

Додаток 3
до галузевих вимог з кіберзахисту
об'єктів критичної інфраструктури
сектору «охорона здоров'я»
(пункт 6 розділу VI)

Гриф обмеження доступу
(зазначається за необхідності після заповнення)

ЗАТВЕРДЖЕНО

(найменування посади керівника суб'єкта

або особи, що його заміщує)

(підпис)

(власне ім'я, прізвище)

____ 20__ р.

МП (у разі наявності)

План кіберзахисту

(найменування суб'єкта)

I. Загальні відомості

1. Відомості про орган державної влади, інший державний орган, орган місцевого самоврядування, державне підприємство, установу та організацію, який/яка є власником або розпорядником 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, оператора критичної інфраструктури, власника або розпорядника об'єкта критичної інформаційної інфраструктури (далі – суб'єкти), а також відомості про інші підприємства, установи та організації, які залучені до забезпечення функціонування систем суб'єкта.

2. Відомості про підрозділ з кіберзахисту, керівника з кіберзахисту суб'єкта (або відповідальної особи, яка виконує його функції й завдання).

3. Опис сфери застосування заходів з кіберзахисту.

II. Описи поточного та/або цільового стану кіберзахисту

№ з/п	Ідентифікатор заходу	Заходи з кіберзахисту	Опис поточного стану кіберзахисту	Опис цільового стану кіберзахисту (конкретні заходи для досягнення цільового стану)	Відповідальна особа	Запланований термін виконання заходів
1	2	3	4	5	6	7
1.	Функція Управління (GV)					
1.	GV.OC-01	Забезпечується розуміння місії суб'єкта та її врахування при управлінні ризиками кібербезпеки				
2.	GV.OC-02	Визначаються внутрішні та зовнішні заінтересовані сторони, забезпечується розуміння та врахування їхніх потреб і очікувань щодо управління ризиками				
3.	GV.OC-03	Визначається та забезпечується виконання співробітниками чинних законодавчих, нормативних та договірних вимог, а також вимог суб'єкта щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод				
4.	GV.RM-01	Визначаються та узгоджуються із заінтересованими сторонами суб'єкта цілі управління ризиками кібербезпеки				
5.	GV.RM-02	Визначається допустимий рівень ризику кібербезпеки, який суб'єкт може прийняти, доводиться до відома всіх співробітників та заінтересованих сторін і підтримується така інформація в актуальному стані				
6.	GV.RM-03	Додається до загальних процесів управління ризиками суб'єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей				
7.	GV.RR-01	Визначається із числа керівництва суб'єкта посадова особа, яка звітує про ризики кібербезпеки та підтримання культури поведінки щодо усвідомлення ризиків та етики, її постійне вдосконалення, а також відповідає за них				
8.	GV.RR-02	Встановлюється, забезпечується комунікація, розуміння та дотримання ролей та повноважень щодо управління ризиками				
9.	GV.RR-03	Визначаються необхідні ресурси відповідно до стратегії управління ризиками кібербезпеки, ролей, відповідальності та політик				
10.	GV.PO-01	Розроблюється та доводиться до відома співробітників суб'єкта політика управління ризиками кібербезпеки, яка визначена з урахуванням структури суб'єкта, стратегії кібербезпеки та пріоритетів				

1	2	3	4	5	6	7
11.	GV.SC-01	Розроблюється програма, стратегія, цілі, політика та процеси управління ризиками кібербезпеки, пов'язаними з ланцюгами постачання, погоджується із заінтересованими сторонами суб'єкта				
12.	GV.SC-02	Розроблюється, здійснюється внутрішня та зовнішня координація ролей з кібербезпеки при їх виконанні постачальниками товарів, робіт, послуг, користувачами та партнерами суб'єкта				
13.	GV.SC-03	Забезпечується інтеграція управління ризиками ланцюга постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки суб'єкта, оцінки ризиків і їх вдосконалення				
14.	GV.SC-05	Встановлюються вимоги, пов'язані з ризиками кібербезпеки в ланцюгах постачання, та впроваджуються в договори/контракти або інші типи договорів з постачальниками товарів, робіт, послуг та відповідними третіми сторонами				
15.	GV.SC-08	Забезпечується залучення відповідних постачальників товарів, робіт, послуг та інших третіх сторін до діяльності щодо планування, реагування на кіберінциденти, кібератаки, кіберзагрози та відновлення після них				
2.	Функція Ідентифікація (ID)					
16.	ID.AM-01	Забезпечується періодичне проведення інвентаризації обладнання, яким керує суб'єкт				
17.	ID.AM-02	Забезпечується періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує суб'єкт				
18.	ID.AM-03	Забезпечується підтримка використання авторизованих мережевих з'єднань та визначаються внутрішні і зовнішні мережеві потоки				
19.	ID.AM-04	Забезпечується періодичне проведення інвентаризації послуг, що надаються постачальниками товарів, робіт, послуг				
20.	ID.AM-05	Проводиться розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта				
21.	ID.AM-08	Забезпечується управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу				

