ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 2026 року № ___

**Методичні рекомендації**
**щодо здійснення заходів з кіберзахисту**

## І. Загальні положення

1. Ці Методичні рекомендації розроблені відповідно до абзацу четвертого пункту 26 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), абзацу п’ятого 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), пункту 6 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, підпунктів 6, $95^4$ пункту 4 та пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, та з метою належного здійснення заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

2. Методичні рекомендації щодо здійснення заходів з кіберзахисту (далі – Методичні рекомендації) розроблено з урахуванням документа NIST Cybersecurity Framework (CSF) 2.0, виданого у 2024 році Національним інститутом стандартів і технології Сполучених Штатів Америки (National Institute of Standards and Technology).

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

4. Методичні рекомендації застосовуються при здійсненні заходів з кіберзахисту органами державної влади, іншими державними органами, органами місцевого самоврядування, державними підприємствами, установами та організаціями, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі – системи), в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена

законом, операторами критичної інфраструктури та власниками або розпорядниками об’єктів критичної інформаційної інфраструктури (далі – суб’єкти) відповідно до 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), 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).

5. Ці Методичні рекомендації також застосовуються:

секторальними органами у сфері захисту критичної інфраструктури для розроблення галузевих вимог з кіберзахисту відповідно до пункту 11 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);

іншими суб’єктами, які безпосередньо проводять у межах своєї компетенції заходи із забезпечення кібербезпеки, для розроблення політик кібербезпеки та здійснення заходів з кіберзахисту згідно з пунктом 5 Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426 (в редакції постанови Кабінету Міністрів України від 20 грудня 2024 року № 1468).

6. У цих Методичних рекомендаціях термін «сфера застосування (scope)» означає офіційно задокументований опис меж (організаційних, фізичних та технічних) і застосовності заходів з кіберзахисту у межах суб’єкта.

Інші терміни вживаються у значеннях, наведених у Законах України «Про основні засади кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про критичну інфраструктуру», «Про електронні комунікації», Про Державну службу спеціального зв'язку та захисту інформації України», Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Загальних вимогах 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), Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 року № 712.

## ІІ. Заходи з кіберзахисту

1. Заходи з кіберзахисту, затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від ___ _____ 2026 року № ___, 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.

2. 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.

3. Відповідно до 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), органи державної влади, інші державні органи, органи місцевого самоврядування, державні підприємства, установи та організації, які є власниками або розпорядниками систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, під час розроблення та затвердження цільового профілю безпеки системи доповнюють його заходами з кіберзахисту, які наведені в:

базових заходах 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;

базових заходах 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.

Суб’єкти, зазначені у цьому пункті, за власним рішенням можуть не доповнювати цільовий профіль безпеки конкретної системи базовими заходами з кіберзахисту. У такому разі заходи з кіберзахисту здійснюються окремо стосовно визначеної суб’єктом сфери їх застосування на основі Каталогу заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки та вимог цих Методичних рекомендацій.

4. Кожний захід з кіберзахисту містить нормативні посилання та приклади їх виконання, які наведено в додатку 1 до цих Методичних рекомендацій. Нормативні посилання забезпечують можливість застосування положень стандартів, нормативних документів системи технічного захисту інформації, рекомендацій міжнародних організацій та спеціальних публікацій Національного інституту стандартів та технологій (NIST) США залежно від встановленого законодавством або обраного суб’єктом набору правил захисту інформації та/або кіберзахисту.

5. Заходи з кіберзахисту включають шість функцій: управління, ідентифікація, забезпечення захисту, виявлення, реагування та відновлення, які діляться на категорії та підкатегорії.

6. Здійснення заходів з кіберзахисту дозволить підвищити рівень забезпечення кібербезпеки суб’єкта, спрямованого на зниження ризиків кібербезпеки, має інтеграційний характер та формує цикл управління кібербезпекою.

## ІІІ. Модель заходів з кіберзахисту

1. Модель заходів з кіберзахисту передбачає взаємозв’язки та взаємозалежність шести функцій одна від одної (рисунок).


