ЗАТВЕРДЖЕНО

Наказ Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України
19 грудня 2024 року № 627/772

(у редакції наказу Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України
від 12 червня 2026 року № 208/437)

РЕКОМЕНДАЦІЇ
з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент»

І. Загальні положення

1. Ці Рекомендації призначені для операторів критичної інфраструктури, які розробляють план захисту об'єкта критичної інфраструктури (далі – ОКІ) за проектною загрозою національного рівня «кібератака/кіберінцидент» (далі – Рекомендації).

2. Рекомендації розроблено відповідно до Законів України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах», постанови Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури» (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), постанови Кабінету Міністрів України від 09 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури», постанови Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» (в редакції постанови Кабінету Міністрів України від 24 грудня 2025 року № 1740), постанови Кабінету Міністрів України від 14 жовтня 2022 року № 1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури», постанови Кабінету Міністрів України від 04 серпня 2023 року № 818 «Деякі питання паспортизації об'єктів критичної інфраструктури» та з урахуванням наказу Адміністрації Держспецзв'язку від 30 січня 2026 року № 75 «Про затвердження Каталогу заходів з кіберзахисту,

базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту», наказу Адміністрації Держспецзв'язку від 18 лютого 2026 року № 143 «Деякі питання реагування на кіберінциденти, кібератаки, кіберзагрози», Проектних загроз критичній інфраструктурі національного рівня, затверджених наказом Адміністрації Держспецзв'язку від 28 липня 2023 року № 219/ДСК.

3. Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання.

4. У цих Рекомендаціях терміни вживаються в такому значенні:

реєстровий номер об'єкта критичної інформаційної інфраструктури – унікальний номер, який присвоюється кожному індивідуально визначеному об'єкту критичної інформаційної інфраструктури (далі – ОКІІ) під час внесення інформації про ОКІІ до державного реєстру об'єктів критичної інформаційної інфраструктури (далі – Реєстр), не повторюється на всій території України, залишається незмінним протягом усього часу існування такого об'єкта критичної інформаційної інфраструктури та не змінюється у разі зміни оператора критичної інфраструктури, форми власності, кінцевого бенефіціарного власника/контролера;

сфера застосування (scope) – офіційно задокументований опис меж (організаційних, фізичних та технічних) і застосовності заходів з кіберзахисту у межах оператора критичної інфраструктури та власника або розпорядника об'єктів критичної інформаційної інфраструктури (далі – суб'єкти).

Інші терміни вживаються у значеннях, наведених в Законах України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» (в редакції постанови Кабінету Міністрів України від 24 грудня 2025 року № 1740), постанові Кабінету Міністрів України від 04 серпня 2023 року № 818 «Деякі питання паспортизації об'єктів критичної інфраструктури», Методичних рекомендаціях щодо здійснення заходів з кіберзахисту, затверджених наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75, та Методичних рекомендаціях щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджених наказом Адміністрації Держспецзв'язку від 18 лютого 2026 року № 143.

5. План захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» (далі – План захисту) розробляється оператором критичної інфраструктури (далі – оператор) за формою, затвердженою наказом Служби безпеки України, Адміністрації Держспецзв'язку від 12 червня 2026 року № 208/437, відповідно до абзацу першого пункту 5 Порядку розроблення та погодження паспорта

безпеки на об’єкт критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 04 серпня 2023 року № 818.

6. Відповідно до абзацу третього пункту 4 Загальних вимог з кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), заходи, передбачені планом кіберзахисту, форма якого затверджена наказом Адміністрації Держспецзв’язку від 30 січня 2026 року № 75, взаємоузгоджуються з Планом захисту, який погоджується з функціональними органами у сфері захисту критичної інфраструктури (далі – функціональні органи) відповідно до Порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 04 серпня 2023 року № 818.

7. Інформація, яка вноситься до Плану захисту, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства у сфері захисту інформації.

8. План захисту подається оператором на погодження функціональним органам разом із супровідним листом і копією загальної характеристики ОКІ.

Підписує супровідний лист і затверджує План захисту керівник оператора або особа, яка виконує його обов’язки.

Оператору необхідно надати дозвіл уповноваженому підрозділу (органу) Служби безпеки України на копіювання поданих документів, що містять інформацію з обмеженим доступом, в порядку, визначеному законодавством.

План захисту, поданий з порушенням встановлених вимог, передбачених пунктами 5, 7 Порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 04 серпня 2023 року № 818, повертається оператору для усунення недоліків.

9. План захисту погоджується та подається у такій послідовності:

1) до уповноваженого підрозділу (органу) Адміністрації Держспецзв’язку;

2) до уповноваженого підрозділу (органу) Служби безпеки України.

