ПРОЄКТ

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від ___ _____ 2025 р. № _____

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

1. У назві та тексті постанови слова “до кіберзахисту” замінити словами “з кіберзахисту”, а слова та цифру “частини другої статті 6” замінити словами та 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 ___ _____ 2025 р. № _____)

ЗАГАЛЬНІ ВИМОГИ
з кіберзахисту об’єктів критичної інфраструктури

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

2. У цих Загальних вимогах терміни вживаються у такому значенні:

базові заходи з кіберзахисту – мінімально необхідний набір заходів з кіберзахисту, як частина каталогу заходів з кіберзахисту;

каталог заходів з кіберзахисту – впорядкований за функціями, категоріями та підкатегоріями загальний набір організаційних та технічних заходів з кіберзахисту, бажаних результатів та відповідних нормативних посилань;

кіберризик – ймовірність реалізації кіберзагрози, що може призвести до завдання шкоди або втрат, а також до порушення функціонування та стійкості інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі – системи);

поточний профіль кіберзахисту – опис фактичного стану впровадження заходів з кіберзахисту за результатами оцінювання поточного стану кіберзахисту;

цільовий профіль кіберзахисту – опис бажаного стану впровадження заходів з кіберзахисту, сформований на основі каталогу заходів з кіберзахисту за результатами управління кіберризиками.

Інші 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".

3. Кіберзахист об'єктів критичної інфраструктури забезпечується шляхом впровадження суб'єктами заходів з кіберзахисту за результатами управління кіберризиками.

Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, а також є частиною заходів із забезпечення безпеки та стійкості критичної інфраструктури.

Усі базові заходи з кіберзахисту є обов'язковими до впровадження суб'єктами.

4. Суб'єкти забезпечують оцінювання поточного стану кіберзахисту систем об'єкта критичної інфраструктури та/або об'єктів критичної інформаційної інфраструктури та формують поточний профіль кіберзахисту суб'єкта.

Суб'єкти за результатами управління кіберризиками на основі каталогу заходів з кіберзахисту формують цільовий профіль кіберзахисту суб'єкта.

Суб'єкти поетапно та послідовно досягають цільового профілю кіберзахисту шляхом впровадження визначених цим профілем заходів з кіберзахисту.

Каталог заходів з кіберзахисту, а також методичні рекомендації щодо впровадження заходів з кіберзахисту затверджуються Адміністрацією Держспецзв'язку.

5. Перше, планове та позапланове оцінювання поточного стану кіберзахисту систем об'єкта критичної інфраструктури та/або об'єктів критичної інформаційної інфраструктури здійснюється відповідно до порядку проведення оцінювання стану кіберзахисту, затвердженого Кабінетом Міністрів України, із урахуванням каталогу заходів з кіберзахисту, особливостей функціонування та архітектури об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури.

Перше оцінювання стану кіберзахисту систем об'єкта критичної інфраструктури та/або об'єктів критичної інформаційної інфраструктури здійснюється протягом 30 календарних днів з дня внесення відомостей про об'єкт критичної інфраструктури до Реєстру об'єктів критичної інфраструктури та/або про об'єкт критичної інформаційної інфраструктури до Реєстру об'єктів критичної інформаційної інфраструктури.

Планове оцінювання стану кіберзахисту систем об’єкта критичної інфраструктури та/або об’єктів критичної інформаційної інфраструктури здійснюється не рідше одного разу на рік.

6. Суб’єкти здійснюють управління кіберризиками на постійній та системній основі із застосуванням підходів, заснованих на міжнародних стандартах.

Управління кіберризиками включає ідентифікацію, оцінку та обробку кіберризиків, їх моніторинг та періодичний перегляд. Методика ідентифікації та оцінки кіберризиків затверджується Адміністрацією Держспецзв’язку.

7. З метою належного впровадження заходів з кіберзахисту суб’єкти затверджують, щорічно переглядають, та за потреби оновлюють план кіберзахисту.

План кіберзахисту розробляється на основі каталогу заходів з кіберзахисту та включає поточний і цільовий профілі кіберзахисту.

Форма плану кіберзахисту, затверджується Адміністрацією Держспецзв’язку.

8. План кіберзахисту одночасно є складовою плану захисту об’єкта критичної інфраструктури за проектною загрозою критичній інфраструктурі, що передбачає заходи із захисту та протидії кібератакам, кіберінцидентам та кіберзагрозам, який погоджується 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. 112).

9. Суб’єкти добровільно або у випадках, визначених законодавством, обов’язково забезпечують проведення авторизації з безпеки систем об’єкта критичної інфраструктури та/або об’єктів критичної інформаційної інфраструктури відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 р. № 712.

10. Суб’єкти забезпечують реагування на кіберінциденти, кібератаки та кіберзагрози з урахуванням національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого Кабінетом Міністрів України.

Суб’єкти невідкладно повідомляють CERT-UA та у разі створення – відповідну галузеву або регіональну команду реагування на кіберінциденти, кібератаки, кіберзагрози, про всі значні кіберінциденти, а також здійснюють інформаційний обмін про кіберінциденти, кіберзагрози, кібератаки відповідно до порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, затвердженого Адміністрацією Держспецзв’язку.

11. Відповідальні особи, які виконують функції та завдання керівників з кіберзахисту, або підрозділи з кіберзахисту суб’єктів здійснюють впровадження заходів з кіберзахисту, управління кіберризиками, реагування на кіберінциденти,

кібератаки та кіберзагрози, обмін інформацією про кіберінциденти, кіберзагрози, кібератаки.

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

13. Суб’єкти забезпечують планування витрат та фінансування заходів кіберзахисту, з урахуванням результатів управління кіберризиками.

14. 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.

_____