватись для передачі повідомлень про кіберінцидент представникам основних суб'єктів національної системи кібербезпеки.</p>
<p>TLP:AMBER (ЖОВТИЙ)</p>	<p>Обмежене поширення, доступне тільки серед представників організації, що є кінцевим одержувачем, або її клієнтів.</p> <p>У разі, коли обмеження поширення повідомлення доступне виключно серед представників організації, що є кінцевим одержувачем, повідомлення маркується як TLP:AMBER+STRICT.</p> <p>Мітка TLP:AMBER використовується, коли для підвищення ефективності обробки інформації необхідна стороння підтримка або допомога, і в той же час її несанкціоноване поширення створює репутаційні ризики або загрози для функціонування сторони, яка поширює інформацію, якщо вона поширюється за межі залучених організацій.</p> <p>Застосовується для обмеженого кола учасників інформаційного обміну, кінцевий одержувач може поширювати таку інформацію тільки серед представників</p>	<p>Мітка TLP:AMBER або TLP:AMBER+STRICT може застосовуватись для передачі індикаторів компрометації до урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA з метою інформування інших організацій про потенційні загрози.</p>

	<p>свої організації, а також передавати клієнтам або замовникам, яким необхідно знати цю інформацію, щоб захистити себе чи запобігти подальшій шкоді (окрім повідомлень, що промарковані міткою TLP:AMBER+STRICT).</p>	
<p>TLP:GREEN (ЗЕЛЕНИЙ)</p>	<p>Обмежене поширення, доступне тільки для представників спільноти або сектору.</p> <p>Мітка TLP:GREEN використовується, коли інформація може підвищити обізнаність усіх учасників інформаційного обміну, а також представників інших організацій або секторів.</p> <p>Застосовується для поширення інформації з організаціями-партнерами у своєму секторі або у спільноті, але без поширення через засоби масової інформації, Інтернет, соціальні мережі.</p> <p>Інформація з міткою TLP:GREEN не може поширюватись за межами спільноти.</p>	<p>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.</p>
<p>TLP:CLEAR (БІЛИЙ)</p>	<p>Необмежене поширення.</p> <p>Мітка TLP:CLEAR використовується, коли інформація несе мінімальний або нульовий прогнозований ризик неправильного використання з урахуванням загальноприйнятних правил публічного оприлюднення.</p>	<p>Інформація з міткою TLP:CLEAR може поширюватись без обмежень з урахуванням вимог законодавства про авторське право.</p>

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 для міток TLP:

Колірна модель		TLP:RED	TLP:AMBER	TLP:GREEN	TLP:CLEAR
1		2	3	4	5
RGB: font	R	255	255	51	255
	G	43	192	255	255
	B	43	0	0	255
RGB: background	R	0	0	0	0
	G	0	0	0	0
	B	0	0	0	0
CMYK: font	C	0	0	79	0
	M	83	25	0	0
	Y	83	100	100	0
	K	0	0	0	0
CMYK: background	C	0	0	0	0
	M	0	0	0	0
	Y	0	0	0	0
	K	100	100	100	100
Hex: font		#FF2B2B	#FFC000	#33FF00	#FFFFFF
Hex: background		#000000	#000000	#000000	#000000

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

Начальник 2 управління
ДЦКЗ Держспецзв'язку
майор



Сергій КРАВЧЕНКО

ЗАТВЕРДЖЕНО

Наказ Державного центру
кіберзахисту Державної служби
спеціального зв'язку та захисту
інформації України
С. Я. Квасець 2023 року № 34

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 містять 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'язані з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі.
			01	Сканування	Scanning	Збір інформації про системи або мережі.
			02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку.
03.	Збір інформації (Information Gathering)		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. Недала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних.
		01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
05.	Втручання (Intrusion)	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.
		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.
06.	Порушення доступності (Availability)	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.

Начальник 2 управління
ДЦКЗ Держспецзв'язку
майор



Сергій КРАВЧЕНКО