РОЗ’ЯСНЕННЯ ДО ПОСТАНОВИ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ВІД 26 ЛИСТОПАДА 2025 РОКУ № 1533 «ДЕЯКІ ПИТАННЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, КІБЕРАТАКИ ТА КІБЕРЗАГРОЗИ»

Законом України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» внесено зміни до Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закону), зокрема доповнено Закон новими статтями 9 та 9^1.

Відповідно до статей 9 та 9^1 Закону в Україні створюється та забезпечується функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози (далі – національна система реагування) та національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (далі – національна система обміну) щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом (далі – систем), об’єктів критичної інформаційної інфраструктури.

Суб’єктами національної системи реагування є:

Держспецзв’язку, яка є уповноваженим органом, що забезпечує її функціонування та функціонування національної системи обміну;

національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (далі – CERT-UA);

галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі – галузеві/регіональні CSIRT);

Національна поліція України, Служба безпеки України;

приватні команди реагування;

Національний координаційний центр кібербезпеки, який здійснює загальну координацію функціонування суб’єктів національної системи реагування.

Відповідно до частини третьої статті 5 Закону Кабінет Міністрів України затверджує національний план реагування.

В рамках функціонування національної системи обміну:

власники або розпорядники систем зобов’язані повідомляти відповідний галузевий/регіональний CSIRT про всі кіберінциденти;

власники або розпорядники об’єктів критичної інформаційної інфраструктури зобов’язані повідомляти відповідний галузевий/регіональний CSIRT про всі значні кіберінциденти;

органи державної влади, державні органи, органи місцевого самоврядування, які не є власниками або розпорядниками критичної інформаційної інфраструктури та отримали інформацію про кіберінцидент щодо критичної інформаційної інфраструктури, зобов'язані повідомляти галузевий/регіональний CSIRT про такі кіберінциденти.

Примітка. Наразі Адміністрацією Держспецзв'язку розроблено проект наказу щодо затвердження Порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та критеріїв визначення значного кіберінциденту, який оприлюднено на офіційному сайті для громадського обговорення.

Інформація про кіберінцидент, кібератаку щодо систем, об'єктів критичної інформаційної інфраструктури та про їхні наслідки є відкритою інформацією, крім інформації про характер, технічні характеристики, інші деталі кіберінциденту, кібератаки, що віднесена до інформації з обмеженим доступом.

Критерії віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мета розкриття такої інформації, у тому числі службової інформації для обміну в межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, порядок публічного інформування або звітування про реагування на кіберінциденти, кібератаки, порядок усунення їх наслідків затверджуються Кабінетом Міністрів України.

З метою підвищення ефективності функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, створення єдиної координаційної рамки реагування на кіберінциденти, кібератаки та кіберзагрози, а також гармонізації українського законодавства з вимогами Директиви Європейського Союзу щодо мережевої та інформаційної безпеки Адміністрацією Держспецзв'язку розроблено постанову Кабінету Міністрів України від 26 листопада 2025 року № 1533, яка затверджує:

Національний план реагування на кіберінциденти, кібератаки та кіберзагрози;

критерії віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мету розкриття такої інформації;

Порядок публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх наслідків.

Постанову Кабінету Міністрів України від 4 квітня 2023 року № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» визнати такою, що **втратила чинність**.

НАЦІОНАЛЬНИЙ ПЛАН
РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, КІБЕРАТАКИ ТА КІБЕРЗАГРОЗИ

(далі – Національний план)

Мета – визначає загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування та суб'єктами забезпечення кібербезпеки, їх роль в рамках функціонування національної системи реагування та національної системи обміну.

Основні терміни – «власна команда реагування на кіберінциденти, кібератаки та кіберзагрози (CSIRT)», «підрозділ з кіберзахисту», «подія кібербезпеки» та «ризик кібербезпеки» визначені у пункті 2 Національного плану.

Основні суб'єкти на кого поширюється дія Національного плану є:

основні суб'єкти національної системи кібербезпеки (частина друга статті 8 Закону);

суб'єкти національної системи реагування (стаття 9 Закону);

органи державної влади, державні органи, органи місцевого самоврядування;

оператори критичної інфраструктури;

власники або розпорядники об'єктів критичної інформаційної інфраструктури;

інші суб'єкти забезпечення кібербезпеки, які відповідно до законодавства залучені до виконання завдань в рамках функціонування національної системи реагування.

Національна система реагування – це комплекс правових та організаційно-технічних заходів і засобів, які забезпечують:

швидке виявлення кіберінцидентів та кібератак;

ідентифікацію та аналіз кіберзагроз;

оперативне інформування про кіберінциденти, кібератаки та кіберзагрози;

мінімізацію наслідків кіберінцидентів, кібератак та кіберзагроз;

усунення виявлених вразливостей;

відновлення сталого і надійного функціонування систем, об'єктів критичної інформаційної інфраструктури (далі - системи).

Загальна концепція щодо поширення на ролі Національного плану зображена на рисунку 1

Рисунок 1 – Загальна схема дії Національного плану реагування

Суб'єкти національної системи реагування та суб'єкти забезпечення кібербезпеки здійснюють **реагування** на кіберінциденти, кібератаки та кіберзагрози **послідовно за етапами**, які зображені на рисунку 2.

Рисунок 2 – Етапи реагування на кіберінциденти, кібератаки та кіберзагрози

У разі потреби під час реагування залучатися додаткові ресурси (кадрові та/або технічні) інших суб'єктів національної системи реагування, міжнародних партнерів, суб'єктів господарювання усіх форм власності або окремих експертів, що провадять діяльність у сфері кібербезпеки.

Примітка. Суб'єкти забезпечення кібербезпеки вживають заходів реагування на кожному з етапів з урахуванням методичних рекомендацій щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджених наказом Адміністрацією Держспецзв'язку від 18 лютого 2026 року № 143.

Модель організації реагування та формування CSIRT

Локальний рівень (Суб'єкт забезпечення кібербезпеки)

Відповідно до пункту 6 Національного плану реагування керівники з кіберзахисту або відповідальні особи, що виконують їх функцію та завдання, підрозділи з кіберзахисту здійснюють заходи з реагування щодо власних систем.

Суб'єкт забезпечення кібербезпеки може створити власну CSIRT:

у складі підрозділу з кіберзахисту;

як окремий структурний підрозділ;

як група визначних осіб.

Галузевий та регіональний рівень

Відповідно до пункту 7 Національного плану органи державної влади та органи місцевого самоврядування можуть створювати галузеві/регіональні CSIRT), а також залучати послуги приватних команд реагування (далі – приватні команди), що можуть виконувати в повному обсязі або частково завдання галузевої, регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) (рисунок 3).

