АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАКАЗ

05.03.2026 № 179

Зареєстровано в Міністерстві юстиції України
07 квітня 2026 року
за № 473/45867

Про затвердження Порядку ведення репозитарію інформації про кіберінциденти

Відповідно до абзацу дев'ятого пункту 1 частини третьої статті 9 Закону України «Про основні засади забезпечення кібербезпеки України», абзацу четвертого пункту 112 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», абзацу четвертого підпункту 95^{41} пункту 4 та пункту 10 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411,

НАКАЗУЮ:

1. Затвердити Порядок ведення репозитарію інформації про кіберінциденти, що додається.

2. Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити в установленому порядку подання цього наказу на державну реєстрацію до Міністерства юстиції України.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова Служби **Олександр ПОТІЙ**

ПОГОДЖЕНО:

Міністр внутрішніх справ України — Ігор КЛИМЕНКО

Перший заступник Міністра оборони України — Олексій ВИСКУБ

Т.в.о. Голови Служби безпеки України генерал-майор — Євгеній ХМАРА

Голова Національної поліції України — Іван ВИГІВСЬКИЙ

Керівник Апарату Ради національної безпеки і оборони України — Анатолій БАРГИЛЕВИЧ

Голова Національного банку України — Андрій ПИШНИЙ

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
05 березня 2026 року № 179

Зареєстровано в Міністерстві юстиції України
07 квітня 2026 року
за № 473/45867

Порядок
ведення репозитарію інформації про кіберінциденти

1. Цей Порядок визначає призначення, механізм функціонування та ведення репозитарію інформації про кіберінциденти (далі - репозитарій).

2. У цьому Порядку терміни вживаються в такому значенні:

актор кіберзагрози - суб'єкт, атрибутований або визначений за інформацією з відкритих джерел як джерело кіберзагрози;

електронний кабінет - персональна вебсторінка (вебсервіс чи інший програмний інтерфейс) користувача, що пройшла електронну ідентифікацію та автентифікацію і призначена для доступу до закритої частини репозитарію;

конектори індикаторів кіберзагроз - реєстраційні номери кіберінцидентів, що формуються та використовуються у платформах обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (у тому числі на платформі MISP) та застосовуються для ідентифікації, обліку й обміну інформацією між суб'єктами забезпечення кібербезпеки;

конектори кіберінцидентів - ідентифікатори (реєстраційні номери) кіберінцидентів, присвоєні національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузевими та регіональними командами реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) у разі проведення ними заходів реагування.

Інші терміни у цьому Порядку вживаються у значенні, наведеному в Законах України «Про інформацію», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронну ідентифікацію та електронні довірчі послуги», Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533.

3. Репозитарій ведеться з метою забезпечення впорядкованого та уніфікованого зберігання, систематизації, поширення інформації про кіберінциденти, що створює єдине сховище даних для суб'єктів забезпечення кібербезпеки та підвищення ефективності виявлення, аналізу, прогнозування кіберзагроз і належного та своєчасного реагування на кіберінциденти, кібератаки, кіберзагрози.

4. Репозитарій є інформаційною системою (електронною базою даних), що функціонує з використанням програмно-технічних засобів і призначений для:

централізованого накопичення та зберігання інформації про кіберінциденти у стандартизованому вигляді відповідно до національної таксономії кіберінцидентів, включаючи категорії, типи, рівні критичності, атрибуцію та інші визначені характеристики, які не віднесені до інформації з обмеженим доступом відповідно до критеріїв віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, переліку підстав, порядку та мети розкриття такої інформації, затверджених постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533;

забезпечення доступу до інформації, що зберігається в репозитарії, відповідно до визначених рівнів доступу;

оцінки та прогнозування ризиків на основі накопичених даних з метою виявлення тенденцій, закономірностей і нових векторів реалізації кіберзагроз;

формування статистичних та аналітичних відомостей для використання суб'єктами забезпечення кібербезпеки у межах їхніх повноважень, зокрема для розроблення політик, рекомендацій, стратегічних документів, впровадження попереджувальних заходів для кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури.

Репозиторій використовує національну таксономію кіберінцидентів та здійснює інформаційну взаємодію з платформою обміну інформацією про кіберінциденти, кібератаки, кіберзагрози.

5. Власником репозитарію є держава в особі Адміністрації Держспецзв'язку.

