ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 31 грудня 2025 р. № 1799

ПОРЯДОК
оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури

1. Цей Порядок визначає механізм проведення оцінювання стану кіберзахисту (далі — оцінювання) інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури (далі — об’єкти оцінювання), власниками або розпорядниками, яких є органи державної влади, інші державні органи, органи місцевого самоврядування, оператори критичної інфраструктури, а також інші юридичні особи незалежно від організаційно-правової форми (далі — власники або розпорядники об’єктів оцінювання).

Оцінювання об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури III і IV категорій критичності проводиться на добровільних засадах або у випадках, визначених пунктами 11 та 17 цього Порядку.

Дія цього Порядку не поширюється на Національний банк, банки, інші установи та осіб, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, а також на операторів платіжних систем, їх учасників та технологічних операторів платіжних послуг.

2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України “Про Державну службу спеціального зв’язку та захисту інформації України”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України”, Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 р. № 712 “Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем” (Офіційний вісник України, 2025 р., № 57, ст. 3921), Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533

“Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози” (Офіційний вісник України, 2025 р., № 99, ст. 6927).

3. Оцінювання проводять юридичні особи, фізичні особи — підприємці або фізичні особи, а також утворені відповідно до законів України військові формування, які проводять оцінювання для власних потреб (далі — суб’єкти оцінювання), включені до переліку суб’єктів оцінювання, ведення якого забезпечується Адміністрацією Держспецзв’язку у визначеному нею порядку.

Юридичні особи, фізичні особи — підприємці або фізичні особи, що проводять оцінювання, повинні відповідати вимогам до суб’єктів оцінювання, що передбачають сукупність кваліфікаційних та інших обов’язкових умов і критеріїв. Вимоги до суб’єктів оцінювання затверджуються Адміністрацією Держспецзв’язку.

4. Забороняється проведення оцінювання об’єкта оцінювання:

одним і тим самим суб’єктом оцінювання понад три роки підряд;

суб’єктом оцінювання, який брав участь у створенні об’єкта оцінювання.

У випадках, коли об’єкти оцінювання створені в межах виданого дозволу на проведення робіт з технічного захисту інформації для власних потреб, створення об’єктів оцінювання та оцінювання таких об’єктів має проводитися різними посадовими особами власника або розпорядника об’єкта оцінювання.

5. Під час оцінювання контроль за дотриманням вимог законодавства у сфері охорони державної таємниці покладається на керівників та режимно-секретні органи власників або розпорядників об’єктів оцінювання.

6. Суб’єкти оцінювання мають право:

отримувати доступ до об’єкта оцінювання;

ознайомлюватися з усіма документами та матеріалами, необхідними для проведення оцінювання;

подавати письмові запити та отримувати інформацію, документи в паперовій та електронній формі, зокрема з обмеженим доступом з дотриманням встановлених правил роботи з документами, які містять інформацію з обмеженим доступом, копії необхідних документів, письмові та усні пояснення посадових осіб з питань, що безпосередньо пов’язані із проведенням оцінювання;

на будь-якому етапі відмовитися від проведення оцінювання у разі виникнення обставин, які перешкоджають проведенню об’єктивного оцінювання.

7. Суб’єктом оцінювання складається звіт про результати оцінювання (далі — звіт) за формою та відповідно до методичних рекомендацій, визначених Адміністрацією Держспецзв’язку.

Примірники звітів зберігаються у суб’єктів оцінювання, а також у власників або розпорядників об’єктів оцінювання протягом трьох років.

Копії звітів надсилаються Адміністрації Держспецзв’язку протягом 30 календарних днів з дати завершення оцінювання.

Звіт використовується для цілей здійснення моніторингу стану кіберзахисту як однієї з форм заходів державного контролю за дотриманням вимог законодавства у сфері кіберзахисту.

Відповідальність за достовірність, актуальність та повноту зазначеної у звіті інформації несе суб’єкт оцінювання.

8. Оцінювання проводиться з урахуванням методичних рекомендацій відповідно до виду оцінювання, що передбачають сукупність методів та заходів щодо організації та проведення оцінювання. Методичні рекомендації затверджуються Адміністрацією Держспецзв’язку.

9. Видами оцінювання є:

1) оцінювання дотримання вимог цільових профілів безпеки системи;

2) оцінювання поточного стану кіберзахисту;

3) оцінювання на відповідність національним стандартам у сферах кіберзахисту та захисту інформації;

4) оцінка стану захищеності державних інформаційних ресурсів.

