КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 13 листопада 2025 р. № 1470

Київ

Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518

Кабінет Міністрів України **постановляє:**

Внести до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури” (Офіційний вісник України, 2019 р., № 50, ст. 1697; 2022 р., № 72, ст. 4364) зміни, що додаються.

Прем’єр-міністр України **Ю. СВИРИДЕНКО**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 13 листопада 2025 р. № 1470

ЗМІНИ,
що вносяться до постанови Кабінету Міністрів України
від 19 червня 2019 р. № 518

1. У постанові:

1) у назві постанови слова “до кіберзахисту” замінити словами “з кіберзахисту”;

2) у постановляючій частині постанови слова і цифру “частини другої статті 6” замінити словами і цифрою “частини третьої статті 5”.

2. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені зазначеною постановою, викласти в такій редакції:

“ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 19 червня 2019 р. № 518
(в редакції постанови Кабінету Міністрів України
від 13 листопада 2025 р. № 1470)

ЗАГАЛЬНІ ВИМОГИ
з кіберзахисту об’єктів критичної інфраструктури

1. Ці Загальні вимоги визначають організаційно-методологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання операторами критичної інфраструктури та власниками або розпорядниками об’єктів критичної інформаційної інфраструктури (далі — суб’єкти).

Дія цих Загальних вимог 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 цих Загальних вимогах терміни вживаються у такому значенні:

базові заходи з кіберзахисту — мінімально необхідна взаємопов’язана сукупність організаційних та технічних заходів з кіберзахисту, визначена Адміністрацією Держспецзв’язку;

каталог заходів з кіберзахисту — необхідна взаємопов’язана сукупність організаційних та технічних заходів з кіберзахисту, визначена Адміністрацією Держспецзв’язку;

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 інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі — системи);

поточний стан кіберзахисту — фактичний стан організації та здійснення заходів з кіберзахисту;

цільовий стан кіберзахисту — плановий стан організації та здійснення заходів з кіберзахисту, визначених на основі каталогу заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

Інші терміни вживаються у значенні, наведеному в Законах України “Про інформацію”, “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”, постанові Кабінету Міністрів України від 21 лютого 2025 р. № 205 “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації” (Офіційний вісник України, 2025 р., № 25, ст. 1666).

3. Кіберзахист об’єктів критичної інфраструктури забезпечується шляхом здійснення суб’єктами заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

Усі базові заходи з кіберзахисту є обов’язковими для здійснення суб’єктами.

4. З метою належного здійснення заходів з кіберзахисту суб’єкти затверджують, щороку переглядають та за потреби (зокрема у разі зміни рівня ризику кібербезпеки) оновлюють план кіберзахисту.

План кіберзахисту розробляється з урахуванням результатів управління ризиками кібербезпеки на основі каталогу заходів з кіберзахисту та включає описи поточного та/або цільового стану кіберзахисту.

Заходи, передбачені планом кіберзахисту, повинні взаємоузгоджуватися з планом захисту об’єкта критичної інфраструктури за проектною загрозою національного рівня “кібератака/кіберінцидент”, який погоджується з функціональними органами у сфері захисту критичної інфраструктури відповідно до Порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 4 серпня 2023 р. № 818 (Офіційний вісник України, 2023 р., № 77, ст. 4366).

Суб’єкти поетапно та послідовно досягають цільового стану кіберзахисту шляхом здійснення визначених планом кіберзахисту заходів з кіберзахисту.

Методичні рекомендації щодо здійснення заходів з кіберзахисту затверджуються Адміністрацією Держспецзв’язку.

5. Суб’єкти забезпечують оцінювання стану кіберзахисту об’єкта критичної інфраструктури та/або об’єктів критичної інформаційної інфраструктури відповідно до порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних 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 (крім систем та об’єктів банків), передбаченого частиною третьою статті 5 Закону України “Про основні засади забезпечення кібербезпеки України”, з урахуванням каталогу заходів з кіберзахисту, особливостей функціонування та архітектури об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури.

6. Суб’єкти здійснюють управління ризиками кібербезпеки на постійній та системній основі для запобігання виникненню кіберінциденту та/або реалізації кіберзагрози і мінімізації можливих наслідків у разі настання кіберінциденту та/або реалізації кіберзагрози.

Управління ризиками кібербезпеки здійснюється із застосуванням національних та міжнародних стандартів управління у сфері кібербезпеки та включає:

організацію управління ризиками кібербезпеки;

оцінювання ризиків кібербезпеки;

запобігання ризикам (мінімізація ризиків) кібербезпеки;

проведення моніторингу і здійснення контролю за ризиками кібербезпеки та перегляд їх актуальності;

здійснення обміну інформацією про ризики кібербезпеки.

Методика оцінювання ризиків кібербезпеки затверджується Адміністрацією Держспецзв’язку.

7. Суб’єкти забезпечують реагування на кіберінциденти, кібератаки та кіберзагрози з урахуванням національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, передбаченого частиною третьою статті 5 Закону України “Про основні засади забезпечення кібербезпеки України”.

8. Керівники з кіберзахисту або відповідальні особи, які виконують функції та завдання керівників з кіберзахисту, або підрозділи з кіберзахисту

суб’єктів здійснюють заходи з кіберзахисту, управління ризиками кібербезпеки, реагування на кіберінциденти, кібератаки та кіберзагрози, обмін інформацією про кіберінциденти, кібератаки та кіберзагрози.

9. Суб’єкти організовують та забезпечують регулярне навчання своїх співробітників з питань кіберзахисту, яке проводиться диференційовано залежно від функціональних обов’язків та з урахуванням професійної кваліфікації співробітників.

10. Суб’єкти забезпечують планування витрат та фінансування заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

11. Секторальні органи у сфері захисту критичної інфраструктури на основі цих Загальних вимог та каталогу заходів з кіберзахисту можуть розробляти галузеві вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури, які відносяться до сфери їх управління. Такі галузеві вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв’язку.”.

3. Додаток до Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених зазначеною постановою, виключити.

_____