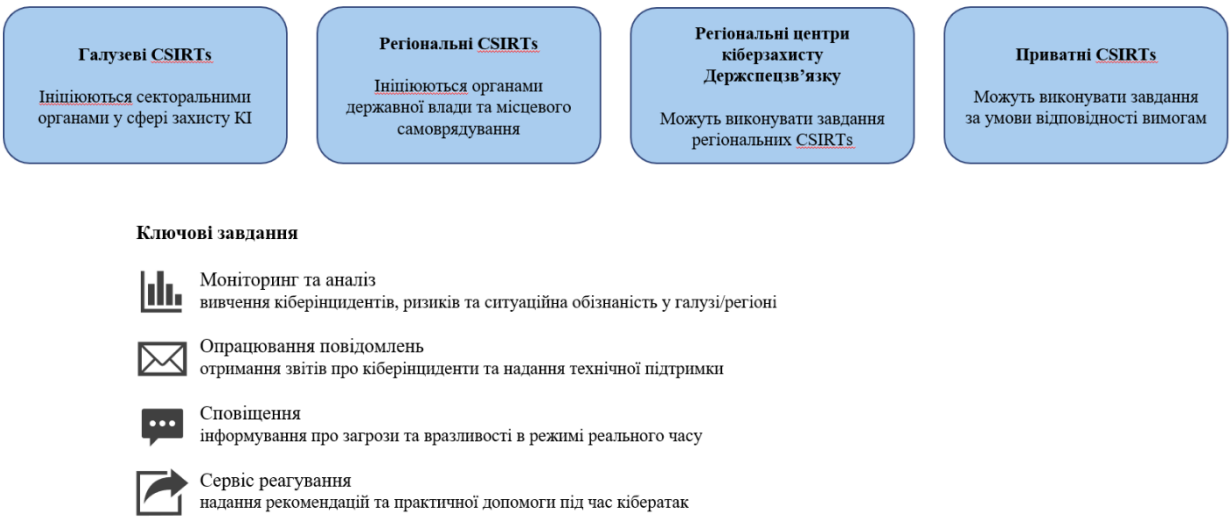

Рисунок 3 - Галузеві та регіональні CSIRTs

Примітка. Вимоги до організаційно-технічних спроможностей національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), буде затверджено наказом Адміністрацією Держспецзв'язку.

Для створення галузевої/регіональної CSIRT попередньо визначаються суб'єкти забезпечення кібербезпеки, які належать до відповідного сектору або регіону, на яких поширюватиметься діяльність відповідної галузевої/регіональної CSIRT.

Після створення галузевої/регіональної CSIRT протягом 15 календарних днів галузева/регіональна CSIRT або органи державної влади та органи місцевого самоврядування, у складі яких вони створені, інформують визначених суб'єктів листом про початок функціонування відповідної галузевої/регіональної CSIRT.

За відсутності галузевої/регіональної CSIRT у відповідній галузі, сфері або відповідному регіоні виконання завдань із реагування на кіберінциденти, кібератаки, кіберзагрози забезпечується CERT-UA.

СБУ забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки.

Організація та здійснення реагування на кіберінциденти, кібератаки та кіберзагрози

Пункти 8-29 Національного плану описують заходи, які проводяться суб'єктами національної системи реагування на кожному етапі реагування.

І-етап – Підготовка до реагування на кіберінциденти, кібератаки та кіберзагрози

Цей етап передбачає виконання комплексу організаційних, технічних та кадрових заходів з метою формування належного рівня готовності до запобігання, виявлення та ефективного реагування на кіберінциденти, кібератаки та кіберзагрози, які описуються в пунктах 8-9 Національного плану реагування, а також продемонстровані на рисунку 4.

Рисунок 4 – Підготовка до реагування

Примітка. На цьому етапі додатково рекомендується використовувати Методику оцінювання ризиків кібербезпеки, яка буде затверджено наказом Адміністрацією Держспецзв'язку, а також *Методичні рекомендації щодо реагування на кіберінциденти, кібератаки та кіберзагрози, яка затверджена наказом Адміністрацією Держспецзв'язку від 18 лютого 2026 року № 143.*

ІІ-етап – Виявлення, аналіз та інформування про кіберінциденти, кібератаки та кіберзагрози

Цей етап охоплює виявлення, первинний аналіз, класифікацію та інформування про кіберінциденти, кібератаки та кіберзагрози.

Його зміст полягає у:

постійному моніторингу систем;

зборі інформації про подій кібербезпеки, що можуть свідчити про наявність кіберінциденту, кібератаки, їх підтвердження та первинну оброку таких подій;

виявленні індикаторів компрометації та підозрілої активності;

ідентифікації та аналізі кіберзагрози;

інформуванні про кіберінциденти, кібератаки та кіберзагрози.

У пунктах 11-14 Національного плану реагування описується порядок ініціювання, класифікації та координації реагування на кіберінциденти, кібератаки й кіберзагрози в межах національної системи кібербезпеки. Загальна схема взаємодії та послідовність дій при реагуванні на кіберінцидент, кібератаку та кіберзагрозу представлено на рисунку 5.

Рисунок 5 – Алгоритм виявлення, аналізу та інформування про кіберінциденти, кібератаки, кіберзагрози

Відповідно до пункту 12 Національного плану реагування суб'єкти забезпечення кібербезпеки самостійно або у взаємодії з CERT-UA або відповідною галузевою/регіональною CSIRT визначають категорію кіберінциденту згідно з національною таксономією кіберінцидентів, його критичність за рівнями, які представлені на рисунку 6.

Рівень	Назва	Характеристика та вплив
Рівень 0	Некритичний (білий)	Не загрожує сталому функціонуванню систем
Рівень 1	Низький (зелений)	Загрожує функціонуванню, але не загрожує даним (збережено цілісність, конфіденційність і доступність)
Рівень 2	Середній (жовтий)	Створює передумови для порушення захищеності інформації та даних
Рівень 3	Високий (помаранчевий)	Загрожує функціонуванню систем, порушується захищеність інформації та даних, виникають потенційні загрози для національної безпеки і оборони, … припинення виконання функцій ОКІ
Рівень 4	Критичний (червоний)	Загрожує функціонуванню кількох систем, порушується захищеність, виникають реальні загрози для національної безпеки і оборони, … припинення виконання функцій ОКІ
Рівень 5	Надзвичайний (чорний)	Загрожує функціонуванню багатьох систем, порушується захищеність, виникають невідворотні загрози для функціонування держави або загроза життю людей

CERT-UA, CSIRTs, інші суб'єкти мають право **самостійно** розпочати реагування на кіберінциденти **високого, критичного та надзвичайного** рівня критичності. Про початок таких дій негайно інформується керівник з кіберзахисту суб'єкта забезпечення кібербезпеки

Рисунок 6 – Класифікація кіберінцидентів

Інформування про кіберінциденти, кібератаки та кіберзагрози здійснюється безперервно в режимі, наближеному до реального часу, з використанням платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та механізму "єдиного вікна" для інформування, дотримання загальних правил обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (протокол TLP).

