ДОКУМЕНТИ

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

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.

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА
від 13 листопада 2025 р. № 1471
Київ

Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності

Відповідно до частини третьої статей 5 і 9 Закону України «Про основні засади забезпечення кібербезпеки України» Кабінет Міністрів України **ПОСТАНОВЛЯЄ**:

Затвердити Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності, що додається.

Прем'єр-міністр України Ю. СВИРИДЕНКО

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 13 листопада 2025 р. № 1471

ПОРЯДОК
взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності

1. Цей Порядок визначає механізм взаємодії:

національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності;

галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності, іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;

Національної поліції, СБУ з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

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», «Про оперативно-розшукову діяльність», «Про розвідку» та Кримінальному процесуальному кодексі України.

3. Взаємодія суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки здійснюється 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) відповідно до процедур, визначених національним планом реагування на кіберінциденти, кібератаки, кіберзагрози, затвердженим Кабінетом Міністрів України, та порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, визначеного Адміністрацією Держспецзв'язку (далі — порядок обміну інформацією).

4. Взаємодія галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) із національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) та приватних команд реагування на кіберінциденти, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування здійснюється в порядку, встановленому Адміністрацією Держспецзв'язку.

5. Взаємодія суб'єктів національної системи реагування з правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності здійснюється шляхом:

обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

проведення спільних заходів під час реагування на кіберінциденти, кібератаки, кіберзагрози;

надання та отримання в установленому законодавством порядку доступу до технічних та інших деталей кіберінциденту чи кібератаки (відомостей про кіберінцидент чи кібератаку) для проведення слідчих (розшукових) дій, контррозвідувальних або оперативно-розшукових заходів;

функціонування міжвідомчих груп із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки.

6. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) в рамках функціонування національної системи реагування та національної системи обміну інформацією невідкладно інформують:

Національний координаційний центр кібербезпеки — про всі значні кіберінциденти та кібератаки;

СБУ — про значні кіберінциденти, кібератаки, кіберзагрози, виявлені або потенційні вразливості інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об'єктів критичної інформаційної інфраструктури;

Національну поліцію — про значні кіберінциденти та кібератаки щодо об'єктів критичної інформаційної інфраструктури;

розвідувальний орган згідно з його компетенцією — про зовнішні кіберзагрози, спрямовані проти національної безпеки, в яких виявлено ознаки дій або потенційних можливостей іноземних держав, організацій та осіб;

Державне бюро розслідувань — про кіберінциденти та кібератаки, якщо в ході реагування на них отримано ознаки кримінальних правопорушень, віднесених до підслідності Державного бюро розслідувань;

Національне антикорупційне бюро — про кіберінциденти та кібератаки, якщо в ході реагування на них виявлено ознаки кримінальних правопорушень, віднесених до підслідності Національного антикорупційного бюро;

БЕБ — про кіберінциденти, кібератаки, кіберзагрози, якщо в ході реагування на них виявлено ознаки кримінальних правопорушень, віднесених до підслідності БЕБ.

Критерії віднесення кіберінциденту до значного визначає Адміністрація Держспецзв'язку.

7. СБУ в межах повноважень, визначених законодавством, інформує інших суб'єктів національної системи реагування про актуальні кіберзагрози у сфері державної безпеки та взаємодіє з ними під час реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням особливостей, встановлених законодавством у зазначеній сфері.

Національна поліція в межах повноважень, визначених законодавством, інформує інших суб'єктів національної системи реагування про організацію, сили, засоби, методи, тактику дій злочинних угрупувань, що стали відомими в ході оперативно-розшукової діяльності та під час обміну інформацією з правоохоронними органами іноземних держав та міжнародними правоохоронними органами, правоохоронними і спеціальними службами інших держав та/або міжнародними правоохоронними організаціями.

Розвідувальні органи в межах повноважень, визначених законодавством, інформують суб'єктів національної системи реагування про зовнішні загрози національній безпеці у кіберпросторі, технічні розвідки іноземних держав, які діють у кіберпросторі, інші події і обставини, що стосуються сфери кібербезпеки.

8. Обмін інформацією про кіберінциденти, кібератаки, кіберзагрози здійснюється за умови дотримання вимог законодавства у сферах захисту інформації та кіберзахисту з урахуванням загальних правил обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (протокол TLP), визначених Адміністрацією Держспецзв'язку.

9. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) проводять з правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності спільні заходи під час реагування на кіберінциденти та кібератаки у разі необхідності здійснення ними своїх повноважень, визначених законом, зокрема спільне технічне дослідження кіберінциденту та кібератаки, аналіз обставин їх виникнення, збір технічних даних із скомпрометованих або уражених інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем та їх дослідження, а також збирання, фіксацію та збереження відомостей в електронній формі.

Організацію спільних заходів під час реагування на кіберінциденти та кібератаки забезпечує національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідна галузева та регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT).

Такі спільні заходи проводяться з урахуванням вимог кримінального процесуального законодавства та законодавства про контррозвідувальну діяльність та необхідності забезпечення для національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідної галузевої та регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) безперервності реагування на кіберінциденти та кібератаки.

10. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) в установленому законодавством порядку надають правоохоронним органам та суб'єктам оперативно-розшукової діяльності доступ до технічних та інших деталей кіберінциденту чи кібератаки (відомостей про кіберінцидент чи кібератаку) з метою здійснення ними своїх повноважень, визначених законом.