10. У випадку погодження Плану захисту уповноваженим підрозділом (органом) Адміністрації Держспецзв’язку та наявності зауважень (пропозицій) до Плану захисту від уповноваженого підрозділу (органу) Служби безпеки України План захисту потребує повторного погодження кожним із вказаних уповноважених підрозділів (органів).

11. Порядок перегляду Плану захисту передбачений пунктом 12 Порядку розроблення та погодження паспорта безпеки на об’єкт критичної

інфраструктури, затвердженого постановою Кабінету Міністрів України від 04 серпня 2023 року № 818.

12. Оператор визначає інформаційні, електронні комунікаційні, інформаційно-комунікаційні або технологічні системи (далі – системи) об’єкта критичної інфраструктури, інформація про які вноситиметься до Плану захисту.

В обов’язковому порядку до Плану захисту вносяться відомості про всі ОКІІ, що експлуатуються на ОКІ.

До Плану захисту вносяться відомості про всі системи (в тому числі такі, що визначені ОКІІ) ОКІ, окрім автоматизованих систем класу «1» (окремих ПЕОМ, які не мають підключень до будь-яких інформаційно-комунікаційних систем або мереж).

Інформація про інші системи ОКІ, які не віднесено до ОКІІ, але є необхідними для стійкого та безперервного функціонування ОКІ, також підлягає обов’язковому внесенню до Плану захисту.

13. Якщо оператором не визначено жодних систем, що експлуатуються на об’єкті критичної інфраструктури, які впливають на виконання життєво важливих функцій та/або надання життєво важливих послуг, інформація про які вноситиметься до Плану захисту, оператор розробляє першу (титульну) сторінку форми Плану захисту та пояснювальну записку, в якій зазначається обґрунтування щодо відсутності критичних елементів ОКІ, на які може вплинути загроза національного рівня «кібератака/кіберінцидент».

ІІ. Порядок заповнення Плану захисту

1. На титульній сторінці Плану захисту зазначаються гриф обмеження доступу, назва ОКІ та реєстровий номер ОКІ.

2. У розділі І Плану захисту зазначаються загальні відомості:

у таблиці 1 Плану захисту зазначається інформація про системи ОКІ відповідно до пункту 12 розділу І цих Рекомендацій, зокрема: повна та скорочена назви всіх систем ОКІ, відомості про проведення ідентифікації ОКІІ та дата повідомлення секторального органу у сфері захисту критичної інфраструктури (далі – секторальний орган) про результати ідентифікації, відомості щодо наявності систем у секторальному переліку ОКІІ та наявності систем у державному реєстрі ОКІІ (реєстровий номер ОКІІ);

у таблиці 2 Плану захисту зазначаються відомості про підрозділ/підрозділи з кіберзахисту, керівника з кіберзахисту (або відповідальну особу, яка виконує його функції й завдання) відповідно до статті 5^1 Закону України «Про основні засади забезпечення кібербезпеки України», а саме: найменування підрозділу(ів) з кіберзахисту (за наявності), прізвище, власне ім'я, по батькові (у разі наявності) керівника з кіберзахисту (або відповідальної особи), займана посада, контактні дані (номер телефону, e-mail адреса);

у таблиці 3 Плану захисту зазначаються відомості про проведення

оцінювання стану кіберзахисту відповідно до постанови Кабінету Міністрів України від 31 грудня 2025 року № 1799 «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури», а саме: вид оцінювання стану кіберзахисту (самооцінювання, зовнішнє оцінювання) та період його проведення, реквізити звіту про результати оцінювання стану кіберзахисту, загальний показник стану кіберзахисту, критична ланка та якісний показник стану кіберзахисту.

Відомості, зазначені в таблиці 3 розділу I Плану захисту, повинні відповідати звіту про результати оцінювання стану кіберзахисту, форма якого затверджена наказом Адміністрації Держспецзв’язку від 16 квітня 2026 року № 285 «Деякі питання проведення оцінювання стану кіберзахисту».

