ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 26 листопада 2025 р. № 1533

НАЦІОНАЛЬНИЙ ПЛАН
реагування на кіберінциденти, кібератаки та кіберзагрози

Загальні положення

1. Цей Національний план визначає загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та суб'єктами забезпечення кібербезпеки, їх роль в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози (далі — національна система реагування) та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (далі — національна система обміну інформацією).

2. У цьому Національному плані терміни вживаються в такому значенні:

власна команда реагування на кіберінциденти, кібератаки та кіберзагрози (CSIRT) — структурний підрозділ або група осіб суб'єкта забезпечення кібербезпеки, що у межах повноважень виконує завдання із реагування на кіберінциденти, кібератаки та кіберзагрози;

підрозділ з кіберзахисту — структурний підрозділ або група осіб суб'єкта забезпечення кібербезпеки, що у межах повноважень виконує завдання із забезпечення кібербезпеки та кіберзахисту та здійснює захист інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури (далі — системи);

подія кібербезпеки — ідентифікована (навмисна або ненавмисна) дія в системі, електронній комунікаційній мережі або стан системи, електронної комунікаційної мережі, яка становить або може становити загрозу сталому, надійному та штатному режиму функціонування системи, електронної комунікаційної мережі та/або порушення конфіденційності, цілісності, доступності інформації в системі, електронній комунікаційній мережі та бути ознакою або передумовою кіберінциденту, кібератаки;

ризик кібербезпеки — можливість виникнення кіберінциденту та/або реалізації кіберзагрози, що може призвести до завдання шкоди або втрат,

а також становить загрозу для забезпечення функціональності, безперервності роботи, відновлюваності, цілісності та стійкості систем.

Інші терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про критичну інфраструктуру”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Державну службу спеціального зв’язку та захисту інформації України”.

3. Дія цього Національного плану поширюється на основних суб’єктів національної системи кібербезпеки, суб’єктів національної системи реагування, органи державної влади, державні органи, органи місцевого самоврядування, операторів критичної інфраструктури, власників або розпорядників об’єктів критичної інформаційної інфраструктури, інших суб’єктів забезпечення кібербезпеки, які відповідно до законодавства залучені до виконання завдань в рамках функціонування національної системи реагування.

4. Національна система реагування є комплексом правових та організаційно-технічних заходів і засобів, спрямованих на швидке виявлення кіберінцидентів та кібератак, ідентифікацію та аналіз кіберзагроз, оперативне інформування про них, вжиття заходів для мінімізації їх наслідків, усунення виявлених вразливостей, а також відновлення сталого і надійного функціонування систем.

5. Реагування на кіберінциденти, кібератаки та кіберзагрози здійснюється суб’єктами національної системи реагування та суб’єктами забезпечення кібербезпеки послідовно за такими етапами, як підготовка до реагування на кіберінциденти, кібератаки та кіберзагрози, виявлення, аналіз та інформування про кіберінциденти, кібератаки та кіберзагрози, стримування, усунення наслідків та відновлення після кіберінцидентів, кібератак та кіберзагроз, а також аналіз ефективності заходів реагування на кіберінциденти, кібератаки та кіберзагрози.

Суб’єкти забезпечення кібербезпеки вживають заходів реагування на кожному з етапів з урахуванням методичних рекомендацій щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджених Адміністрацією Держспецзв’язку.

У разі потреби під час реагування відповідно до законодавства можуть 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.

6. Керівники з кіберзахисту або відповідальні особи, які виконують функції та завдання керівників з кіберзахисту, підрозділи з кіберзахисту суб’єктів забезпечення кібербезпеки безпосередньо здійснюють заходи з

реагування на кіберінциденти, кібератаки та кіберзагрози щодо власних систем.

Для виконання завдань із реагування на кіберінциденти, кібератаки та кіберзагрози суб'єкт забезпечення кібербезпеки може створити власну команду реагування на кіберінциденти, кібератаки та кіберзагрози (CSIRT) у складі підрозділу з кіберзахисту або як окремий структурний підрозділ, або групу осіб.

7. Органи державної влади та органи місцевого самоврядування як суб'єкти забезпечення кібербезпеки в установленому законодавством порядку можуть створювати галузеві або регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), а також залучати послуги приватних команд реагування, що можуть виконувати в повному обсязі або частково завдання галузевої, регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), з урахуванням вимог до організаційно-технічних спроможностей національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), затверджених Адміністрацією Держспецзв'язку.

Створення галузевих команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) ініціюється секторальними органами у сфері захисту критичної інфраструктури.