Рисунок. Модель заходів з кіберзахисту

2. Функція «Управління» (GV) знаходиться в центрі циклу та забезпечує контроль суб'єктом за функціонуванням всього циклу управління ризиками.

Функція «Управління» передбачає отримання результатів, які допоможуть суб'єктам визначити пріоритетність заходів інших п'яти функцій у рамках впровадження системи управління ризиками та виправдати очікування заінтересованих сторін. Упровадження заходів функції «Управління» має вирішальне значення, оскільки передбачає включення питання забезпечення кібербезпеки до стратегії управління ризиками суб'єкта, яка охоплює положення організаційного контексту, управління ризиками кібербезпеки ланцюга постачання, ролі, обов'язки та повноваження співробітників суб'єкта, політику та контроль за виконанням стратегії кібербезпеки суб'єкта.

3. Упровадження функції «Ідентифікація» (ID) дозволяє суб'єктам пріоритизувати свої ресурси та можливості відповідно до стратегії управління ризиками та потреб, визначених у функції «Управління».

«Ідентифікація» також передбачає заходи з удосконалення політик, планів, процесів та процедур суб'єкта, які підтримують управління ризиками кібербезпеки, з метою інформування про впроваджені заходи з кіберзахисту за функціями «Управління», «Ідентифікація», «Забезпечення захисту», «Виявлення», «Реагування», «Відновлення».

4. Заходи з кіберзахисту функції «Забезпечення захисту» (PR) після того, як активи і ризики визначені та пріоритизовані в функції «Ідентифікація», спрямовано на підтримку здатності суб'єкта захистити ці активи, щоб запобігти або зменшити ймовірність впливу несприятливих подій у сфері кібербезпеки, а також підвищити можливості використання переваги новітніх розробок та здобутків у сферах кібербезпеки та кіберзахисту.

Упровадження заходів функції «Забезпечення захисту» включає управління ідентифікацією, автентифікацією та контролем доступу, забезпечення обізнаності та навчання співробітників, включає безпеку даних, безпеку

фізичних та віртуальних платформ (захист апаратного, програмного забезпечення, фізичної площини, віртуальної площини) та стійкість технологічної інфраструктури.

5. Функція «Виявлення» (DE) дозволяє своєчасно виявляти та аналізувати кіберзагрози, аномалії, індикатори компрометації та інші потенційно несприятливі події, які вказують на те, що відбуваються кібератака або кіберінциденти. Ця функція підтримує успішне реагування на кіберінциденти та заходи з відновлення.

6. Функція «Реагування» (RS) підтримує здатність стримувати наслідки кіберінцидентів, кібератак, аналізувати та мінімізувати їх наслідки, звітувати про виконані дії та здійснювати ефективну комунікацію.

7. Функція «Відновлення» (RC) передбачає відновлення суб'єктом активів та операцій, що постраждали від кіберінциденту або кібератаки, і спрямована на підтримку своєчасного відновлення нормальної роботи, щоб зменшити наслідки кіберінцидентів та кібератак, забезпечити належну комунікацію під час відновлювальних робіт.

8. Наприклад, суб'єкт класифікує активи в рамках функції «Ідентифікація» та вживає заходів для захисту цих активів у рамках функції «Забезпечення захисту». Інвестиції в планування і тестування функцій «Управління» та «Ідентифікація» сприятимуть своєчасному виявленню неочікуваних подій у функції «Виявлення», а також забезпеченню реагування на кіберінциденти, кібератаки та відновлення після них у функціях «Реагування» та «Відновлення». Функція «Управління» знаходиться в центрі циклу, оскільки вона аналізує та описує те, як суб'єкт буде впроваджувати заходи інших п'яти функцій.

9. Усі заходи шести функцій виконуються одночасно. Заходи функцій «Управління», «Ідентифікація», «Забезпечення захисту» і «Виявлення» повинні виконуватися безперервно, а заходи функцій «Реагування» і «Відновлення» повинні бути готовими в будь-який час виконуватися в разі виникнення кіберінцидентів або кібератак. Усі заходи з кіберзахисту відіграють важливу роль у реагуванні на кіберінциденти, кібератаки та кіберзагрози. Заходи функцій «Управління», «Ідентифікація», «Забезпечення захисту» сприяють запобігання кіберінцидентам і готовність суб'єкта до них, тоді як заходи функцій «Управління», «Виявлення», «Реагування» та «Відновлення» допомагають суб'єкту виявляти та реагувати на кіберінциденти, кібератаки та кіберзагрози.

