



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 28 березня 2025 р. № 447

Київ

**Про внесення змін щодо кіберзахисту
державних інформаційних ресурсів та
критичної інформаційної інфраструктури
до деяких постанов Кабінету Міністрів України**

Кабінет Міністрів України **постановляє:**

Внести до постанов Кабінету Міністрів України зміни щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, що додаються.



Прем'єр-міністр України

Д. ШМИГАЛЬ

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 28 березня 2025 р. № 447

ЗМІНИ

щодо кіберзахисту державних інформаційних
ресурсів та критичної інформаційної інфраструктури,
що вносяться до постанов Кабінету Міністрів України

1. У Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 (Офіційний вісник України, 2006 р., № 13, ст. 878; 2011 р., № 69, ст. 2624; 2022 р., № 47, ст. 2595):

1) абзац четвертий пункту 3 викласти в такій редакції:

“Інші терміни вживаються у значенні, наведеному в Законах України “Про інформацію”, “Про доступ до публічної інформації”, “Про державну таємницю”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про електронні комунікації”, “Про основні засади забезпечення кібербезпеки України”, Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27 вересня 1999 р. № 1229, Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426 (Офіційний вісник України, 2022 р., № 4, ст. 219).”;

2) доповнити Правила пунктами 26 і 27 такого змісту:

“26. Власники (розпорядники) систем, у яких обробляються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом:

здійснюють управління ризиками у сфері кібербезпеки, що передбачає ідентифікацію та періодичну оцінку ризиків, їх моніторинг і перегляд, а також процедури, які забезпечують впровадження, перегляд і вдосконалення політики управління ризиками;

здійснюють базові заходи з кіберзахисту;

затверджують, переглядають та оновлюють плани кіберзахисту, політики кібербезпеки, плани реагування на кібератаки та кіберінциденти;

здійснюють виявлення кіберінцидентів та кібератак і реагування на них, усунення їх наслідків;

невідкладно інформують урядову команду реагування на комп’ютерні надзвичайні події України CERT-UA та Ситуаційний центр забезпечення кібербезпеки СБУ про інциденти кібербезпеки від середнього рівня критичності та вище;

здійснюють інформаційний обмін щодо виявлених та потенційних кіберзагроз між силами кіберзахисту та відповідними підрозділами інших суб'єктів забезпечення кібербезпеки;

отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на системи закордонних дипломатичних установ України;

проводять навчання та тренінги для співробітників з питань кібербезпеки, зокрема щодо підвищення рівня обізнаності про кіберзагрози, методів запобігання їх виникненню, управління ризиками у сфері кібербезпеки та дотримання принципів кібергігієни.

Методика ідентифікації та оцінки ризиків у сфері кібербезпеки затверджується Адміністрацією Держспецзв'язку.

27. Моніторинг стану кіберзахисту систем, у яких обробляються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, забезпечується їх власниками (розпорядниками) шляхом:

оцінки стану кіберзахисту не рідше ніж один раз на рік відповідно до методичних рекомендацій щодо здійснення базових заходів з кіберзахисту;

використання систем виявлення, запобігання та нейтралізації кіберзагроз, за допомогою яких здійснюються збір та аналіз мережевої телеметрії, а також реагування на кіберінциденти та кібератаки;

аудиту інформаційної безпеки, у тому числі шляхом залучення незалежних аудиторів інформаційної безпеки.

Результати такого моніторингу використовуються:

власниками (розпорядниками) систем, у яких обробляються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, під час аналізу ефективності та коригування здійснених заходів з кіберзахисту, а також для планування заходів з управління ризиками у сфері кібербезпеки;

Адміністрацією Держспецзв'язку під час:

- проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

- здійснення державного контролю у сферах захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації;

- проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.”.

2. У додатку до постанови Кабінету Міністрів України від 16 грудня 2015 р. № 1057 “Про визначення сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання” (Офіційний вісник України, 2015 р., № 102, ст. 3519; 2020 р., № 11, ст. 434; 2023 р., № 65, ст. 3712) позицію “Адміністрація Держспецзв’язку” у графі “Сфера діяльності, в якій здійснюються функції технічного регулювання (об’єкти технічних регламентів)” після слів “технічного захисту інформації)” доповнити словами “, кіберзахист об’єктів критичної інфраструктури, протидії технічним розвідкам, захист державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності”.

3. У постанові Кабінету Міністрів України від 9 жовтня 2020 р. № 943 “Деякі питання об’єктів критичної інформаційної інфраструктури” (Офіційний вісник України, 2020 р., № 84, ст. 2709; 2022 р., № 72, ст. 4364):

1) у Порядку формування переліку об’єктів критичної інформаційної інфраструктури, затвердженому зазначеною постановою:

пункт 1 доповнити абзацом такого змісту:

“Дія цього Порядку не поширюється на банки, інші юридичні особи, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг.”;

пункт 2 викласти в такій редакції:

“2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України “Про електронні комунікації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України” та “Про критичну інфраструктуру”.”;

у пункті 12 слова “паспорта об’єкта” замінити словами “паспорта безпеки на об’єкт”;

у пункті 13 слова “уповноважених органів за сектори (підсектори) критичної інфраструктури держави” замінити словами “секторальних органів у сфері захисту критичної інфраструктури”;

пункт 15 викласти в такій редакції:

“15. Оператор критичної інфраструктури здійснює базові заходи з кіберзахисту щодо власних об’єктів критичної інформаційної інфраструктури.”;

у тексті Порядку:

слова “Оператор основних послуг”, “оператор основних послуг” в усіх відмінках і формах числа замінити словами “Оператор критичної

інфраструктури”, “оператор критичної інфраструктури” у відповідному відмінку і числі;

слова “Уповноважений орган”, “уповноважений орган” в усіх відмінках і формах числа замінити словами “Секторальний орган у сфері захисту критичної інфраструктури”, “секторальний орган у сфері захисту критичної інфраструктури” у відповідному відмінку і числі;

слова “основних послуг” замінити словами “життєво важливих послуг та функцій”;

у додатку до Порядку слова “основних послуг” замінити словами “життєво важливих послуг та функцій”, а слова “уповноваженого органу сектору (підсектору) критичної інфраструктури” — словами “секторального органу у сфері захисту критичної інфраструктури”;

2) у Порядку внесення об’єктів критичної інформаційної інфраструктури до державного реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування, затвердженому зазначеною постановою:

пункт 2 викласти в такій редакції:

“2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України “Про електронні комунікації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України” та “Про критичну інфраструктуру”.”;

у пункті 6:

в абзацах третьому і четвертому слова “основних послуг” замінити словами “життєво важливих послуг та функцій”;

в абзаці п’ятому слова “уповноважений орган сектору (підсектору) критичної інфраструктури, до” замінити словами “секторальний орган у сфері захисту критичної інфраструктури, до сектору (підсектору) критичної інфраструктури”;

в абзаці першому пункту 7 слова “основних послуг” замінити словами “критичної інфраструктури”, а слова “підписані кваліфікованим електронним підписом керівника об’єкта критичної інфраструктури або уповноваженої на те особи,” виключити;

у пункті 10 слова “уповноваженому органу” замінити словами “секторальному органу у сфері захисту критичної інфраструктури”;

доповнити Порядок пунктом 11 такого змісту:

“11. Відомості реєстру надсилаються СБУ в електронній формі один раз на рік (до 1 березня поточного року), а також за окремим запитом (у разі виникнення додаткової потреби) з метою виконання завдань, покладених на СБУ відповідно до закону.”.