3. У таблиці 4 розділу II Плану захисту зазначається опис систем ОКІ:

вид інформації за порядком доступу, яка обробляється або планується для оброблення в системах. Якщо в переліку не зазначено вид інформації, яка обробляється або планується для оброблення в системах, у графі «Інше» зазначити, яка саме;

наявність підключення до мережі Інтернет. У разі підключення до мережі Інтернет вказати повне найменування постачальника електронних комунікаційних мереж та/або послуг (далі – постачальник), перелік IP-адрес, що використовуються, та контактні дані постачальника (номер телефону, e-mail адреса). У разі отримання послуг доступу до мережі Інтернет від декількох постачальників наводяться відомості щодо кожного з них;

відомості щодо взаємодії з іншими системами, які не входять до складу систем ОКІ, а саме: повне найменування інших систем, реєстровий номер ОКІІ (за наявності), опис цієї взаємодії;

використання бездротових технологій (Wi-Fi, Bluetooth тощо). У разі використання слід вказати, які саме технології використовуються. Якщо в переліку не зазначено необхідного варіанта, в графі «Інше» варто зазначити, які саме бездротові технології використовуються;

відомості щодо використання програмних та/або апаратних засобів:

а) що мають походження або виготовлені державою-агресором;

б) внесених до відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання;

в) отриманих на безоплатній основі від фізичних або юридичних осіб, що використовуються на ОКІІ.

Для підпунктів «а» і «б» зазначається опис використання програмних та/або апаратних засобів для всіх систем, для підпункту «в» вказуються відомості лише стосовно тих засобів, що використовуються на ОКІІ.

У разі використання необхідно вказати назви програмного(их) та/або апаратного(их) засобу(ів), компанії-розробника такого(их) засобу(ів), компанії-постачальника такого(их) засобу(ів), компанії, що здійснює підтримку такого(их) засобу(ів), наявність плану по заміщенню такого(их) засобу(ів) (для підпунктів «а» і

«б»), орієнтовні терміни заміщення такого(их) засобу(ів) (для підпунктів «а» і «б»);

відомості щодо наявності взаємодії з платформами обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (MISP-UA, MISP CERT-UA або інші з переліку) (за наявності), і з якою (якими) саме. Якщо в переліку не зазначено платформу обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з якою є взаємодія, в графі слід «Інша» зазначити, яка саме використовується;

відомості щодо проведення авторизації з безпеки систем відповідно до постанови Кабінету Міністрів України від 18 червня 2025 року № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» (або отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності, або атестата відповідності комплексної системи захисту інформації) та реквізити наявних документів, зокрема реквізити повідомлення щодо включення такої системи до переліку авторизованих систем з безпеки відповідно до пункту 12 Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 року № 712. За наявності іншого документа, що засвідчує дотримання вимог щодо захисту інформації в системі, в графі «Інше» слід зазначити, який саме.

Також у розділі II Плану захисту розміщується:

рисунок загальної функціональної схеми систем (мереж) ОКІ;

опис загальної функціональної схеми систем (мереж) ОКІ та технології обробки інформації. Мають бути описані основні функції, завдання, технології обробки інформації, наявний вплив на виконання життєво важливої(их) функції(й) та/або надання життєво важливої(их) послуги(г). Опис має давати загальне уявлення про системи (мережі) ОКІ та не має перевищувати двох аркушів.

4. У таблиці 5 розділу III Плану захисту зазначаються властивості проектних загроз національного, секторального та об’єктового (за наявності) рівнів.

5. У таблиці 6 розділу IV Плану захисту зазначається опис сфери застосування заходів з кіберзахисту.

Для проведення 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.

У таблиці 6 розділу IV Плану захисту зазначаються перелік та межі підрозділів і основних операційних процесів суб’єкта, перелік систем, електронно-комунікаційних мереж та програмного забезпечення, на які

поширюються заходи з кіберзахисту, а також географічне розташування систем, приміщення, опис серверних кімнат тощо.

Чітке визначення сфери застосування в плані кіберзахисту (таблиця 7 розділу IV Плану захисту) є основою для об'єктивного оцінювання поточного стану та встановлення досяжних цілей для цільового стану кіберзахисту.

6. Таблиця 7 розділу IV Плану захисту містить сукупність усіх необхідних заходів з кіберзахисту, а також сукупність обов'язкових заходів з кіберзахисту, які в першу чергу (але не обмежуючись ними в діяльності з підвищення рівня кіберзахисту критичної інформаційної інфраструктури) мають бути впроваджені або заплановані для впровадження на ОКІ.

Модель заходів з кіберзахисту передбачає взаємозв'язки та взаємозалежність шести функцій одна від одної: «Управління» (GV), «Ідентифікація» (ID), «Забезпечення захисту» (PR), «Виявлення» (DE), «Реагування» (RS), «Відновлення» (RC).

Модель заходів з кіберзахисту описана в розділі III Методичних рекомендацій щодо здійснення заходів з кіберзахисту, затверджених наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75.

Заходи з кіберзахисту, наведені в таблиці 7 розділу IV Плану захисту, взаємоузгоджуються з планом кіберзахисту, форма якого затверджена наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75.

