Роз’яснення щодо нормативно-правового регулювання діяльності та взаємодії команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT)

Відповідно до статті 9 Закону України «Про основні засади забезпечення кібербезпеки України» (https://zakon.rada.gov.ua/laws/show/2163-19#Text), створено та забезпечується функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози. Уповноваженим органом, що забезпечує функціонування такої системи є Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку).

До складу національної системи реагування на кіберінциденти, кібератаки, кіберзагрози входять:

1. Вимоги до організаційно-технічної спроможності команд реагування на кіберінциденти – наказ Адміністрації Держспецзв’язку від 03 лютого 2026 року № 87, зареєстрований в Мін'юсті 09.03.2026 за № 316/45710 **(https://zakon.rada.gov.ua/laws/show/z0316-26#Text)**

Документ визначає оцінку спроможності для національного CSIRT (CERT-UA), а також галузевих та регіональних CSIRT.

ВАЖЛИВО: Для функціонування в національній системі кібербезпеки регіональні та галузеві CSIRT зобов’язані відповідати щонайменше початковому рівню зрілості.

На основі балів параметрів командам присвоюється один із чотирьох рівнів зрілості:

Початковий: початок виконання завдань, більшість інструментів та процесів можуть мати значення «0», але базові організаційні параметри (О-1 – О-5, О-10) вже мають бути чітко визначені (значення «3»).

Базовий: прогрес за всіма показниками, наявність сформованих внутрішніх правил (значення «2»).

Проміжний: процеси врегульовані керівництвом, або команда має статус «ACCREDITED» у міжнародній спільноті TF-CSIRT.

Розвинутий: максимальний досвід, постійний аудит та оптимізація процесів, або наявність статусу «CERTIFICATED» у TF-CSIRT.

2. Вимоги до сервісу з реагування на кіберінциденти – наказ Адміністрації Держспецзв'язку від 19 травня 2026 року № 360, зареєстрований в Мін'юсті 04.06.2026 за № 817/46211 **(https://zakon.rada.gov.ua/laws/show/z0817-26#Text)**

Документ деталізує перелік, зміст та функції сервісів, які надають CERT-UA, галузеві/регіональні CSIRT, а також залучені приватні команди реагування.

ВАЖЛИВО: За відсутності галузевих або регіональних CSIRT органи влади, місцеве самоврядування та оператори критичної інфраструктури мають право залучати приватні команди реагування для власних потреб або потреб галузі/регіону.

Встановлено чітку вертикаль та правила взаємодії між державними, регіональними та приватними командами реагування:

1. Галузеві та регіональні CSIRT надають сервіси виключно користувачам у межах своєї визначеної галузі, сфери чи регіону.

2. Якщо в певній галузі або регіоні державну команду ще не створено, надання сервісів може тимчасово здійснювати національна команда – CERT-UA.

3. Органи державної влади, місцевого самоврядування та оператори критичної інфраструктури мають право залучати приватні команди реагування (на договірних засадах) як для захисту всієї галузі/регіону (за відсутності державної команди), так і суто для власних потреб.

4. Сервіси можуть надаватися як за договором, так і без нього. При цьому сервіси з категорії «Управління кіберінцидентами» (прийняття повідомлень, аналіз, стримування, відновлення) надаються CERT-UA та CSIRT без укладання жодних договорів та оплати.

НАГОЛОШУЄМО: Кожна команда реагування зобов'язана чітко визначити перелік своїх сервісів відповідно до власної організаційно-технічної спроможності. Цей перелік затверджується органом, який створив команду, та обов'язково публікується на офіційному вебсайті. Надання інших сервісів (не передбачених цим переліком) дозволяється лише за наявності додаткових спроможностей.

Описи сервісів з реагування на кіберінциденти мають включати посилання на відповідні заходи з кіберзахисту, що передбачені для впровадження суб'єктами забезпечення кібербезпеки. Орієнтовне співвідношення сервісів з реагування та заходів з кіберзахисту відповідно до Каталогу заходів з кіберзахисту, затвердженого наказом Адміністрації Держспецзв'язку від 30 січня 2026 р. № 75, наведено в таблиці.