Для обміну інформацією про кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки використовується адаптований програмний продукт "Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" (MISP-UA)", функціонування якого забезпечує Ситуаційний центр забезпечення кібербезпеки СБУ.

Примітка. Національна таксономія кіберінцидентів, Загальні правила обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (протокол TLP), а також Методичні рекомендації щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджено наказом Адміністрацією Держспецзв'язку від 18 лютого 2026 року № 143.

Алгоритм інформування про кіберінциденти описаний у пунктах 15-20 та візуально представлений на рисунку 7.

Повідомлення про кіберінцидент формується суб'єктами забезпечення кібербезпеки за формою, затвердженою Адміністрацією Держспецзв'язку, а банками, іншими особами, що провадять діяльність на ринку фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг за формою, затвердженою Національним банком.

Примітка. Форма повідомлення про кіберінцидент, кібератаку, кіберзагрозу затверджено наказом Адміністрацією Держспецзв'язку від 18 лютого 2026 року № 143.

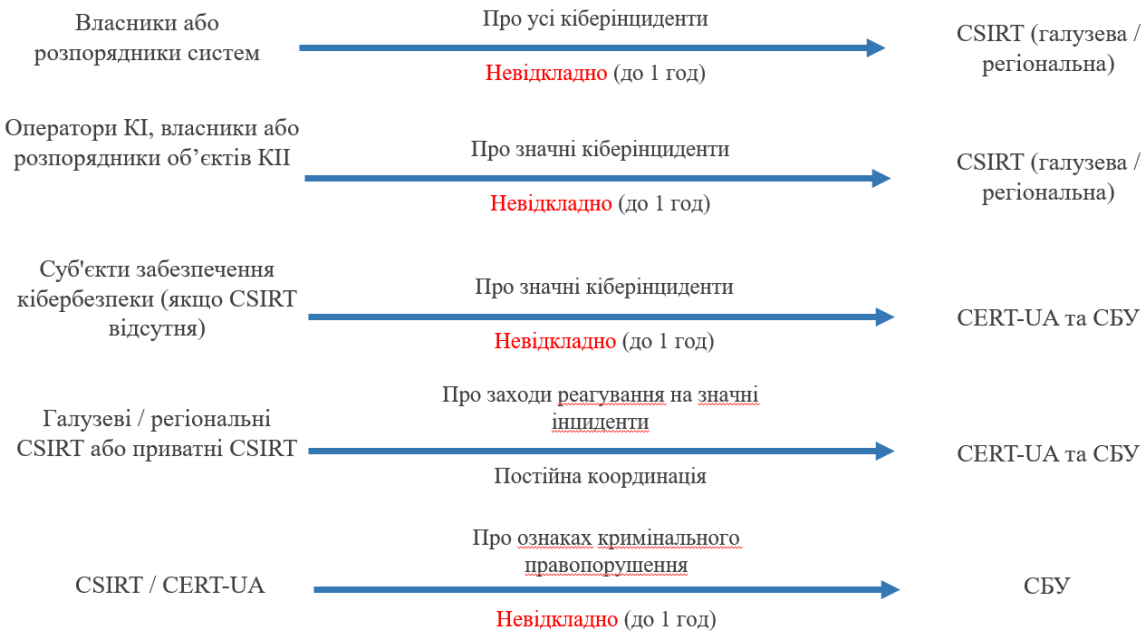

Рисунок 7 – Алгоритм інформування про кіберінциденти

CERT-UA, Ситуаційний центр забезпечення кібербезпеки СБУ, галузева/ регіональна CSIRT після отримання повідомлення про кіберінцидент у взаємодії із суб'єктом забезпечення кібербезпеки проводять аналіз інформації про рівень критичності кіберінциденту та у разі потреби уточнюють або коригують його з урахуванням інформації, яка може свідчити про масштабність кіберінциденту, його повторюваність або інші кіберзагрози.

Суб'єкти національної системи реагування відповідно до порядку обміну інформацією невідкладно інформують Національний координаційний центр кібербезпеки про всі значні кіберінциденти. Попереднє повідомлення - протягом 24 годин після виявлення значного кіберінциденту; поточний звіт - протягом 72 годин; остаточний звіт - протягом місяця після інциденту.

Примітка. Адміністрацією Держспецзв'язку розроблено проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та критеріїв визначення значного кіберінциденту», який оприлюднено на сайті для громадського обговорення.

III-етап – Стримування, усунення наслідків та відновлення після кіберінцидентів, кібератак та кіберзагроз

Пункти 21-24 Національного плану реагування регламентують процедуру під час якої суб'єкти забезпечення кібербезпеки самостійно або разом із суб'єктами національної системи реагування вживають заходів до зниження негативного впливу кіберінциденту, кібератаки, запобігання порушенню безпеки, несанкціонованому втручанню в їх роботу, забезпечення сталого, надійного та штатного режиму функціонування систем, захищеності

(конфіденційності, цілісності і доступності) інформації та даних, що у них обробляються (рисунок 8).

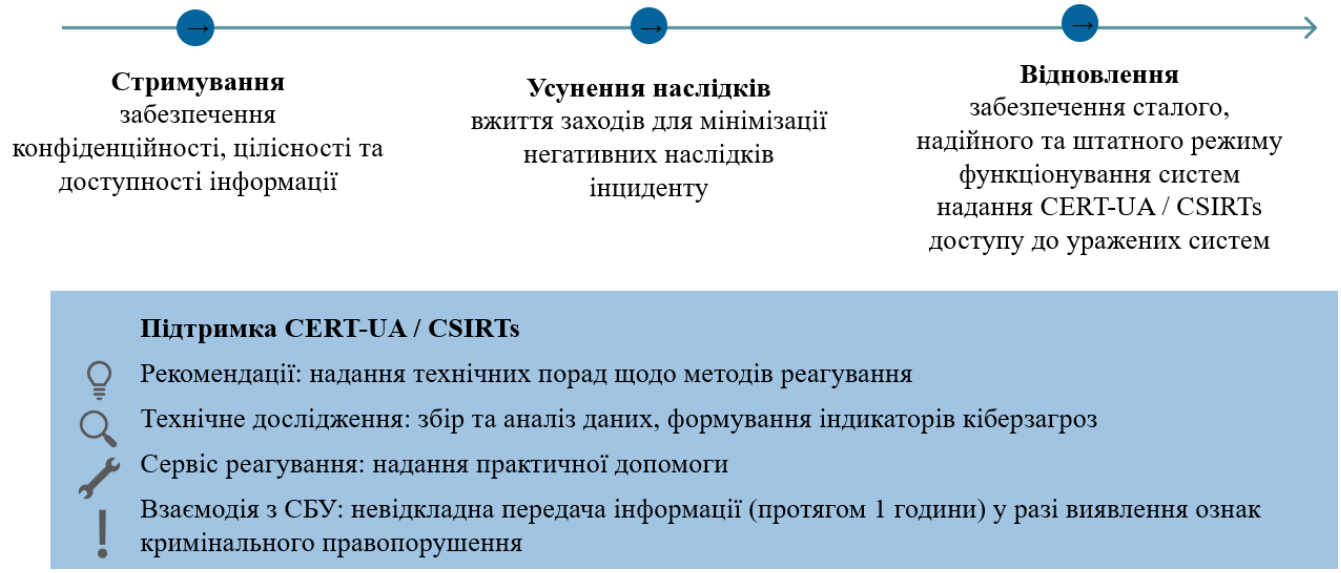

Рисунок 8 – Заходи під час стримування, усунення наслідків та відновлення

CERT-UA або відповідна галузева/регіональна CSIRT після отримання та опрацювання повідомлень про кіберінциденти, кібератаки, кіберзагрози надають суб'єктам забезпечення кібербезпеки рекомендації щодо можливих заходів реагування та технічної підтримки (у разі потреби), а також виконують інші дії, які показано на рисунку 9.