Створення регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) ініціюється органами державної влади та органами місцевого самоврядування з урахуванням адміністративно-територіального устрою.

Регіональні центри кіберзахисту Держспецзв'язку можуть виконувати завдання регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) для відповідного регіону.

Створення галузевих або регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) здійснюється після попереднього визначення суб'єктів забезпечення кібербезпеки, які належать до відповідного сектору або регіону, на яких поширюватиметься діяльність відповідної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT). За результатами такого визначення галузеві або регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) або органи державної влади та органи місцевого самоврядування, у складі яких вони створені, протягом 15 календарних днів з дня створення надсилають суб'єктам забезпечення кібербезпеки та суб'єктам національної системи реагування лист про початок функціонування відповідної галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT).

Галузеві або регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) діють у складі національної системи обміну інформацією та національної системи реагування з урахуванням нормативно-правових та організаційно-розпорядчих актів органів державної влади та органів місцевого самоврядування, у сфері управління яких вони перебувають.

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

СБУ забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки з урахуванням особливостей, встановлених законодавством у зазначеній сфері.

Підготовка до реагування на кіберінциденти, кібератаки та кіберзагрози

8. Реагування на кіберінциденти, кібератаки та кіберзагрози розпочинається з етапу підготовки, під час якого суб'єктами національної системи реагування та суб'єктами забезпечення кібербезпеки проводяться заходи з вивчення та дослідження існуючих видів кіберінцидентів, кібератак та кіберзагроз, розроблення методів і механізму запобігання та протидії можливим кіберінцидентам та кібератакам.

9. Під час зазначеного етапу суб'єкти забезпечення кібербезпеки створюють організаційні, технічні та кадрові умови для ефективного реагування на кіберінциденти, кібератаки та кіберзагрози та, зокрема:

планують заходи з реагування на кіберінциденти, кібератаки та кіберзагрози на постійній та системній основі з урахуванням результатів управління ризиками кібербезпеки;

забезпечують взаємодію між своїми керівниками з кіберзахисту або відповідальними особами, які виконують функції та завдання керівників з кіберзахисту, або підрозділами з кіберзахисту та власними командами реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) (за наявності) та суб'єктами національної системи реагування;

розробляють та підтримують в актуальному стані стандартні операційні процедури для реагування на різні категорії кіберінцидентів, кібератак з урахуванням методичних рекомендацій щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджених Адміністрацією Держспецзв'язку;

організовують та забезпечують регулярне навчання з питань реагування на кіберінциденти, кібератаки та кіберзагрози для своїх співробітників, яке проводиться диференційовано залежно від функціональних обов'язків та з урахуванням професійної кваліфікації співробітників;

створюють технічні можливості підключення власних систем до засобів і технічних систем реагування суб'єктів національної системи реагування, зокрема до системи реагування на кіберінциденти, кібератаки, кіберзагрози щодо об'єктів кіберзахисту, функціонування та розвиток якої забезпечується Державним центром кіберзахисту Держспецзв'язку.

Виявлення, аналіз та інформування про кіберінциденти, кібератаки та кіберзагрози

10. На етапі виявлення, аналізу та інформування суб'єкти національної системи реагування та суб'єкти забезпечення кібербезпеки проводять постійний моніторинг систем, збір інформації про події кібербезпеки, що можуть свідчити про наявність кіберінциденту, кібератаки, проводять підтвердження та первинну обробку таких подій, виявлення індикаторів компрометації та підозрілої активності, ідентифікують та аналізують кіберзагрози, а також здійснюють інформування про кіберінциденти, кібератаки та кіберзагрози.

11. Ініціювання реагування на кіберінциденти, кібератаки, кіберзагрози та відповідне інформування здійснюються у разі:

виявлення кіберінцидентів, кібератак, кіберзагроз суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози щодо суб'єктів забезпечення кібербезпеки, зокрема шляхом використання засобів та технічних систем реагування на кіберінциденти, кібератаки, кіберзагрози, моніторингу кіберпростору, отримання інформації за результатами пошуку та/або виявлення потенційних вразливостей в системах, із платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, а також інформації, отриманої з інших джерел, отриманої у межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

виявлення суб'єктами забезпечення кібербезпеки кіберінцидентів, кібератак і кіберзагроз щодо систем, власниками або розпорядниками яких вони є, зокрема шляхом інформування співробітниками суб'єкта забезпечення кібербезпеки та використання засобів і технічних систем реагування на кіберінциденти, кібератаки, кіберзагрози.