Таблиця

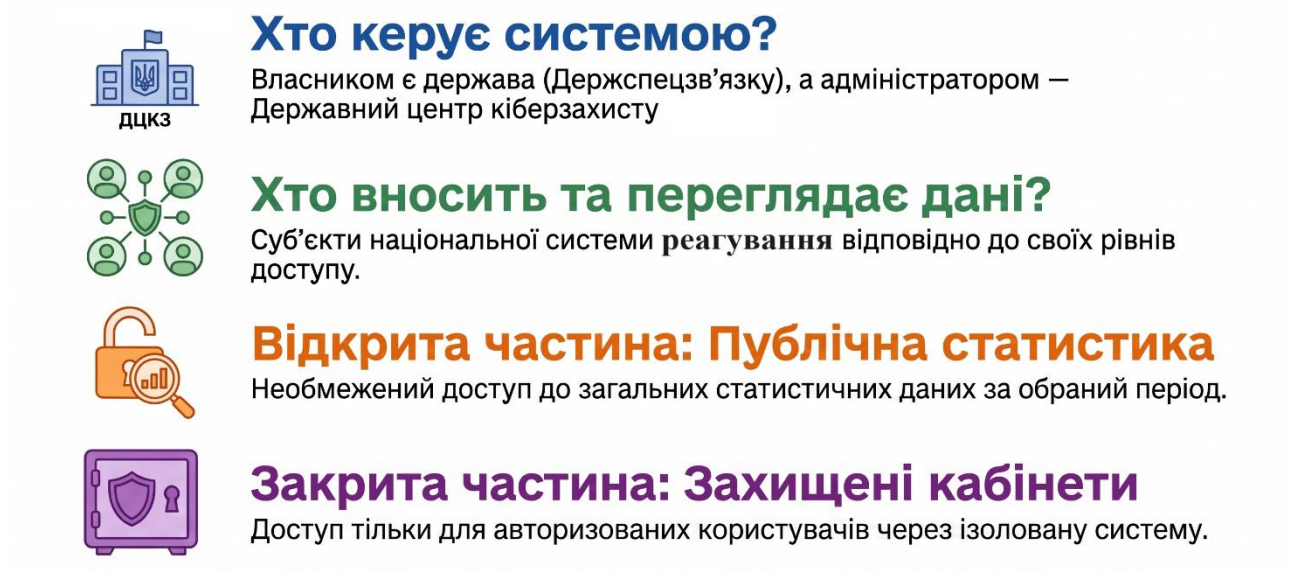
Категорія	Сервіс	Заходи з кіберзахисту
Управління подіями кібербезпеки	Моніторинг та виявлення	DE.CM-01, DE.CM-09, DE.CM-06, PR.PS-04
	Аналіз подій кібербезпеки	DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-08
Управління кіберінцидентами	Аналіз кіберінцидентів	RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08
	Стримування, усунення наслідків та відновлення	RS.MA-05, RS.MI-01, RS.MI-02, RC.RP-01 – RC.RP-06
	Координація реагування на кіберінциденти	RS.MA-01, RS.CO-03, RC.CO-03, RC.CO-04
	Аналіз артефактів	RS.AN-03, RS.AN-06, RS.AN-07, DE.AE-07
	Прийняття повідомлень про кіберінциденти	RS.MA-02, RS.CO-02
	Підтримка кризового управління	RS.MA-04, RS.CO-03, RC.CO-03
Управління вразливостями	Виявлення/дослідження вразливостей	ID.RA-01, ID.RA-02, ID.RA-08
	Аналіз вразливостей	ID.RA-04, PR.PS-02