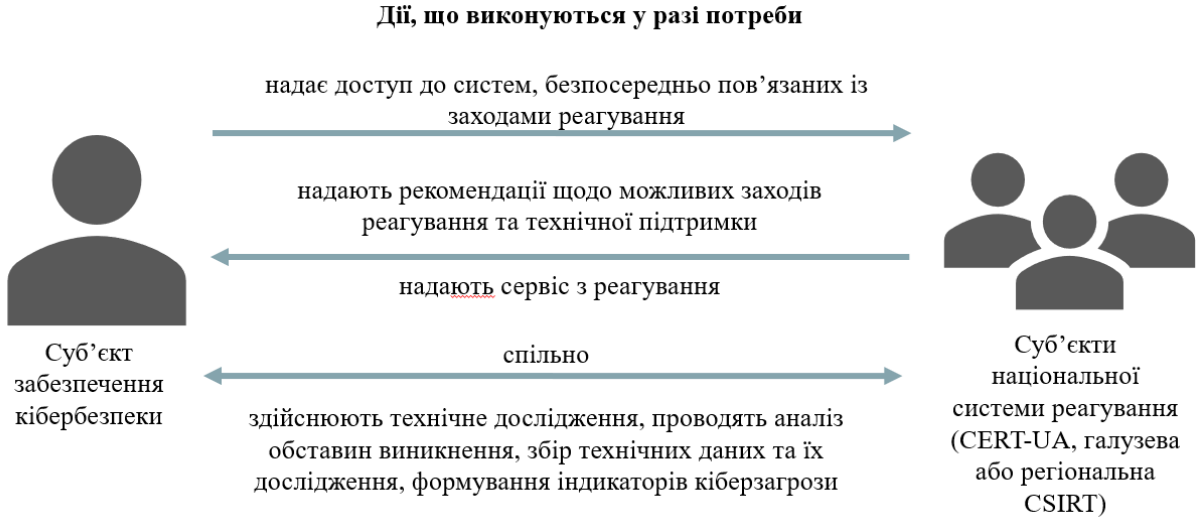

Рисунок 9 – Дії, що виконуються у разі потреби

Порядок надання командою реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT-NBU) сервісу з реагування на кіберінциденти, кібератаки, кіберзагрози затверджується Національним банком.

Важливо! Якщо під час технічного дослідження CERT-UA або відповідною галузевою/регіональною CSIRT виявлено ознаки кримінального

правопорушення, така інформація невідкладно (протягом години) передається до СБУ.

Відповідно до пункту 24 Національно плану реагування Адміністрація Держспецзв'язку та СБУ з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози в межах повноважень надають вимоги про реагування, які є обов'язковими до виконання суб'єктами забезпечення кібербезпеки. Загальний алгоритм надання таких вимог зображено на рисунку 10.

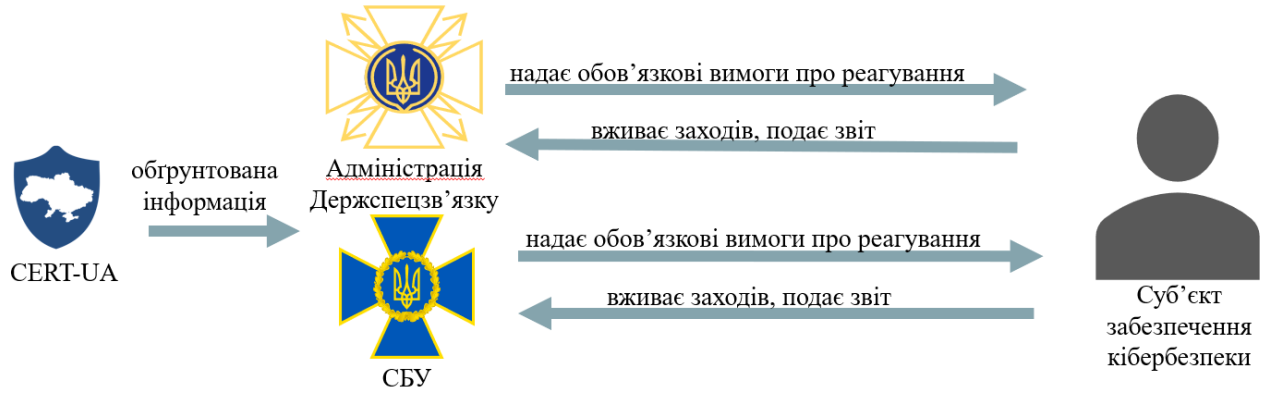

Рисунок 10 – Алгоритм надання вимог про реагування

Примітка. Адміністрацією Держспецзв'язку розроблено проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України ««Про затвердження Порядку визначення підстав для надання вимог про реагування на кіберінциденти, кібератаки, кіберзагрози та надання звіту про результати вжитих заходів реагування», який оприлюднено на сайті для громадського обговорення.

IV – Аналіз ефективності заходів реагування на кіберінциденти, кібератаки та кіберзагрози

Відповідно до пунктів 25-27 Національного плану реагування після завершення реагування на кіберінцидент суб'єкти кібербезпеки разом із CERT-UA, СБУ або галузевими CSIRT аналізують ефективність вжитих заходів. Результати фіксуються у звіті. Про інцидент обов'язково інформують CERT-UA та Ситуаційний центр СБУ (або відповідні CSIRT). Отриманий досвід використовується для посилення технічного захисту, оновлення внутрішніх політик, планів реагування та навчання персоналу, щоб запобігти подібним випадкам у майбутньому (рисунок 11).

Рисунок 11 – Заходи в рамках аналізу ефективності реагування

Публічне інформування про кіберінциденти (зокрема під час кризової ситуації) здійснюється відповідно до порядку, затвердженого постановою КМУ № 1533 від 26.11.2025.

Важливо! CERT-UA, галузева або регіональна CSIRT, інші суб'єкти національної системи реагування мають право самостійно розпочати реагування на кіберінциденти високого (помаранчевого), критичного (червоного) та надзвичайного (чорного) рівня критичності без попереднього погодження із суб'єктом забезпечення кібербезпеки, якщо зволікання може призвести до непоправних наслідків для національної безпеки, оборони, функціонування критичної інфраструктури або життя людей.