12. Якщо подія кібербезпеки віднесена до кіберінциденту, суб'єкти забезпечення кібербезпеки самостійно або у взаємодії з національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідною галузевою/регіональною командою реагування

на кіберінциденти, кібератаки, кіберзагрози (CSIRT) визначають категорію кіберінциденту згідно з національною таксономією кіберінцидентів, яка затверджується Адміністрацією Держспецзв'язку, а також визначають його критичність відповідно до методичних рекомендацій щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджених Адміністрацією Держспецзв'язку, за такими рівнями:

рівень 0, некритичний (білий) — кіберінцидент не загрожує сталому, надійному та штатному режиму функціонування систем;

рівень 1, низький (зелений) — кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що в них обробляються;

рівень 2, середній (жовтий) — кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що в них обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою;

рівень 3, високий (помаранчевий) — кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що в них обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою;

рівень 4, критичний (червоний) — кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що в них обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою;

рівень 5, надзвичайний (чорний) — кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що в них обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю людей.

Визначення категорії кіберінциденту здійснюється суб'єктами національної системи реагування та суб'єктами забезпечення кібербезпеки відповідно до національної таксономії кіберінцидентів.

13. Якщо подія кібербезпеки класифікована як кібератака, суб'єкти забезпечення кібербезпеки невідкладно інформують про неї в порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, затвердженого Адміністрацією Держспецзв'язку (далі — порядок обміну інформацією) національну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідну галузеву/регіональну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) та в подальшому разом вживають оперативних заходів для запобігання її реалізації, мінімізації потенційних наслідків згідно з рекомендаціями, наданими відповідною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT).

14. У разі виявлення кіберзагрози суб'єкти забезпечення кібербезпеки ідентифікують її та проводять первинний аналіз, інформують про неї національну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідну галузеву/регіональну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) в установленому порядку, забезпечують обмін технічною інформацією про загрозу та в подальшому вживають превентивних заходів до усунення вразливостей та посилення кіберзахисту, а також здійснюють моніторинг для запобігання можливій кібератаці чи кіберінциденту.

15. 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), визначених Адміністрацією Держспецзв'язку.

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.

16. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) відповідно до порядку обміну інформацією надають суб'єктам забезпечення кібербезпеки попередження про кіберзагрози, забезпечують інформування про кіберінциденти, кібератаки, кіберзагрози у режимі за можливості, наближеному до реального часу.

17. Власники або розпорядники систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, відповідно до порядку обміну інформацією невідкладно (протягом години) повідомляють галузевій або регіональній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) про всі кіберінциденти.

Оператори критичної інфраструктури, власники або розпорядники об'єктів критичної інформаційної інфраструктури відповідно до порядку обміну інформацією невідкладно (протягом години) повідомляють відповідній галузевій/регіональній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) про всі значні кіберінциденти.

Галузеві, регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) або приватні команди реагування, що виконують їх завдання, координують свою діяльність та інформують національну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) і Ситуаційний центр забезпечення кібербезпеки СБУ про відповідні заходи реагування.

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.

18. За відсутності галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) у відповідній галузі (сфері) або у відповідному регіоні суб'єкти забезпечення кібербезпеки невідкладно (протягом години) повідомляють національній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) та Ситуаційному центру забезпечення кібербезпеки СБУ про всі значні кіберінциденти.

19. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), Ситуаційний центр забезпечення кібербезпеки СБУ, галузева або регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (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.

20. 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.

Критерії віднесення кіберінциденту до значного визначає Адміністрація Держспецзв'язку.

Стримування, усунення наслідків та відновлення після кіберінцидентів, кібератак та кіберзагроз

21. Під час етапу стримування, усунення наслідків та відновлення 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.

22. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідна галузева/регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (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).

За такої потреби національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідна галузева/регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) надає сервіс з реагування відповідно до вимог до сервісу з реагування на кіберінциденти, затверджених Адміністрацією Держспецзв'язку.

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

23. Під час надання сервісу з реагування на кіберінциденти національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідна галузева/регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) у взаємодії із суб'єктом забезпечення кібербезпеки здійснює технічне дослідження кіберінциденту, проводить аналіз обставин його виникнення, збір технічних даних з скомпрометованих або уражених систем та їх дослідження, формування індикаторів кіберзагрози, виявлення додаткових систем, на які вплинули кіберінцидент, кібератака.

Якщо під час технічного дослідження національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідною галузевою/регіональною командою реагування на

кіберінциденти, кібератаки, кіберзагрози (CSIRT) виявлено ознаки кримінального правопорушення, така інформація невідкладно (протягом години) передається до СБУ.