	Реагування на вразливості	PR.PS-02
	Прийняття повідомлень про вразливості	ID.RA-08
	Координація вразливостей	
	Розкриття інформації про вразливості	
Ситуаційна обізнаність	Збір даних	ID.AM-01, ID.AM-02, ID.AM-04, ID.AM-07
	Аналіз та висновки	ID.RA-03, ID.RA-05, GV.OV-01
	Взаємодія	GV.RM-05
Навчання та тренінги	Навчальні вправи	ID.IM-02, PR.AT-01, PR.AT-02
	Підвищення обізнаності	PR.AT-01, PR.AT-02
	Навчання	PR.AT-02
	Надання консультацій	GV.OC-03, ID.IM-01

3. Порядку ведення репозитарію інформації про кіберінциденти – наказ Адміністрації Держспецзв'язку від 05 березня 2026 року № 179, зареєстрований в Мін'юсті 07.04.2026 за № 473/45867 **(https://zakon.rada.gov.ua/laws/show/z0473-26#Text)**

Документ регламентує функціонування електронної бази даних, яка створена для накопичення, аналізу та прогнозування ризиків на основі інформації про кібератаки в Україні.

ВАЖЛИВО: До репозитарію обов'язково вноситься інформація про всі значні кіберінциденти згідно з національною таксономією. При цьому інформація з обмеженим доступом (зокрема державна таємниця та службова інформація) в репозитарії НЕ обробляється і НЕ зберігається.



Доступ до закритої частини здійснюється через електронний кабінет за допомогою КЕП (кваліфікованого електронного підпису) уповноважених осіб.

У разі звільнення співробітника або порушення ним правил безпеки користувач зобов’язаний поінформувати адміністратора протягом 1 робочого дня. Адміністратор блокує доступ протягом 1 робочого дня.

4. Порядок делегування завдань CERT-UA галузевим та регіональним CSIRT – наказ Адміністрації Держспецзв’язку від 06 лютого 2026 року № 104, зареєстрований в Мін'юсті 16.03.2026 за № 342/45736 (https://zakon.rada.gov.ua/laws/show/z0342-26#Text)

Документ визначає умови та етапи, за яких регіональні та галузеві команди отримують офіційні повноваження національного рівня для роботи у своїй сфері відповідальності.

ВАЖЛИВО (КРИТЕРІЇ ДЕЛЕГУВАННЯ): Завдання CERT-UA можуть бути делеговані команді CSIRT лише за умови, що вона відповідає щонайменше Базовому рівню зрілості спроможності (згідно з наказом Адміністрації Держспецзв’язку від 03.02.2026 № 87, зареєстрованим в Мін'юсті 09.03.2026 за № 316/45710) та обов'язково надає 4 базові сервіси: прийняття повідомлень, аналіз, стримування/відновлення та координацію реагування.

Делегування припиняється протягом 30 днів за рішенням Адміністрації Держспецзв’язку у разі:

Письмового звернення команди або органу;

Припинення надання хоча б одного з обов'язкових сервісів;

Пропущення строків оновлення інформації про команду;

Пропущення або ігнорування встановлених термінів планового моніторингу;

Не усунення виявлених порушень у роботі або порушення правил національної системи обміну інформацією про кіберінциденти, кібератаки,

кіберзагрози або національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

НАГОЛОШУЄМО: Повторно подати запит на делегування завдань після виключення з Переліку дозволяється не раніше ніж через 3 місяці та виключно за умови документального підтвердження усунення всіх попередніх недоліків.

5. Порядок взаємодії галузевих та регіональних CSIRT з CERT-UA та приватних команд реагування на кіберінциденти, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози – наказ Адміністрації Держспецзв'язку від 08 червня 2026 року № 425, зареєстрований в Мін'юсті 30.06.2026 за № 954/46348 **(https://zakon.rada.gov.ua/laws/show/z0954-26#Text)**

Документ визначає правила координації, обміну даними та розподілу обов'язків усередині національної системи реагування на кіберінциденти, кібератаки та кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки та кіберзагрози.

ВАЖЛИВО: Взаємодія та обмін індикаторами кіберзагроз (IoC) між усіма командами здійснюються в режимі, наближеному до реального часу. Всі суб'єкти зобов'язані проводити регулярні спільні кібернавчання для відпрацювання сценаріїв захисту.