Про початок таких дій CERT-UA, галузева або регіональна CSIRT негайно інформує керівника з кіберзахисту або відповідальну особу, яка виконує функції та завдання керівника з кіберзахисту, суб'єкта забезпечення кібербезпеки.

Заходи реагування на кіберінциденти, кібератаки та кіберзагрози, що передбачають або можуть спричинити тимчасові обмеження роботи систем, що належать Міноборони, здійснюються за погодженням з Міноборони (в частині, що стосується Збройних Сил, - за погодженням з Генеральним штабом Збройних Сил) та проводяться разом з командами реагування на кіберінциденти, кібератаки та кіберзагрози Міноборони або Збройних Сил відповідно.

КРИТЕРІЇ
ВІДНЕСЕННЯ ІНФОРМАЦІЇ ПРО ХАРАКТЕР, ТЕХНІЧНІ ТА ІНШІ ДЕТАЛІ КІБЕРІНЦИДЕНТУ, КІБЕРАТАКИ ДО ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ, ПЕРЕЛІК ПІДСТАВ, ПОРЯДОК ТА МЕТА РОЗКРИТТЯ ТАКОЇ ІНФОРМАЦІЇ
(далі – Критерії)

Мета Критерій – визначення умов віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мету розкриття такої інформації, зокрема службової інформації для обміну в межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози.

Критерії застосовуються суб'єктами національної системи реагування, власниками або розпорядниками систем.

Відкритою інформацією є інформація про кіберінцидент, кібератаку щодо систем та про їх наслідки, а також інформація про індикатори кіберзагроз, отримана під час реагування на кіберінциденти, кібератаки, кіберзагрози.

До інформації з обмеженим доступом відноситься інформація про характер, технічні та інші деталі кіберінциденту, кібератаки щодо систем належить, якщо вона відповідає хоча б одному з критеріїв, які зазначені в пункті 5 Критеріїв.

Така інформація може бути повністю або частково розкрита власником або розпорядником систем у випадках, зазначених пунктом 7 Критеріїв.

Віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки щодо систем до інформації з обмеженим доступом, а також доступ до неї здійснюються власником або розпорядником системи.

ПОРЯДОК
ПУБЛІЧНОГО ІНФОРМУВАННЯ АБО ЗВІТУВАННЯ ПРО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, КІБЕРАТАКИ, УСУНЕННЯ ЇХ НАСЛІДКІВ

(далі – Порядок)

Порядок визначає процедури публічного інформування або звітування про реагування на кіберінциденти, кібератаки та усунення їх наслідків.

Дія Порядку поширюється на суб'єктів національної системи реагування, власників або розпорядників систем.

Публічне інформування здійснюється щодо кіберінцидентів, кібератаки від середнього рівня критичності та вище і лише в тому обсязі, який не створює додаткових загроз національній безпеці, не заважає реагуванню на кіберінциденти, кібератаки і не порушує вимог законодавства щодо захисту інформації з обмеженим доступом.

Основні деталі публічного інформування зображені на рисунку 12.

Рисунок 12 – особливості публічного інформування

РОЗ'ЯСНЕННЯ ДО ПОРЯДКУ ВЗАЄМОДІЇ СУБ'ЄКТІВ НАЦІОНАЛЬНОЇ СИСТЕМИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, КІБЕРАТАКИ, КІБЕРЗАГРОЗИ ІЗ СУБ'ЄКТАМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, ПРАВООХОРОННИМИ, КОНТРРОЗВІДУВАЛЬНИМИ, РОЗВІДУВАЛЬНИМИ ОРГАНАМИ ТА СУБ'ЄКТАМИ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ (ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ВІД 13 ЛИСТОПАДА 2025 Р. № 1471)

Законом України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» внесено зміни до Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закону), зокрема доповнення Закону новими статтями 9 та 9^1.

Відповідно до статей 9 та 9^1 Закону в Україні створюється та забезпечується функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози (далі – національна система реагування) та національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (далі – національна система обміну) щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом (далі – систем), об'єктів критичної інформаційної інфраструктури.

Однією із цілей національної системи реагування та національної системи обміну є забезпечення узгодження дій суб'єктів національної системи реагування та суб'єктів забезпечення кібербезпеки, спрямованих на швидке виявлення кіберінцидентів та кібератак, ідентифікацію та аналіз кіберзагроз, оперативне інформування про них, вжиття заходів для мінімізації їх наслідків, усунення виявлених вразливостей, впровадження організаційно-технічних заходів щодо створення національної системи обміну, забезпечення функціонування платформи обміну відповідною інформацією.

Суб'єктами національної системи реагування є:

Держспецзв'язку, яка є уповноваженим органом, що забезпечує її функціонування та функціонування національної системи обміну;

національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (далі – CERT-UA);

галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі - галузеві, регіональні CSIRT);

Національна поліція України, Служба безпеки України;

приватні команди реагування;

Національний координаційний центр кібербезпеки, який здійснює загальну координацію функціонування суб'єктів національної системи реагування.

Для належного функціонування національної системи реагування передбачається низка взаємодій в порядку, встановленому Кабінетом Міністрів України, а саме взаємодія:

CERT-UA з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності;

галузевих, регіональних CSIRT з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності, іншими суб'єктами національної системи реагування;

Національної поліції України, Служби безпеки України з іншими суб'єктами національної системи реагування.

Зазначені порядки взаємодії об'єдналися в одному Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності, який затверджений постановою Кабінету Міністрів України від 13 листопада 2025 року № 1471 (далі – Порядок).

Порядок описує:

взаємодію CERT-UA та галузевих, регіональних CSIRT з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності;

галузевих, регіональних CSIRT та Національної поліції України, Служби безпеки України з іншими суб'єктами національної системи реагування.

Взаємодія між суб'єктами національної системи реагування здійснюється у рамках національної системи реагування, національної системи обміну та за процедурами, визначеними національним планом реагування та порядком обміну інформацією.

Взаємодія CSIRT-ів (галузевих, регіональних, приватних) з CERT-UA та іншими суб'єктами національної системи здійснюється в порядку, який затверджує Адміністрація Держспецзв'язку.

Примітка. Наразі Адміністрацією Держспецзв'язку розробляється проекти наказів «Про затвердження Порядку взаємодії галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози із національною командою реагування на кіберінциденти, кібератаки, кіберзагрози та приватних команд реагування на кіберінциденти, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування» та «Про затвердження Порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози».

Взаємодія між суб'єктами національної системи реагування та правоохоронними, розвідувальними й контррозвідувальними органами та суб'єктами оперативно-розшукової діяльності здійснюється через:

обмін інформацією;

спільні заходи реагування;

надання даних, необхідних для слідства чи розвідки;

роботу міжвідомчих груп.