Суб'єкти забезпечення кібербезпеки надають національній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), відповідній галузевій або регіональній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) безпосередній доступ до систем, безпосередньо пов'язаних із заходами реагування.

Доступ національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) до систем Міноборони та Збройних Сил надається з урахуванням вимог законодавства у сфері охорони державної таємниці та організаційно-розпорядчих актів Міноборони та Збройних Сил.

24. 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.

Суб'єкти забезпечення кібербезпеки зобов'язані вжити визначених вимогою про реагування заходів та подати звіт про результати вжитих заходів.

Підстави для надання на основі отриманої від національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) інформації вимог про реагування, а також визначення строків та порядку вжиття визначених відповідною вимогою про реагування заходів реагування та подання звіту про їх виконання затверджуються Адміністрацією Держспецзв'язку.

Аналіз ефективності заходів реагування на кіберінциденти, кібератаки та кіберзагрози

25. За результатами вжиття заходів реагування на кіберінциденти, кібератаки та кіберзагрози суб'єкти забезпечення кібербезпеки у взаємодії із національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) та/або Ситуаційним центром забезпечення кібербезпеки СБУ, та/або відповідною галузевою/регіональною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) проводять аналіз ефективності реагування на кіберінциденти, кібератаки або кіберзагрози.

26. Під час етапу проведення аналізу ефективності реагування на кіберінциденти, кібератаки або кіберзагрози забезпечується документування інциденту шляхом формування звіту про реагування на кіберінцидент, кібератаку або кіберзагрозу, інформування національної

команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) та Ситуаційного центру забезпечення кібербезпеки СБУ або відповідну галузеву/регіональну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) відповідно до порядку обміну інформацією, удосконалення захисних механізмів систем і мереж, перегляд внутрішньої документації та політик безпеки для запобігання подібним інцидентам у майбутньому, а також застосування набутого досвіду для покращення управління майбутніми кіберінцидентами, кібератаками або кіберзагрозами.

Результати такого аналізу враховуються під час оновлення планів реагування на кіберінциденти, кібератаки або кіберзагрози, внутрішніх політик кібербезпеки та плану кіберзахисту, а також під час планування і проведення навчань, тренувань та інших заходів підготовки персоналу до реагування на кіберінциденти, кібератаки або кіберзагрози.

27. Публічне інформування або звітування про реагування на кіберінциденти, кібератаки та усунення їх наслідків, зокрема під час кризової ситуації у сфері кібербезпеки, здійснюється відповідно до Порядку публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх наслідків, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533 “Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози”.

Особливості реагування на кіберінциденти високого (помаранчевого), критичного (червоного) та надзвичайного (чорного) рівня критичності

28. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузева або регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (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 національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузева або регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) негайно інформує керівника з кіберзахисту або відповідальну особу, яка виконує функції та завдання керівника з кіберзахисту, суб’єкта забезпечення кібербезпеки.

29. 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.

_____

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 26 листопада 2025 р. № 1533

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

1. Ці критерії визначають умови 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 (далі — національна система обміну інформацією).

2. У цих критеріях терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про критичну інфраструктуру”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Державну службу спеціального зв’язку та захисту інформації України”.

3. Ці критерії застосовуються суб’єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози (далі — національна система реагування), власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури (далі — системи).

4. Інформація про кіберінцидент, кібератаку щодо систем та про їх наслідки є відкритою інформацією.

5. Інформація про характер, технічні та інші деталі кіберінциденту, кібератаки щодо систем належить до інформації з обмеженим доступом, якщо вона відповідає хоча б одному з таких критеріїв:

містить неоприлюднені відомості про архітектуру, конфігурацію, технічні характеристики або вразливості системи, щодо якої здійснено кіберінцидент, кібератаку;

містить відомості про скомпрометовані облікові записи, системи, вектори реалізації кіберінцидентів, кібератак або масштаби впливу, які можуть бути використані для повторних кіберінцидентів, кібератак;

безпосередньо стосується або дає змогу встановити перебіг, зміст або результати оперативно-розшукових, контррозвідувальних заходів, слідчих дій або розвідувальної діяльності;

надана з вимогою обмеження доступу міжнародними, міжурядовими чи приватними партнерами суб’єктів національної системи реагування;

дає змогу ідентифікувати фізичних чи юридичних осіб або містить персональні дані осіб, пов’язаних з кіберінцидентом, кібератакою.

6. 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 відповідно до вимог Законів України “Про інформацію”, “Про доступ до публічної інформації”.