10. Назва кожного із шести функцій з кіберзахисту та категорій описує їх зміст. Кожна функція поділяється на категорії, пов'язані із заходами з кіберзахисту, які вони включають, кожна категорія поділяється на підкатегорію, які в свою чергу поділяються на більш конкретні заходи технічного та управлінського характеру. Підкатегорії містять приклади заходів, які не є вичерпними, але вони описують детальні результати, які підтримують досягнення кожного заходу з кіберзахисту в кожній підкатегорії та категорії.

11. Шість функцій, їх категорії та підкатегорії застосовуються до всієї сфери застосування, яку визначив суб’єкт, тобто до всіх інформаційно-комунікаційних технологій, що використовує суб’єкт, включаючи інформаційні технології, Інтернет речей та операційні технології. Вони також застосовуються до всіх типів технологічних середовищ, включаючи хмарні, мобільні та системи штучного інтелекту.

12. У додатку 1 наведено розгорнуту характеристику заходів з кіберзахисту, надано нормативні посилання та приклади впровадження таких заходів.

Нормативні посилання відображають взаємозв’язки між підкатегоріями та різними стандартами, рекомендаціями, нормативно-правовими актами та іншими документами. Інформативні посилання допомагають визначити, як суб’єкт може досягти бажаних результатів кожного заходу з кіберзахисту. Інформативні посилання можуть бути специфічними для сектору критичної інфраструктури, об’єднань підприємств або для конкретної технології. Суб’єкти можуть визначити найбільш відповідні інформативні посилання при здійснення заходів з кіберзахисту та формуванні плану кіберзахисту.

Приклади впровадження надають уявні приклади лаконічних, дієвих кроків для досягнення результатів підкатегорій. Дієслова, які використовуються в прикладах: поділитися, задокументувати, розробити, виконати, контролювати, аналізувати, оцінювати, забезпечити, пересвідчитися тощо. Приклади не є вичерпним списком всіх можливих дій, які треба виконати суб’єкту для досягнення бажаного результату, і вони не являють собою базовий набір обов’язкових дій для вирішення питання кіберзахисту на об’єкті.

13. Суб’єкт при здійсненні заходів з кіберзахисту має враховувати свою місію та ризики кібербезпеки.

З розумінням очікувань заінтересованих сторін та допустимого рівня ризику (як описано в функції «Управління») суб’єкт може пріоритизувати заходи з кіберзахисту для прийняття обґрунтованих рішень щодо витрат і дій.

Доцільним є впровадження в діяльність суб’єкта ведення реєстру ризиків кібербезпеки (кіберризиків) або їх об’єднань. Суб’єкти здійснюють управління ризиками кібербезпеки на постійній та системній основі для запобігання виникненню кіберінциденту, кібератаки та/або реалізації кіберзагрози і мінімізації можливих їх наслідків.

Суб’єкт обирає прийнятний спосіб обробки ризику: зменшення, передача, уникнення або прийняття негативних ризиків та реалізацію, спільне використання, підвищення або прийняття позитивних ризиків (залежно від потенційних наслідків та ймовірності).

Суб’єкт може використовувати заходи з кіберзахисту як внутрішній інструмент для управління своєю кібербезпекою, так і зовнішній – для контролю або комунікації з третіми сторонами.

Відповідно до пункту 6 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 третього пункту 28 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), методика оцінювання ризиків кібербезпеки затверджується Адміністрацією Держспецзв'язку.

14. Заходи з кіберзахисту передбачають покращення комунікації щодо очікувань, планування та ресурсів у сфері кібербезпеки. Вони сприяють двосторонньому обміну інформацією між керівниками, які зосереджуються на пріоритетах та стратегічних напрямах функціонування суб'єкта, і менеджерами, які управляють конкретними ризиками кібербезпеки, що можуть вплинути на досягнення цих пріоритетів. Також сприяють обміну між менеджерами та фахівцями, які впроваджують та експлуатують технології.