10. Результати оцінювання дотримання вимог цільових профілів безпеки або зовнішнього оцінювання як частини оцінювання поточного стану кіберзахисту враховуються під час проведення іншого виду оцінювання у разі дотримання таких умов:

між першим та наступним оцінюванням пройшло не більше року;

є документальне підтвердження, що за період між першим та наступним оцінюванням власником або розпорядником об’єкта оцінювання здійснювалися необхідні періодичні заходи з кіберзахисту;

до підтвердних документів, які використовувалися під час проведення першого оцінювання, не вносилися зміни;

до нормативно-правових актів, вимоги яких враховуються під час проведення оцінювання, не вносилися зміни.

11. Оцінювання дотримання вимог цільових профілів безпеки системи проводиться з метою авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем.

12. Власники або розпорядники об’єктів оцінювання здійснюють оцінювання дотримання вимог цільових профілів безпеки системи з метою авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 р. № 712 (Офіційний вісник України, 2025 р., № 57, ст. 3921), та з урахуванням рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи, затверджених Адміністрацією Держспецзв’язку.

13. Оцінювання поточного стану кіберзахисту (самооцінювання та зовнішнє оцінювання) проводиться з метою підготовки та перегляду планів кіберзахисту, які включають описи поточного та/або цільового станів кіберзахисту, або отримання об’єктивної інформації про фактичний стан виконання вимог законодавства у сфері кіберзахисту, повноти запроваджених заходів кіберзахисту.

14. Власники або розпорядники об’єктів оцінювання здійснюють такі види самооцінювання поточного стану кіберзахисту:

планове самооцінювання поточного стану кіберзахисту — щороку;

позапланове самооцінювання поточного стану кіберзахисту — за рішенням власника або розпорядника об’єкта оцінювання.

15. Самооцінювання поточного стану кіберзахисту мають право здійснювати посадові особи власників або розпорядників об’єктів оцінювання, які відповідають вимогам до суб’єктів оцінювання для такого виду оцінювання та включені до переліку суб’єктів оцінювання.

Власники або розпорядники об’єктів оцінювання з метою проведення самооцінювання поточного стану кіберзахисту мають право залучати інших суб’єктів оцінювання.

16. Оператори критичної інфраструктури, власники або розпорядники об’єктів критичної інформаційної інфраструктури здійснюють планове зовнішнє оцінювання поточного стану кіберзахисту не рідше ніж один раз на два роки.

17. Позапланове зовнішнє оцінювання поточного стану кіберзахисту здійснюється на таких підставах:

1) виявлення щодо об’єкта оцінювання кіберінциденту, який за рівнем критичності кваліфіковано як критичний або надзвичайний, та під час заходів реагування національною, галузевими або регіональними командами реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози виявлено недоліки у здійсненні

заходів захисту або ознаки порушення вимог законодавства у сферах кіберзахисту та захисту інформації.

У такому випадку власники або розпорядники об’єктів оцінювання проводять позапланове оцінювання поточного стану кіберзахисту протягом трьох місяців з дати завершення надання сервісу з реагування, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози національною, галузевими або регіональними командами реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT);

2) за рішенням власника або розпорядника об’єкта оцінювання;

3) за рішенням суду.

18. Власники або розпорядники об’єктів оцінювання для проведення зовнішнього оцінювання поточного стану кіберзахисту залучають суб’єктів оцінювання, які відповідають вимогам до суб’єктів оцінювання для такого виду оцінювання, включені до переліку суб’єктів оцінювання та не є посадовими особами власників або розпорядників об’єктів оцінювання.

19. Оцінювання на відповідність національним стандартам у сферах кіберзахисту та захисту інформації проводиться за рішенням власника або розпорядника об’єкта оцінювання для підтвердження відповідності об’єкта оцінювання вимогам стандарту у сферах кіберзахисту та захисту інформації.

20. Оцінка стану захищеності державних інформаційних ресурсів здійснюється з метою виявлення існуючих загроз державним інформаційним ресурсам та запобігання несанкціонованим діям щодо інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах в порядку, визначеному Адміністрацією Держспецзв’язку.

21. Планова оцінка стану захищеності державних інформаційних ресурсів проводиться не частіше одного разу на три роки Державним центром кіберзахисту Держспецзв’язку на підставі внесення об’єкта оцінювання до плану проведення оцінки стану захищеності державних інформаційних ресурсів.

22. Позапланова оцінка стану захищеності державних інформаційних ресурсів здійснюється за рішенням власника або розпорядника об’єкта оцінювання одним із таких суб’єктів:

Державним центром кіберзахисту Держспецзв’язку;

посадовими особами власника або розпорядника об’єкта оцінювання, які відповідають вимогам до суб’єктів оцінювання для такого виду оцінювання;

суб’єктами оцінювання.

_____