CERT-UA та галузеві, регіональні CSIRT мають невідкладно інформувати відповідні суб'єкти забезпечення кібербезпеки залежно від характеру кіберінциденту, кібератаки та кіберзагрози зокрема:

НКЦК – про всі значні кіберінциденти та кіберзагрози;

СБУ – про значні кіберінциденти, кібератаки, кіберзагрози, що стосуються систем, в яких обробляються державні інформаційні ресурси, службова інформація та інформація, що становить державну таємницю, а також об'єктів критичної інформаційної інфраструктури;

Нацполіцію – про значні кіберінциденти та кібератаки на об'єкти критичної інформаційної інфраструктури;

розвідувальні органи – про зовнішні кіберзагрози проти національної безпеки, в яких виявлено ознаки дій іноземних держав.

ДБР, НАБУ, БЕБ – про кіберінциденти, кібератаки, кіберзагрози, якщо є ознаки кримінальних правопорушень відповідної підслідності.

Примітка. Критерії віднесення кіберінциденту до значного визначає Адміністрація Держспецзв'язку.

Порядок визначає також вид інформації, інформування якою має забезпечувати СБУ, Національна поліція та розвідувальні органи в межах своїх повноважень, суб'єктів національної системи реагування.

СБУ – про актуальні кіберзагрози у сфері державної безпеки.

Національна поліція – про організацію, сили, засоби, методи, тактику дій злочинних угрупувань, що стали відомими в ході оперативно-розшукової діяльності та під час обміну інформацією з правоохоронними органами іноземних держав та міжнародними правоохоронними органами, правоохоронними і спеціальними службами інших держав та/або міжнародними правоохоронними організаціями.

розвідувальні органи – про зовнішні загрози національній безпеці у кіберпросторі, технічні розвідки іноземних держав, які діють у кіберпросторі, інші події і обставини, що стосуються сфери кібербезпеки.

Обмін інформацією про кіберінциденти, кібератаки, кіберзагрози здійснюється відповідно до протоколу TLP.

Примітка. Протокол TLP затверджений наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі».

CERT-UA, галузеві та регіональні CSIRT можуть організовувати та проводити спільні дії з правоохоронними, розвідувальними й контррозвідувальними органами та суб'єктами оперативно-розшукової діяльності у разі здійснення ними своїх повноважень, а також з урахуванням вимог кримінального процесуального законодавства та законодавства про контррозвідувальну діяльність та необхідності забезпечення безперервності реагування на кіберінциденти та кібератаки. Такі спільні дії включають:

технічне дослідження кіберінциденту та кібератаки;

аналіз обставин їх виникнення;

збір технічних даних із скомпрометованих або уражених систем та їх дослідження;

збирання, фіксацію та збереження відомостей в електронній формі.

Також Порядок передбачає, що CERT-UA, галузеві та регіональні CSIRT надають зазначеним органом та суб'єктам технічні та інших деталі кіберінциденту чи кібератаки, які необхідні їм для виконання своїх законних повноважень.

Порядок передбачає взаємодію в межах функціонування міжвідомчих груп із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки, зокрема в межах постійно діючої Об'єднаної групи реагування на кіберінциденти, кібератаки, кіберзагрози.

Примітка. Відповідно до підпункту 5 частини третьої статті 9 Закону України «Про основні засади забезпечення кібербезпеки» для забезпечення скоординованого, оперативного та ефективного реагування на кризову ситуацію у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою у складі НКЦК утворюється та функціонує постійно діюча Об'єднана група реагування на кіберінциденти, кібератаки, кіберзагрози, до складу якої входять представники НКЦК, Держспецзв'язку, СБУ, Національної поліції та представники інших основних суб'єктів національної системи кібербезпеки (за обґрунтованої необхідності).

Керівником Об'єднаної групи реагування, який затверджує її персональний склад та порядок роботи з урахуванням визначених законом компетенції та повноважень її учасників, є заступник керівника НКЦК.

Взаємодія в межах функціонування міжвідомчих груп передбачає:

обмін інформацією, технічними даними та результатами досліджень щодо кіберінцидентів, кібератак, кіберзагроз;

узгодження та координацію дій з локалізації та нейтралізації кіберінцидентів та кібератак, усунення їх наслідків;

визначення необхідності залучення додаткових ресурсів суб'єктів національної системи реагування або міжнародних партнерів;

проведення аналізу отриманої інформації, розроблення рекомендацій і пропозицій щодо подальших заходів реагування.

РОЗ’ЯСНЕННЯ
ЩОДО НАКАЗУ АДМІНІСТРАЦІЇ ДЕРЖСПЕЦЗВ'ЯЗКУ ВІД 18 ЛЮТОГО 2026 РОКУ № 143 «ДЕЯКІ ПИТАННЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, КІБЕРАТАКИ»

Наказ Адміністрації Держспецзв'язку від 18 лютого 2026 року № 143 «Деякі питання реагування на кіберінциденти, кібератаки» (далі – наказ № 143) затверджений з метою підвищення ефективності реагування на кіберінциденти, кібератаки та кіберзагрози (далі – КІ, КА, КЗ).

Зазначеним наказом затверджуються:

Методичні рекомендації щодо реагування на КІ, КА, КЗ;

Загальні правила обміну інформацією про кіберінциденти (протокол TLP);

Національна таксономію кіберінцидентів;

Форма повідомлення про КІ, КА, КЗ.

Також визнається таким, що втратив чинність, наказ 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» (далі – наказ № 570).

Основні відмінності наказу № 143 від наказу № 570:

оновлена законодавча та нормативно-правова база;

різні види подій в кіберпросторі доповнено кіберзагрозами;

окремий фокус на використанні ризико-орієнтованого підходу (управління ризиками кібербезпеки) у сфері реагування на КІ, КА, КЗ;

кількість етапів реагування зменшено з 6 (шести) етапів до 4 (чотирьох) етапів задля більш системного та комплексного підходу до реагування;

деякі додатки до наказу № 570 тепер затверджено як окремі документи (Загальні правила обміну інформацією про кіберінциденти (протокол TLP), Національна таксономія кіберінцидентів та Форма повідомлення про КІ, КА, КЗ);

Перелік категорій і типів кіберінцидентів з наказу № 570 доповнено та трансформовано в Національну таксономію кіберінцидентів.

ЩОДО МЕТОДИЧНИХ РЕКОМЕНДАЦІЙ ЩОДО РЕАГУВАННЯ НА КІ, КА, КЗ

Методичні рекомендації щодо реагування на кіберінциденти, кібератаки та кіберзагрози (далі – Рекомендації) розроблено на основі кращих світових практик (NIST, CISA, MITRE ATT&CK) та національних стандартів для систематизації дій суб’єктів забезпечення кібербезпеки.

Ці Рекомендації мають інформаційний та рекомендаційний характер. Вони є добровільними, проте їх впровадження критично важливе для

забезпечення сталого функціонування ІКС у разі виникнення позаштатних ситуацій.