## IV. План кіберзахисту

1. 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, відповідно до абзацу першого 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), та абзацу першого пункту 26 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).

2. 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.

3. 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.

4. Для визначення ступеня здійснення 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 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.

5. План кіберзахисту використовується для розуміння суб'єктом кількості заходів з кіберзахисту, яких необхідно вжити або адаптувати раніше вжиті заходи відповідно до шести функцій моделі заходів з кіберзахисту.

6. План кіберзахисту містить опис сфери застосування заходів з кіберзахисту, визначеної суб'єктом відповідно до пункту 2 розділу II цих Методичних рекомендацій. Опис сфери застосування в плані кіберзахисту має включати: 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 є основою для об'єктивного оцінювання поточного стану та встановлення досяжних цілей для цільового стану кіберзахисту.

7. Форма плану кіберзахисту затверджується наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від ___ _____ 2026 року № ___.

8. План кіберзахисту взаємоузгоджується з планом захисту об'єкта критичної інфраструктури за проєктною 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 04 серпня 2023 року № 818.

9. Суб'єкти поетапно та послідовно досягають цільового стану кіберзахисту шляхом здійснення заходів з кіберзахисту, передбачених планом кіберзахисту.

10. При розробці та оновленні плану кіберзахисту рекомендовано враховувати результати проведення аналізу ефективності реагування на кіберінциденти, кібератаки або кіберзагрози.

## V. Рівні впровадження заходів з кіберзахисту

1. Суб'єкт для формування поточного та цільового стану кіберзахисту може використовувати рівні їх впровадження (зрілості). Рівні характеризують контроль і суворе дотримання практик управління ризиками кібербезпеки, а також надають контекст того, як суб'єктом розглядаються ризики кібербезпеки та процеси, що застосовуються для управління цими ризиками.

2. Рівні відображають практики суб’єкта з управління ризиками кібербезпеки як часткові (Рівень 1), ризико-орієнтовані (Рівень 2), повторювані (Рівень 3) та адаптивні (Рівень 4).

Рівні описують перехід від неформальних, ситуативних заходів реагування до підходів, які є гнучкими, заснованими на оцінці ризиків кібербезпеки та постійно вдосконалюються. Вибір рівнів допомагає задати загальний тон тому, як суб’єкт керуватиме ризиками кібербезпеки.

3. Рівні характеризують суворість практик організації з управління ризиками кібербезпеки («Управління») і практик управління ризиками кібербезпеки («Ідентифікація», «Забезпечення захисту», «Виявлення», «Реагування» та «Відновлення»).

4. Рівень 1: частковий. Застосування організаційної стратегії ризиків кібербезпеки управляється в індивідуальному порядку. Пріоритизація є випадковою і формально не базується на цілях чи середовищі загроз.

Обізнаність про ризики кібербезпеки на організаційному рівні обмежена.

Суб’єкт впроваджує управління ризиками кібербезпеки на нерегулярній основі, від випадку до випадку.

Суб’єкт може не мати процесів, які дозволяють обмінюватися інформацією про кібербезпеку всередині. Суб’єкт, як правило, не знає про ризики кібербезпеки, пов’язані з його постачальниками товарів, робіт, послуг, які він придбав та використовує.

5. Рівень 2: поінформований про ризик. Методи управління ризиками затверджуються керівництвом та можуть (не можуть) бути встановлені як загальна організаційна політика. Пріоритизація діяльності з кібербезпеки та потреб у захисті безпосередньо залежить від цілей організаційних ризиків, середовища загроз або вимог суб’єкта, його місії.

Існує усвідомлення ризиків кібербезпеки на організаційному рівні, але загально-організаційного підходу до управління ризиками кібербезпеки не встановлено.

Урахування кібербезпеки в організаційних цілях і програмах може мати місце на деяких, але не на всіх рівнях. Оцінка ризиків кібербезпеки організаційних та зовнішніх активів здійснюється, але зазвичай не є повторюваною або періодичною.