11. Суб'єкти національної системи реагування та правоохоронні, контррозвідувальні, розвідувальні органи та суб'єкти оперативно-розшукової діяльності в межах повноважень, визначених законодавством, здійснюють взаємодію в межах функціонування міжвідомчих груп із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки, зокрема в межах постійно діючої Об'єднаної групи реагування на кіберінциденти, кібератаки, кіберзагрози.

Взаємодія в межах функціонування міжвідомчих груп передбачає:

обмін інформацією, технічними даними та результатами досліджень щодо кіберінцидентів, кібератак, кіберзагроз;

узгодження та координацію дій з локалізації та нейтралізації кіберінцидентів та кібератак, усунення їх наслідків;

визначення необхідності залучення додаткових ресурсів (фінансових, матеріально-технічних, людських тощо) суб'єктів національної системи реагування або міжнародних партнерів;

проведення аналізу отриманої інформації, розроблення рекомендацій і пропозицій щодо подальших заходів реагування.

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА
від 13 листопада 2025 р. № 1472
Київ

Про затвердження Порядку проведення моніторингу та ведення переліку органів державної влади та органів місцевого самоврядування, в яких запроваджено системи енергетичного менеджменту

Відповідно до абзацу першого частини восьмої статті 12 Закону України «Про енергетичну ефективність» Кабінет Міністрів України **ПОСТАНОВЛЯЄ:**

Затвердити Порядок проведення моніторингу та ведення переліку органів державної влади та органів місцевого самоврядування, в яких запроваджено системи енергетичного менеджменту, що додається.

Прем'єр-міністр України Ю. СВИРИДЕНКО

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 13 листопада 2025 р. № 1472

ПОРЯДОК
проведення моніторингу та ведення переліку органів державної влади та органів місцевого самоврядування, в яких запроваджено системи енергетичного менеджменту

1. Цей Порядок визначає механізм проведення моніторингу та ведення переліку органів державної влади та органів місцевого самоврядування, в яких запроваджено системи енергетичного менеджменту (далі — перелік).

2. Проведення моніторингу та ведення переліку здійснюється Держенергоефективності з метою збору, узагальнення та аналізу інформації про стан запровадження та забезпечення функціонування систем енергетичного менеджменту органами державної влади, зокрема підприємствами, установами, організаціями, що належать до сфери їх управління, та органами місцевого самоврядування (далі — суб'єкти запровадження системи енергетичного менеджменту).

3. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України «Про енергетичну ефективність», «Про енергетичну ефективність будівель», інших нормативних документах та нормативно-правових актах у сфері забезпечення енергетичної ефективності.

4. Проведення моніторингу та ведення переліку передбачає здійснення заходів, спрямованих на отримання, узагальнення, оброблення, збереження та проведення аналізу інформації про фактичний стан запровадження та функціонування системи енергетичного менеджменту, дотримання вимог законодавства у сфері забезпечення енергетичної ефективності, а також на визначення перспектив подальшого розвитку системи енергетичного менеджменту в Україні.

5. Під час проведення моніторингу та ведення переліку збирається інформація про:

суб'єкта запровадження системи енергетичного менеджменту (найменування юридичної особи, у тому числі скорочене (за наявності); код згідно з ЄДРПОУ);

контактну особу (прізвище, власне ім'я, по батькові (за наявності), посада, контактний номер телефону);

рішення про запровадження системи енергетичного менеджменту;

спосіб запровадження та функціонування системи енергетичного менеджменту (покладення обов'язків на структурний підрозділ, посадову особу, підрядну організацію);

план діяльності системи енергетичного менеджменту (дата затвердження, дата останнього перегляду);

сертифікацію системи енергетичного менеджменту;

декларацію енергетичної політики;

цілі запровадження системи енергетичного менеджменту (у натуральному (тонн нафтового еквіваленту) та відносному (відсотків) показниках);

інші відомості, визначені Держенергоефективності.

6. Суб'єкти запровадження системи енергетичного менеджменту подають Держенергоефективності інформацію за формою та у строки, визначені Держенергоефективності, або розміщують її в національній системі моніторингу енергоефективності (за наявності).

7. Держенергоефективності протягом десяти робочих днів з дня отримання інформації від суб'єктів запровадження системи енергетичного менеджменту проводить її перевірку щодо достовірності, повноти та наявності технічних помилок.

У разі виявлення Держенергоефективності в інформації, отриманої від суб'єкта запровадження системи енергетичного менеджменту, технічної помилки (описки, друкарської, граматичної, орфографічної помилки) або подання інформації не за визначеною формою Держенергоефективності інформує в установленому порядку про це суб'єкта запровадження системи енергетичного менеджменту з метою уточнення інформації.

Суб'єкт запровадження системи енергетичного менеджменту протягом двох робочих днів перевіряє правильність поданої інформації та повідомляє про результат Держенергоефективності.

8. Перелік формується на основі отриманої Держенергоефективності інформації та складається з відомостей про суб'єкта запровадження системи енергетичного менеджменту (найменування юридичної особи, у тому числі скорочене (за наявності); код згідно з ЄДРПОУ), рішення про запровадження системи енергетичного менеджменту, сертифікацію системи енергетичного менеджменту.

9. Перелік, інформація про стан і результати запровадження системи енергетичного менеджменту публікуються щопівроку до 20 лютого та 20 серпня на офіційному веб-сайті Держенергоефективності.

10. Узагальнений звіт щодо проведення моніторингу та ведення переліку разом з пропозиціями щодо визначення перспектив подальшого розвитку системи енергетичного менеджменту в Україні надсилаються Держенергоефективності щопівроку до 20 лютого та 20 серпня Мінрозвитку.