Встановлення обмеження доступу до інформації не звільняє суб’єктів національної системи реагування та суб’єктів забезпечення кібербезпеки щодо здійснення обов’язкового інформування про кіберінциденти, кібератаки, передбаченого законодавством, зокрема в межах функціонування національної системи обміну інформацією.

Віднесення такої інформації до державної таємниці, доступ до неї та розсекречування її матеріальних носіїв здійснюються власником або розпорядником системи відповідно до вимог Закону України “Про державну таємницю”.

7. Інформація про характер, технічні та інші деталі кіберінциденту, кібератаки, віднесена до інформації з обмеженим доступом, може бути повністю або частково розкрита власником або розпорядником систем відповідно до вимог Законів України “Про інформацію”, “Про доступ до публічної інформації” у такому разі:

у межах функціонування національної системи реагування або національної системи обміну інформацією за умови, що таке розкриття є обґрунтовано необхідним для виконання визначених законодавством повноважень суб’єктів національної системи реагування, залучених до реагування на кіберінциденти та кібератаки, обміну інформацією про кіберінциденти, кібератаки чи розслідування кіберінцидентів та кібератак;

за погодженням із суб’єктом національної системи реагування, який прийняв рішення про обмеження доступу, у разі потреби забезпечення координації реагування або розслідування кіберінциденту та кібератаки;

коли розкриття є необхідним для запобігання подальшим кіберінцидентам і кібератакам або мінімізації їх наслідків.

Таке розкриття здійснюється за умови, якщо обробка інформації буде здійснюватися з визначеною метою розкриття, а також якщо це не створює загроз національній безпеці України, не порушує вимог законодавства про захист персональних даних, комерційної, банківської, державної таємниці або інших вимог захисту інформації, визначених законом.

8. Інформація про індикатори кіберзагроз, отримана під час реагування на кіберінциденти, кібератаки, кіберзагрози, є відкритою інформацією і

поширюється у порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, визначеному Адміністрацією Держспецзв’язку, а також може публічно поширюватися для виявлення загроз та запобігання ним іншими суб’єктами національної системи реагування.

_____

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 26 листопада 2025 р. № 1533

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

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

2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про критичну інфраструктуру”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Державну службу спеціального зв’язку та захисту інформації України”.

3. Дія цього Порядку поширюється на суб’єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози (далі — національна система реагування), власників або розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури (далі — системи).

4. Власники або розпорядники систем у взаємодії з відповідною галузевою або регіональною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), а у разі її відсутності з національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) здійснюють публічне інформування про реагування на кіберінциденти, кібератаки та усунення їх наслідків (далі — публічне інформування) щодо систем, власниками або розпорядниками яких вони є, забезпечуючи своєчасність і достовірність повідомлень.

Публічне інформування здійснюється щодо кіберінцидентів, кібератаки від середнього рівня критичності та вище.

Публічне інформування здійснюється шляхом публікації спільних прес-релізів, офіційних повідомлень або заяв на інформаційних ресурсах відповідної галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), а у разі її відсутності — національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) та власника або розпорядника системи, щодо якої здійснено кіберінцидент, кібератаку.

Публічне інформування здійснюється 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.

У разі коли СБУ безпосередньо забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки, публічне інформування здійснюється за погодженням з відповідним підрозділом/органом СБУ, який забезпечує таке реагування.

Якщо факт кіберінциденту або кібератаки є предметом дослідження в рамках досудового розслідування, публічне інформування здійснюється лише з письмового дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають можливим.

5. Усунення наслідків кіберінцидентів, кібератак здійснюється відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533 “Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози”.

6. Публічне звітування про реагування на кіберінциденти, кібератаки та усунення їх наслідків здійснюються у вигляді узагальнених аналітичних звітів. Такі звіти можуть містити аналітичну, технічну, статистичну інформацію про характер загроз, основні вектори атак, тенденції у сфері кібербезпеки, ефективність заходів реагування та інші аспекти, що мають значення для національної системи кібербезпеки.

Узагальнені аналітичні звіти можуть формуватися суб’єктами національної системи реагування та публікуватися у відкритому або обмеженому доступі залежно від змісту. Публікація таких звітів спрямована на інформування суб’єктів забезпечення кібербезпеки, громадськості та міжнародних партнерів, а також на підвищення прозорості та обізнаності щодо кіберзагроз.

7. Особливості публічного інформування або звітування про реагування на кіберінциденти, кібератаки та усунення їх наслідків щодо систем, що належать Міноборони, визначаються Міноборони разом з Генеральним штабом Збройних Сил. Такі особливості публічного інформування або звітування погоджуються з Адміністрацією Держспецзв’язку та СБУ.