Послідовність заходів до кіберзахисту етапів реагування на кіберінциденти, кібератаки, кіберзагрози графічно наведено у додатку 1 до Рекомендацій.

Типовий перелік заходів з реагування на кіберінциденти, кібератаки, кіберзагрози для одночасного відстеження заходів наведено у додатку 2 до Рекомендацій, що відстежувати усі заходи з кіберзахисту (у формі чекліста).

Крок 1: Етап підготовки до реагування на КІ, КА та КЗ

Підготовка до реагування на кіберінциденти, кібератаки, кіберзагрози починається заздалегідь до того, як вони відбудуться, заради пом'якшення будь-якого впливу на об'єкти кіберзахисту суб'єкта забезпечення кібербезпеки. На цьому етапі потрібно також призначити відповідальних за реагування на КІ, КА, КЗ співробітників (команди реагування на КІ, КА, КЗ) з-поміж персоналу підрозділу з кіберзахисту або інших структурних підрозділів.

На цьому етапі необхідно забезпечити:

чітке управління ризиками: ідентифікацію активів, оцінку вразливостей та встановлення показників «штатного» режиму функціонування;

ефективне документування: розроблення внутрішніх політик реагування, планів на випадок надзвичайних ситуацій та інструкцій для персоналу;

надійний інструментарій: впровадження систем виявлення вторгнень (IDS/IPS), брандмауерів, систем захисту кінцевих точок (EDR/XDR), збору логів (SIEM) та інших рішень;

періодичне навчання: проведення регулярних тренінгів та інструктажів з кібергігієни для усіх працівників.

Для цього етапу створений окремий перелік заходів для одночасного відстеження (чекліст), що допоможе відповідальним співробітникам впровадити усі необхідні заходи з кіберзахисту та бути підготовленими до реагування.

Крок 2: Етап виявлення, аналізу та інформування про КІ, КА, КЗ

Найскладніше завдання – точне виявлення та оцінювання можливих подій кібербезпеки, визначення того, чи стався кіберінцидент, кібератака або є кіберзагроза, і якщо це трапилося, визначення типу та масштабу компрометації систем/мереж, що були (або можуть бути) уражені.

Алгоритм дій на цьому етапі:

1. *Збір даних*: у разі підозри необхідно негайно забезпечити збереження журналів (логів), дампів оперативної пам'яті та образів дисків.

2. *Класифікація*: визначення категорії та типу інциденту згідно з національною таксономією кіберінцидентів.

3. *Пріоритизація*: якщо подій декілька, першочергово зменшуємо наслідки для систем, що впливають на критичні бізнес-процеси та надання послуг

Важливо, що про будь-яку кібератаку інформують національну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідну галузеву/регіональну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, за формою повідомлення про кіберінцидент, кібератаку, кіберзагрозу, яка також затверджена цим наказом.

Для об'єктивної оцінки рівня критичності кіберінциденту використовується система за трьома критеріями:

Критерій А: Загроза штатному режиму функціонування (від відсутності загрози до транскордонного впливу).

Критерій Б: Загроза порушення властивностей інформації.

Критерій В: Загроза національній безпеці, економіці чи життю громадян.

За результатами зіставлення визначається рівень від 0 (білий – некритичний) до 5 (чорний – надзвичайний) відповідно до таблиці Визначення рівня критичності кіберінцидентів. Зіставлення критеріїв критичності кіберінциденту необхідно здійснювати послідовно від А до В.

Крок 3: Етап стримування, усунення наслідків і відновлення після КІ, КА, КЗ

Метою цього етапу є припинення подальшої діяльності зловмисника, мінімізація та повне усунення наслідків кіберінциденту (для запобігання повторному проникненню), а також безпечне відновлення штатного режиму функціонування систем і мереж.

Відповідно до даного етапу, подальшими кроками є:

стримування: ізоляція уражених сегментів мережі, блокування скомпрометованих облікових записів, оновлення правил брандмауера;

усунення: видалення шкідливого ПЗ, заміна скомпрометованих файлів з чистих резервних копій, встановлення необхідних патчів;

відновлення: поступове підключення систем до мережі, ретельне тестування та посилений моніторинг операцій протягом часу тестування.

Крок 4: Етап аналізу ефективності заходів реагування на КІ, КА, КЗ

На цьому етапі необхідно задокументувати усі події кібербезпеки (сформувати звіту щодо реагування на КІ, КА, КЗ), поінформувати керівництво, удосконалити захисні пристрої систем/мереж, переглянути документацію та політики для запобігання подібним подіям кібербезпеки у майбутньому відповідно до набутого досвіду. Крім того, необхідно:

підготувати остаточний звіт про КІ, КА, КЗ;

удосконалити налаштування засобів захисту на основі ТТП (тактик і технік) зловмисника;

переглянути посадові інструкції та плани реагування.

ЩОДО ЗАГАЛЬНИХ ПРАВИЛ ОБМІНУ ІНФОРМАЦІЄЮ ПРО КІБЕРІНЦИДЕНТИ (ПРОТОКОЛ TLP)

Загальні правила обміну інформацією (протокол TLP) базуються на міжнародному стандарті форуму команд реагування на інциденти FIRST щодо протоколу TLP v.2.0 та рекомендаціях CISA. Це система маркування, яка дозволяє стороні, що надає інформацію, чітко вказати межі її поширення. Це створює довіру між суб'єктами забезпечення кібербезпеки: наприклад, суб’єкт знає, що його дані не потраплять у медіа, якщо вони промарковані як «червоні».

Кожен колір визначає коло осіб, які можуть бачити повідомлення (рисунок 13).

Призначений для використання під час формування повідомлень про кіберінцидент

TLP:RED (ЧЕРВОНИЙ)	Не для поширення, тільки для кінцевого одержувача
TLP:AMBER (ЖОВТИЙ)	Обмежене поширення, доступне тільки серед представників організації, що є кінцевим одержувачем, або її клієнтів
TLP:GREEN (ЗЕЛЕНИЙ)	Обмежене поширення, доступне тільки для представників спільноти або сектору
TLP:CLEAR (БІЛИЙ)	Необмежене поширення

Рисунок 13 – Протокол TLP

Текст: мітка пишеться великими літерами (наприклад, TLP:RED).

Шрифт: не менше 12 пунктів.

Електронні листи: мітка обов'язково вказується в темі листа та безпосередньо в тексті перед самою інформацією.

Паперові документи: мітка ставиться у верхньому та нижньому колонтитулах кожної сторінки.

Колір міток: для того, щоб мітки були помітними, Протоколом встановлено конкретні колірні моделі, які наведено в таблиці Кольори для міток TLP.

Важливо ! Протокол TLP не призначений для позначення інформації, що становить державну, банківську таємницю та службову інформацію. Така інформація передається відповідно до законодавства України..