7. Заходи з кіберзахисту, затверджені наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75, поділяються на Каталог заходів з кіберзахисту, як сукупність усіх необхідних заходів з кіберзахисту, та Базові заходи з кіберзахисту, як сукупність обов'язкових для здійснення заходів з кіберзахисту відповідно до абзацу другого пункту 3 Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), абзацу другого пункту 25 Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (в редакції постанови Кабінету Міністрів України від 26 листопада 2025 року № 1531).

Базові заходи з кіберзахисту поділяються на:

базові заходи з кіберзахисту для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури I та II категорій критичності;

базові заходи з кіберзахисту для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури III та IV категорій критичності;

базові заходи з кіберзахисту для 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;

базові заходи з кіберзахисту для 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.

8. У таблиці 7 розділу IV Плану захисту описується поточний і цільовий стан кіберзахисту. Для визначення ступеня проведення заходів з кіберзахисту, визначених на основі Каталогу заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки, доцільно здійснювати оцінювання поточного стану кіберзахисту та визначення цільового стану кіберзахисту, де:

поточний стан кіберзахисту – фактичний стан організації та проведення заходів з кіберзахисту;

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

При заповненні опису поточного стану кіберзахисту необхідно вказати стан реалізації заходу (реалізовано, частково реалізовано, не реалізовано) та зазначити деталізований опис фактично вжитих заходів. Також варто зазначити конкретні заходи для досягнення цільового стану кіберзахисту, визначити та вказати відповідальну особу за їх виконання, зазначити запланований термін виконання заходів з кіберзахисту (це має бути найкоротший достатній строк).

9. Оператори критичної інфраструктури та власники або розпорядники об’єктів критичної інформаційної інфраструктури поетапно та послідовно досягають цільового стану кіберзахисту шляхом проведення заходів з кіберзахисту, передбачених планом кіберзахисту.

10. При заповненні таблиці 7 розділу IV Плану захисту необхідно вказати наявні ресурси, а для підтвердження вказати назву документа, номер та дату реєстрації, в якому підтверджується виконання заходу з кіберзахисту. При заповненні таблиці 7 розділу IV Плану захисту рекомендовано використовувати Методичні рекомендації щодо здійснення заходів з кіберзахисту, затверджені наказом Адміністрації Держспецзв’язку від 30 січня 2026 року № 75, та додаток до них, що містить характеристику заходів з кіберзахисту.

11. План реагування на кіберінциденти, кібератаки та кіберзагрози, який передбачений розділом V Плану захисту, розробляє керівник з кіберзахисту (або відповідальна особа, яка виконує його функції й завдання) та/або підрозділ з кіберзахисту (за наявності).

План реагування на кіберінциденти, кібератаки та кіберзагрози розробляється відповідно до постанови Кабінету Міністрів України

від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» та з урахуванням Методичних рекомендацій щодо реагування на кіберінциденти, кібератаки та кіберзагрози, затверджених наказом Адміністрації Держспецзв'язку від 18 лютого 2026 року № 143 (далі – Методичні рекомендації щодо реагування).

Відповідно до пункту 5 Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 (далі – Національний план реагування), реагування на кіберінциденти, кібератаки та кіберзагрози здійснюється суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та суб'єктами забезпечення кібербезпеки послідовно за такими етапами, як підготовка до реагування на кіберінциденти, кібератаки та кіберзагрози, виявлення, аналіз та інформування про кіберінциденти, кібератаки та кіберзагрози, стримування, усунення наслідків і відновлення після кіберінцидентів, кібератак та кіберзагроз, а також аналіз ефективності заходів реагування на кіберінциденти, кібератаки та кіберзагрози.

Оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури вживають заходів реагування на кожному з етапів відповідно до Національного плану реагування та з урахуванням Методичних рекомендацій щодо реагування.

У пункті 1 розділу V Плану захисту зазначаються реквізити плану реагування на кіберінциденти, кібератаки та кіберзагрози.

Відповідно до особливостей функціонування та затвердженого плану реагування на кіберінциденти, кібератаки та кіберзагрози на ОКІ в пункті 2 розділу V Плану захисту рекомендовано описати стисле викладення дій, що виконуються на ОКІ відповідно до етапів та процедур реагування, визначених Національним планом реагування, з урахуванням Методичних рекомендацій щодо реагування.

При заповненні пункту 2 розділу V Плану захисту рекомендовано використовувати типовий перелік заходів підготовки до реагування на кіберінциденти, кібератаки, кіберзагрози для одночасного відстеження, який викладено у додатку 3 до Методичних рекомендацій щодо реагування, та типовий перелік заходів з реагування на кіберінциденти, кібератаки, кіберзагрози для одночасного відстеження заходів до їх завершення, який викладено у додатку 2 до Методичних рекомендацій щодо реагування.