Суб’єкт усвідомлює ризики кібербезпеки, пов’язані з його постачальниками товарів, робіт, послуг, які він придбав та використовує, але не діє послідовно чи формально у відповідь на ці ризики.

6. Рівень 3: повторюваний. Практика управління ризиками офіційно затверджена та виражена як політика. Політики, процеси та процедури з урахуванням ризиків визначаються, впроваджуються за призначенням і переглядаються.

Організаційні практики кібербезпеки регулярно оновлюються на основі застосування процесів управління ризиками до змін у вимогах суб’єкта, його місії, загрозах і технологічному ландшафті.

Існує загально-організаційний підхід до управління ризиками кібербезпеки. Інформація про кібербезпеку регулярно передається. Існують узгоджені методи для ефективного реагування на зміни ризику. Персонал суб’єкта володіє знаннями та навичками для виконання своїх призначених ролей і обов'язків.

Суб’єкт постійно та точно відстежує ризики кібербезпеки активів. Керівники вищої ланки з кібербезпеки та поза кібербезпекою регулярно спілкуються щодо ризиків кібербезпеки. Керівники суб’єкта забезпечують врахування кібербезпеки на всіх напрямах діяльності.

Стратегія ризиків ґрунтується на ризиках кібербезпеки, пов’язаних з постачальниками товарів, робіт, послуг суб’єкта, які він придбав і використовує.

Співробітники суб’єкта офіційно реагують на ці ризики за допомогою таких механізмів, як письмові договори, що визначають базові вимоги, структури управління (наприклад, відділ з управління ризиками), а також впровадження та моніторинг політики. Ці дії впроваджуються послідовно та за призначенням, а також постійно контролюються та переглядаються.

7. Рівень 4: адаптивний. Існує загально-організаційний підхід до управління ризиками кібербезпеки, який використовує політику, процеси та процедури з урахуванням ризиків для вирішення потенційних подій кібербезпеки.

Взаємозв’язок між ризиками кібербезпеки та цілями чітко розуміється та враховується під час прийняття рішень. Керівники суб’єкта контролюють ризики кібербезпеки в тому самому контексті, що й фінансові та інші організаційні ризики.

Бюджет суб’єкта формується з урахуванням аналізу поточного та прогнозованого середовища ризику, а також рівня прийнятної толерантності до ризику.

Процес управління ризиками кібербезпеки є частиною організаційної культури суб’єкта. Цей процес ґрунтується на аналізі попереднього досвіду діяльності та забезпеченні постійного моніторингу операцій у системах та мережах.

Суб’єкт оперативно та ефективно адаптується до змін у цілях діяльності або завданнях, пов’язаних з основною місією. Це дозволяє своєчасно коригувати підходи до управління ризиками та інформувати про них відповідно до актуальних потреб інших суб’єктів.

Суб’єкт адаптує свої практики кібербезпеки на основі попередньої та поточної діяльності з кіберзахисту, включаючи отримані уроки та прогнозні показники. Завдяки процесу безперервного вдосконалення, який включає передові технології та практики кібербезпеки, суб’єкт активно адаптується до мінливого технологічного ландшафту та своєчасно й ефективно реагує на складні кіберзагрози, що розвиваються.

Суб’єкт застосовує інформацію в реальному часі або максимально наближену до нього для оцінки ризиків кібербезпеки, пов’язаних з постачальниками товарів, робіт, послуг, які закуповуються та використовуються. Це дозволяє своєчасно і послідовно реагувати на виявлені загрози та мінімізувати потенційні ризики.

## VI. Оцінювання стану кіберзахисту

1. Суб’єкт з метою визначення поточного стану та/або цільового стану кіберзахисту забезпечує оцінювання стану кіберзахисту 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.

2. Оцінювання стану кіберзахисту здійснюється на основі рівнів їх впровадження (зрілості) з урахуванням каталогу заходів з кіберзахисту, особливостей функціонування та архітектури систем. Рівні впровадження (зрілості) характеризують контроль і суворе дотримання практик управління ризиками кібербезпеки, а також надають контекст того, як суб’єктом розглядаються ризики кібербезпеки та процеси, що застосовуються для управління цими ризиками.

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