Органи державної влади та місцевого самоврядування мають право офіційно наймати приватні команди для повного або часткового виконання функцій галузевого/регіонального CSIRT (якщо державну команду ще не створено). Будь-яка взаємодія з приватними компаніями оформлюється виключно на підставі меморандумів та договорів про нерозголошення. Якщо приватна команда виконує роль галузевого або регіонального CSIRT, на неї повною мірою покладаються всі функції, права, обов'язки та вимоги щодо звітності перед CERT-UA та СБУ, які визначені для державних команд.

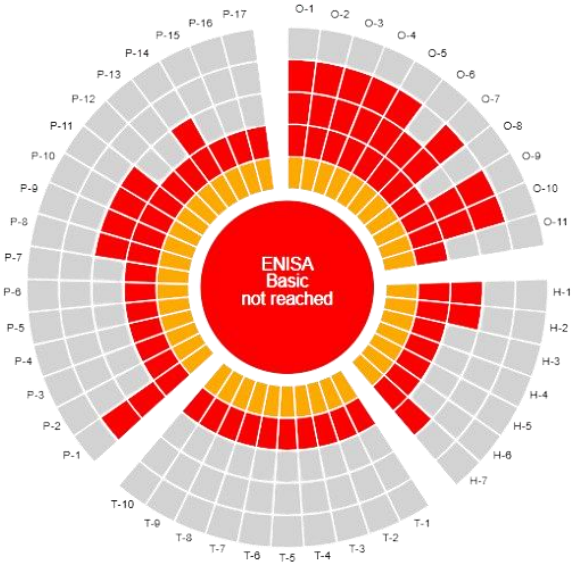
***6. Порядок здійснення моніторингу за діяльністю CERT-UA, галузевих і регіональних CSIRT – наказ Адміністрації Держспецзв'язку від 14 травня 2026 року № 353, зареєстрований в Мін'юсті 26.05.2026 за № 757/46151* (https://zakon.rada.gov.ua/laws/show/z0757-26#Text)**

Документ встановлює правила оцінювання відповідності команд реагування рівням зрілості (згідно з наказом Адміністрації Держспецзв'язку від 03.02.2026 № 87, зареєстрованим в Мін'юсті 09.03.2026 за № 316/45710) та визначає наслідки у разі виявлення порушень.

ВАЖЛИВО: Якщо CSIRT не усуне виявлені під час моніторингу невідповідності у встановлений строк, делегування завдань CERT-UA негайно припиняється, а саму команду виключають із Переліку.

ОБМЕЖЕННЯ: Не можна залучати одну й ту саму команду двічі поспіль, а також заборонено "перехресне" оцінювання (коли дві команди оцінюють одна одну по черзі).

Команди з акредитацією TF-CSIRT (ACCREDITED) або проміжним рівнем проходять оцінку раз на 5 років. Команди зі статусом CERTIFICATED або розвинутим рівнем звільняються від взаємної оцінки.



Для відображення результатів оцінки/самооцінки/взаємної оцінки у вигляді діаграми можна використовувати інструменти незалежної некомерційної організації Open CSIRT Foundation для проведення самооцінки за стандартом SIM3v2 Interim - Security Incident Management Maturity Model за посиланням: https://sim3-check.opencsirt.org/#/.

Адміністрація Держспецзв’язку систематично здійснює аналіз результатів моніторингу. У разі виявлення балів, нижчих за затверджений мінімум, Адміністрація Держспецзв’язку протягом 45 днів надсилає команді офіційну вимогу про усунення недоліків. CSIRT надається 3 місяці для повного усунення порушень та письмового звітування. Не усунення недоліків або не надіслання повідомлення про результати у встановлений 3-місячний строк є прямою підставою для анулювання акредитації та ліквідації статусу делегованої команди.

Т.в.о. заступника директора департаменту –
начальника відділу Департаменту кіберзахисту
Адміністрації Держспецзв’язку Кирило ЗАПОРОЖЕЦЬ