Роз'яснення до постанов Кабінету Міністрів України від 19.06.2019 № 518 та від 29.03.2006 № 373 в частині забезпечення кіберзахисту, а також наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту»

Постанови Кабінету Міністрів України від 13.11.2025 № 1470 та від 26.11.2025 № 1531 виклали у новій редакції Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури та Мінімальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, затверджені постановами Кабінету Міністрів України від 19.06.2019 № 518 та від 29.03.2006 № 373 відповідно.

Відповідно до зазначених нормативних документів органи державної влади, інші державні органи, органи місцевого самоврядування, державні підприємства, установи та організації, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі - система), в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, оператори критичної інфраструктури та власники або розпорядники об’єктів критичної інформаційної інфраструктури (далі - суб’єкти) забезпечують кіберзахист своєї інформаційної інфраструктури шляхом здійснення заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки. Це вимагатиме від суб’єктів більш глибокого аналізу власних ризиків та побудови адаптивної системи безпеки.

Зазначені вище Вимоги запроваджують чіткий алгоритм дій для суб’єктів, який складається з трьох послідовних етапів:

оцінка поточного стану: кожен суб’єкт повинен провести оцінювання власної системи кіберзахисту та зафіксувати її поточний стан кіберзахисту;

визначення цілей: на основі управління ризиками кібербезпеки та використовуючи єдиний каталог заходів з кіберзахисту, суб’єкт має визначити цільовий (бажаний) стан кіберзахисту;

упровадження заходів: для досягнення цільового стану кіберзахисту суб’єкт розробляє та реалізує поетапний план вжиття необхідних заходів кіберзахисту та фіксує їх в плані кіберзахисту.

На виконання зазначених вище постанов Адміністрацією Держспецзв’язку затверджено наказ від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту» (далі – Наказ № 75). Документ розроблено з урахуванням NIST Cybersecurity Framework (CSF) 2.0 та впроваджено сучасний диференційований підхід до кіберзахисту на основі управління ризиками кібербезпеки.

Для здійснення заходів з кіберзахисту суб’єкти визначають **сферу їх застосування.** Визначаючи сферу застосування заходів з кіберзахисту, суб’єкти мають враховувати:

організаційно-штатну структуру: підрозділи, основні операційні процеси, зони відповідальності тощо;

технічні компоненти: системи, електронно-комунікаційні мережі, операційні системи, бази даних, програмне забезпечення тощо;

фізичні межі: географічне розташування систем, приміщення, серверні кімнати тощо.

Каталог заходів з кіберзахисту, який затверджений Наказом № 75, поширюється на суб'єктів та визначає необхідну взаємопов’язану сукупність усіх організаційних та технічних заходів з кіберзахисту.

Основним призначенням Каталогу є застосування при оцінюванні поточного стану кіберзахисту, визначенні цільового стану кіберзахисту та розробці плану кіберзахисту відповідно до оновлених Загальних вимог з кіберзахисту об'єктів критичної інфраструктури та Мінімальних вимог до захисту інформаційних систем.

Важливою функцією Каталогу є можливість його використання секторальними органами у сфері захисту критичної інфраструктури для розроблення галузевих вимог з кіберзахисту, які адаптуються до специфіки відповідного сектора.

Структурно Каталог організовано за функціями кіберзахисту: управління (GV), ідентифікація (ID), захист (PR), виявлення (DE), реагування (RS) та відновлення (RC). Кожна функція включає категорії та конкретні заходи з кіберзахисту, що забезпечує комплексний підхід до організації кіберзахисту.

Суб'єкти зобов'язані використовувати Каталог для оцінювання поточного стану кіберзахисту та визначення заходів, які необхідно впровадити для досягнення цільового стану з урахуванням результатів управління ризиками кібербезпеки. На основі цього розробляється план кіберзахисту, який затверджується керівництвом суб'єкта та підлягає щорічному перегляду.

Наказом № 75 затверджуються **Базові заходи з кіберзахисту**, які визначають мінімальний обов'язковий набір заходів, що підлягають впровадженню суб'єктами. Виконання базових заходів з кіберзахисту є обов'язковим для всіх без винятку суб’єктів. Базові заходи є підмножиною Каталогу та забезпечують базовий рівень кіберзахисту, необхідний для всіх суб'єктів незалежно від результатів оцінювання ризиків.

Базові заходи з кіберзахисту, сформовані за диференційованим підходом, поділяються для:

операторів критичної інфраструктури та власників або розпорядників об’єктів критичної інформаційної інфраструктури I та II категорій критичності;

операторів критичної інфраструктури та власників або розпорядників об’єктів критичної інформаційної інфраструктури III та IV категорій критичності;

органів державної влади, інших державних органів, органів місцевого самоврядування, державних підприємств, установ та організацій, які є власниками або розпорядниками систем, в яких обробляються державні інформаційні ресурси;

органів державної влади, інших державних органів, органів місцевого самоврядування, державних підприємств, установ та організацій, які є власниками або розпорядниками систем, в яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Наказ № 75 також затверджує **Форму плану кіберзахисту**. Суб’єкт з метою належного здійснення заходів з кіберзахисту розробляє, затверджує, щорічно переглядає та за потреби (зокрема у разі зміни рівня ризику кібербезпеки) оновлює план кіберзахисту.

План кіберзахисту розробляється з урахуванням результатів управління ризиками кібербезпеки на основі Каталогу заходів з кіберзахисту з урахуванням обов’язкових до виконання Базових заходів з кіберзахисту та описує поточний та/або цільовий стани кіберзахисту.

План кіберзахисту – додатковий інструмент, який допоможе суб’єкту оцінити достатність ресурсів, визначити пріоритетні заходи з кіберзахисту, забезпечити поінформованість про результати з метою обізнаності всіх співробітників суб’єкта, враховуючи при цьому місії функціонування систем, очікування заінтересованих сторін, актуальні виклики та загрози, а також законодавчі вимоги у сферах кіберзахисту та захисту інформації.

Крім того, наказом № 75 затверджуються **Методичні рекомендації щодо здійснення заходів з кіберзахисту,** які надають практичні настанови суб'єктам щодо впровадження заходів з кіберзахисту.

З набранням чинності наказу № 75 визнаються такими, що втратили чинність накази Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами) та від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту».

Т.в.о. директора Департаменту кіберзахисту
Адміністрації Держспецзв’язку Дмитро ПАХОЛЬЧЕНКО
___.___.2026