6. Держателем та адміністратором репозитарію є Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

7. Адміністратор репозитарію:

забезпечує формування і ведення репозитарію;

здійснює контроль за дотриманням вимог законодавства щодо захисту інформації та кіберзахисту;

забезпечує необхідними ресурсами з метою створення умов для стабільного функціонування репозитарію;

забезпечує функціонування та цілодобовий доступ до репозитарію;

здійснює його технічне адміністрування, контроль і моніторинг за станом функціонування;

забезпечує захист репозитарію від несанкціонованого доступу, кіберінцидентів, кібератак, кіберзагроз;

надає консультативну допомогу усім користувачам репозитарію;

вносить інформацію про кіберінцидент до репозитарію;

забезпечує актуалізацію статистичних даних щодо кіберінцидентів з періодичністю раз на квартал;

забезпечує цілодобовий доступ до відкритої інформації на своєму офіційному вебсайті;

створює електронні кабінети, надає, припиняє доступ до них, управляє правами доступу користувачів.

8. Користувачами репозитарію є:

суб'єкти національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, які мають право вносити інформацію про кіберінциденти до репозитарію, переглядати записи з інформацією про кіберінцидент у репозитарії з урахуванням прав доступу, визначених адміністратором репозитарію;

основні суб'єкти національної системи кібербезпеки, які мають повний доступ до закритої частини репозитарію.

9. Користувачі репозитарію зобов'язані:

дотримуватися правил користування репозитарієм, визначених цим Порядком;

дотримуватися вимог законодавства у сфері кібербезпеки та захисту інформації;

використовувати інформацію з репозитарію виключно в цілях, що визначаються законодавством у сферах національної безпеки, кібербезпеки та захисту інформації.

10. До репозитарію вноситься інформація про всі значні кіберінциденти, їх категорії та рівні критичності відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533.

Інформація з обмеженим доступом, у тому числі інформація, що становить державну таємницю, службова інформація у репозитарії не обробляється та не зберігається.

11. Репозитарій має відкриту та закриту частини, які функціонують як дві окремі інформаційні системи.

12. Відкрита частина репозитарію призначена для перегляду статистичної інформації про кіберінциденти за обраний період, доступ до якої необмежений.

13. Наповнення та супровід відкритої частини репозитарію здійснюються адміністратором репозитарію.

Відкрита частина репозитарію містить статистичні дані та графічні матеріали про кіберінциденти (категорія та тип кіберінцидента згідно з національною таксономією кіберінцидентів, рівень критичності кіберінциденту, відповідний сектор або галузь, де відбувся кіберінцидент).

14. До закритої частини репозитарію вноситься така інформація про кіберінциденти:

ідентифікаційний номер кіберінциденту (унікальний для кожного кіберінциденту);

дата реєстрації кіберінциденту;

повне найменування, код згідно з ЄДРПОУ юридичної особи, в якій відбувся кіберінцидент;

категорія та тип кіберінцидента згідно з національною таксономією кіберінцидентів;

рівень критичності кіберінциденту;

відповідний сектор або галузь, де відбувся кіберінцидент;

конектори кіберінцидентів;

конектори індикаторів кіберзагроз;

відомості щодо віднесення кіберінцидентів до акторів кіберзагроз.

15. Для створення електронного кабінету користувачі подають до Адміністрації Держспецзв'язку інформацію про своїх уповноважених осіб (повна назва посади, прізвище, власне ім'я, по батькові (за наявності), електронна адреса та контактний телефон).

16. Електронна ідентифікація та автентифікація користувачів здійснюється через електронний кабінет, зокрема за допомогою інтегрованої системи електронної ідентифікації, шляхом використання користувачами кваліфікованого електронного підпису.

17. Доступ уповноваженої особи до електронного кабінету та інформації закритої частини репозитарію підлягає припиненню або обмеженню у разі:

звільнення уповноваженої особи з посади;

припинення виконання уповноваженою особою своїх посадових обов’язків на тимчасовій або постійній основі;

порушення уповноваженою особою вимог законодавства у сферах національної безпеки, кібербезпеки та захисту інформації.

Користувач зобов’язаний невідкладно, але не пізніше ніж протягом одного робочого дня, письмово або в електронній формі повідомити адміністратора репозитарію про необхідність припинення або обмеження доступу уповноваженої особи до репозитарію.

Адміністратор репозитарію протягом одного робочого дня з дати отримання відповідної інформації забезпечує припинення або обмеження доступу уповноваженої особи до репозитарію.

18. Захист та обробка інформації в репозитарії здійснюються з дотриманням вимог Законів України «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації».

Т.в.о. директора
Департаменту кіберзахисту
Адміністрації Держспецзв’язку **Дмитро ПАХОЛЬЧЕНКО**

Публікації документа

- **Офіційний вісник України** від 24.04.2026 — 2026 р., № 34, стаття 2343, код акта 138719/2026