Під час обміну інформацією про кіберінциденти, кібератаки, кіберзагрози оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури керуються Загальними правилами обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (протокол TLP) та Національною таксономією кіберінцидентів, затвердженими наказом Адміністрації Держспецзв'язку від 18 лютого 2026 року № 143.

У пункті 3 розділу V необхідно вказати відповідальну особу за інформування про кіберінциденти, кібератаки та кіберзагрози із зазначенням прізвища, власного імені, по батькові (у разі наявності) відповідальної особи, посади та контактного телефону.

У пункті 4 розділу V необхідно зазначити контакти для інформування суб’єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози про кіберінциденти, кібератаки та кіберзагрози:

1) Ситуаційного центру забезпечення кібербезпеки Служби безпеки України та регіонального центру забезпечення регіонального органу Служби безпеки України за місцезнаходженням (адресою) оператора критичної інфраструктури з метою:

забезпечення Службою безпеки України реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки відповідно до пункту 3 частини другої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»;

невідкладного (негайного) інформування Служби безпеки України про кіберінциденти, а також загрози та ризики актів кібертероризму проти систем управління, операційних та інших систем об’єктів критичної інфраструктури відповідно до вимог пункту 9 частини першої, пункту 2 частини четвертої статті 21 Закону України «Про критичну інфраструктуру»;

невідкладного (протягом години) повідомлення Ситуаційного центру забезпечення кібербезпеки Служби безпеки України про всі значні кіберінциденти відповідно до вимог пункту 18 Національного плану реагування (за відсутності галузевої/регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT));

2) національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) з метою невідкладного (протягом години) повідомлення їй про всі значні кіберінциденти відповідно до вимог пункту 18 Національного плану реагування (за відсутності галузевої/регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT)) або у випадку отримання від CERT-UA в установленому порядку сервісу у зв’язку з реагуванням на кіберінциденти, кібератаки, кіберзагрози відповідно до абзацу п’ятого пункту 1 частини третьої статті 9 Закону України «Про основні засади забезпечення кібербезпеки України»;

3) галузевої/регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) з метою невідкладного (протягом години) повідомлення їй про всі значні кіберінциденти відповідно до вимог пункту 17 Національного плану реагування (за наявності такої команди реагування);

4) приватної команди реагування на кіберінциденти, кібератаки, кіберзагрози, що виконує завдання галузевої/регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) та/або може залучатися для надання операторам критичної інфраструктури, власникам або розпорядникам об’єктів критичної інформаційної інфраструктури окремих послуг, пов’язаних з реагуванням на кіберінциденти, відповідно до абзацу першого пункту 4 частини третьої статті 9 Закону України «Про основні засади забезпечення кібербезпеки України» (за наявності такої команди реагування).

12. У таблиці 8 розділу VI Плану захисту передбачено наведення зведених відомостей про моніторинг рівня безпеки об’єкта критичної інфраструктури

щодо нейтралізації загрози національного рівня «кібератака/кіберінцидент», де описуються зведені відомості про результати:

оцінки стану захищеності ОКІ (зокрема за критерієм «забезпечення кіберзахисту ОКІ»), яка проводиться відповідно до вимог статті 23 Закону України «Про критичну інфраструктуру» та Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 22 липня 2022 року № 821;

оцінювання стану кіберзахисту систем ОКІ, що здійснюється відповідно до Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури, затвердженого постановою Кабінету Міністрів України від 31 грудня 2025 року № 1799;

перевірок додержання вимог законодавства у сфері кіберзахисту, що проводяться відповідно до Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, затвердженого постановою Кабінету Міністрів України від 17 грудня 2025 року № 1668.

Після таблиці 8 розділу VI вказується відповідальна особа за заповнення Плану захисту (посада, власне ім'я та прізвище), підпис та дата підписання.

13. Таблицю додатка до Плану захисту заповнює керівник з кіберзахисту (або відповідальна особа, яка виконує його функції й завдання) у разі необхідності внесення змін до Плану захисту, які не потребують погодження функціональними органами. Після таблиці додатка до Плану захисту вказується відповідальна за заповнення Плану захисту особа (посада, власне ім'я та прізвище), підпис та дата підписання.

14. Оператори несуть відповідальність за достовірність відомостей, внесених до Плану захисту, відповідно до законодавства.

Т. в. о. начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України	Директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України
Володимир КАРАСТЕЛЬОВ	Дмитро ПАХОЛЬЧЕНКО