Дозвіл на поширення. Якщо суб’єктом отримано інформацію з міткою TLP:AMBER, але є необхідність її публікації, суб’єкт зобов’язаний отримати письмовий дозвіл від відправника.

ЩОДО НАЦІОНАЛЬНОЇ ТАКСОНОМІЇ КІБЕРІНЦИДЕНТІВ

Рекомендації кажуть, як діяти, Протокол TLP – вказує межі на поширення інформації, Національна таксономія кіберінцидентів (далі − Таксономія) впроваджує єдиний перелік категорій та типів кіберінцидентів як інструменту для обміну інформацією щодо кіберінцидентів.

Таксономія розроблена на основі стандартів ENISA та Європолу. Вона впроваджує єдину систему класифікації, щоб усі суб'єкти кібербезпеки однаково розуміли природу подій.

Суб’єкти забезпечення кібербезпеки застосовують цю Таксономію для формування у разі потреби власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням найменування категорій кіберінцидентів, визначених цією Таксономією (таблиця), а також при обміні та поширенні інформації про кіберінциденти, підготовці звітів і публічних повідомлень про кіберінциденти відповідно до пункту 12 Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози. затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533.

Кожен кіберінцидент отримує свій цифровий код, що складається з коду категорії (XX.) та коду типу (.XX). Наприклад, код 02.01 означає: Категорія «Шкідливий програмний код», тип «Зараження ШПЗ».

Таксономія виділяє 12 категорій кіберінцидентів (рисунок 14).

Код	Категорія інциденту	Тип інциденту
01.	Шкідливий (образливий) вміст (Abusive content)	Спам Загрозливий вміст Дезінформація / Неправдивий вміст
02.	Шкідливий програмний код (Malicious Code)	Зараження / виконання ШПЗ Розповсюдження ШПЗ Сервер керування (C&C) Шкідливе підключення
03.	Збір інформації (Information Gathering)	Сканування Перебір Соціальна інженерія
04.	Спроби втручання (Intrusion Attempts)	Спроба експлуатація вразливості Спроби автентифікації
05.	Втручання (Intrusion)	Несанкціонований доступ Компрометація системи Компрометація додатка Несанкціоноване використання ресурсів
06.	Порушення доступності (Availability)	Атака на відмову в обслуговуванні (DoS/DDoS) Саботаж Випадковий збій Програми-вимагачі
07.	Порушення властивостей інформації (Information Content Security)	Несанкціонований доступ до інформації Несанкціонована модифікація Несанкціоноване розкриття Підозра на витік даних Викриття облікових даних Збір платіжних даних

08.	Шахрайство (Fraud)	Збір платіжних даних Імперсонація Шахрайство Порушення авторських прав
09.	Вразливість (Vulnerability)	Відома вразливість Некоректна конфігурація Відкритий сервіс
10.	Порушення політик (Policies Violation)	Використання нелегітимного ПЗ Порушення політик безпеки
11.	Порушення фізичної безпеки (Physical Security Breach)	Втрачений або вкрадений пристрій Несанкціонований фізичний доступ
12.	Адміністративний (Administrative)	Інше Не кіберінцидент

Рисунок 14 – Національна таксономія кіберінцидентів

Чому це важливо? Єдиний перелік категорій та типів кіберінцидентів дозволяє:

автоматизувати звітність, коли відбувається звітування, використання категорій та типів з Таксономії дозволяє аналітикам та експертам швидше обробляти дані;

покращити аналітичне відстеження та пріоритезацію: можливість відстеження, які типи атак найчастіше трапляються у конкретного суб'єкта (наприклад, якщо 80% інцидентів – це код 10.02, потрібно терміново переглянути політику паролів);

підвищити гнучкість: якщо суб'єкт з зіткнулися з новим видом загрози, якого немає в списку, можна встановити новий код у межах існуючої категорії (наприклад, 01.04).

ЩОДО ФОРМИ ПОВІДОМЛЕННЯ ПРО КІ, КА, КЗ

Форма повідомлення про КІ, КА, КЗ (далі – Форма) розроблена з метою отримання повної технічної та організаційної інформації про подію кібербезпеки та максимально швидко відреагувати на неї.

Для заповнення Форми необхідно виконати ряд кроків.

Крок 1: Маркування та ідентифікація

Мітка TLP: необхідно вибрати колір мітки (RED, AMBER, GREEN або CLEAR) відповідно до Протоколу TLP, щоб визначити, як національна команда реагування на КІ, КА, КЗ (CERT-UA) або галузева/регіональна команда реагування на КІ, КА, КЗ може поширювати інформацію.

Час виявлення: зазначається точний час у форматі GMT.

Дані заявника: інформація про контактну особу, з якою технічні фахівці зможуть зв'язатися для уточнення даних.

Крок 2: Оцінка ситуації та джерело виявлення

Джерело: необхідно вказати яким чином було виявлено проблему: від антивірусу, системи EDR, IDS/IPS чи безпосередньо від адміністратора/користувача.

Рівень критичності: необхідно вибрати рівень від 0 (білий) до 5 (чорний), спираючись на критерії з Рекомендацій.

Сектор: зазначається галузь (наприклад, урядова організація, фінансовий сектор або енергетика) та доменна зону.

Крок 3: Технічні деталі компрометації

Цей блок є найважливішим для технічного аналізу:

Таксономія: зазначається категорію та тип інциденту (наприклад, 02.01 — Зараження ШПЗ).

Об’єкти кібервпливу: для кожної ураженої системи (сервера чи робочої станції) необхідно вказати операційну систему та її налаштування, перелік використаних вразливостей (CVE), облікові записи, які могли бути скомпрометовані, масштаб − кількість уражених систем (1-10, 10-50 тощо).

Крок 4: Координація та допомога

Потреба в допомозі: необхідно чітко зазначити «Так» або «Ні» у полі щодо потреби залучення фахівців національної команди реагування на КІ, КА, КЗ (CERT-UA) або галузевої/регіональної команди реагування на КІ, КА, КЗ.

Інформування інших: необхідно надати інформацію чи було повідомлено про подію кібербезпеки СБУ, Кіберполіцію, НБУ чи НКЦК. Це допоможе уникнути дублювання запитів та скоординувати дії сил кіберзахисту та основних суб'єктів забезпечення кібербезпеки (за потреби).

Крок 5: Індикатори компрометації (IoC)

Наприкінці форми необхідно додати конкретні «сліди» зловмисника:

Мережеві: IP-адреси, домени, URL-посилання.

Хостові: шляхи до файлів, підозрілі команди, гілки реєстру.

Файлові: назви файлів та їхні хеш-суми (MD5 та інші).

Важливо! Не потрібно намагатися заповнити форму ідеально, якщо час іде на хвилини. Головне – надіслати первинну інформацію про факт КІ, КА, КЗ та потребу в допомозі, а технічні деталі (наприклад, індикатори компрометації) можна додати згодом.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку Дмитро ПАХОЛЬЧЕНКО