1	2	3	4	5	6	7
22.	ID.RA-01	Ідентифікуються, підтверджуються та ведуться записи щодо вразливих місць активів				
23.	ID.RA-02	Організується отримання інформації про кіберзагрози та вразливості з платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з репозиторію інформації про кіберінциденти, інших офіційних джерел				
24.	ID.RA-03	Визначаються та документуються внутрішні та зовнішні кіберзагрози				
25.	ID.RA-04	Визначаються та документуються потенційні наслідки та вірогідні загрози, пов'язані з експлуатацією кіберзагроз та вразливостей				
26.	ID.RA-06	Визначаються заходи реагування на ризики кібербезпеки та встановлюється їх пріоритетність, забезпечується їх відслідковування та комунікація щодо них				
27.	ID.RA-08	Визначаються процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості				
28.	ID.RA-09	Проводиться перевірка автентичності і цілісності обладнання та програмного забезпечення перед його придбанням і використанням				
29.	ID.IM-01	Визначаються напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту				
30.	ID.IM-04	Розроблюються, затверджуються, доводяться до відома співробітників, переглядається та удосконалюється план реагування на кіберінциденти, кібератаки або кіберзагрози відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, внутрішні політики кібербезпеки, план кіберзахисту та інші регламентуючі документи, які впливають на діяльність суб'єкта				
3.	Функція Забезпечення захисту (PR)					
31.	PR.AA-01	Забезпечується на рівні суб'єкта керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення				
32.	PR.AA-03	Забезпечується автентифікація користувачів, служб та апаратного забезпечення				

1	2	3	4	5	6	7
33.	PR.AA-05	Визначаються в політиці, дотримуючись принципів найменших привілеїв і розподілу обов'язків, дозволи доступу, повноваження та авторизації, керувати ними, застосовувати та переглядати				
34.	PR.AA-06	Здійснюється управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки				
35.	PR.AT-01	Систематично проводяться інструктажі та тренінги з кібергігієни, а також забезпечується обізнаність і навченість співробітників таким чином, що вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки				
36.	PR.AT-02	Забезпечується обізнаність та навченість співробітників, які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту таким чином, що вони мали знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки				
37.	PR.DS-01	Забезпечується конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб'єкта				
38.	PR.DS-02	Забезпечується конфіденційність, цілісність і доступність даних, що передаються				
39.	PR.DS-10	Забезпечується конфіденційність, цілісність і доступність даних, що використовуються: до яких є доступ; які обробляються та регулярно оновлюються застосунками, користувачами або пристроями суб'єкта				
40.	PR.DS-11	Забезпечується створення, захист, підтримка та тестування резервних копій даних				
41.	PR.PS-01	Встановлюються та застосовуються методи керування конфігурацією				
42.	PR.PS-04	Створюються записи журналів подій, які зроблені доступними для постійного моніторингу				
43.	PR.PS-05	Забораються встановлення та виконання несанкціонованого програмного забезпечення				
44.	PR.IR-01	Забезпечується захист мережі та середовища від неавторизованого логічного доступу та використання				
45.	PR.IR-03	Реалізуються механізми для досягнення вимог стійкості в нормальних і несприятливих ситуаціях				
4.	Функція Виявлення (DE)					
46.	DE.CM-01	Проводиться постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій				

1	2	3	4	5	6	7
47.	DE.CM-03	Проводиться постійний моніторинг діяльності співробітників і використання ними технологій для виявлення потенційно несприятливих подій				
48.	DE.CM-06	Проводиться постійний моніторинг діяльності і послуг зовнішнього постачальника товарів, робіт, послуг для виявлення потенційно несприятливих подій				
49.	DE.CM-09	Проводиться постійний моніторинг використання комп'ютерного обладнання та програмного забезпечення, середовища їх виконання та даних для виявлення потенційно несприятливих подій				
50.	DE.AE-02	Періодично проводиться аналіз потенційно несприятливих подій для кращого розуміння пов'язаних подій				
51.	DE.AE-06	Забезпечується передавання інформації про несприятливі події до уповноважених суб'єктів для використання відповідного інструментарію				
52.	DE.AE-07	Забезпечується збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації				
5.	Функція Реагування (RS)					
53.	RS.MA-01	Упроваджується виконання плану реагування на кіберінциденти, кібератаки або кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту				
54.	RS.MA-03	Упроваджується таксономія та пріоритизація кіберінцидентів				
55.	RS.AN-03	Упроваджується проведення аналізу для встановлення того, що відбулося під час кіберінциденту та які джерела виникнення кіберінциденту				
56.	RS.AN-06	Упроваджується здійснення запису дій, які виконуються під час розслідування кіберінциденту, та забезпечується цілісність і збереження таких записів				
57.	RS.AN-07	Упроваджується здійснення збору та забезпечується цілісність та збереження даних про кіберінциденти та метаданих				
58.	RS.CO-02	Упроваджується сповіщення внутрішніх та зовнішніх заінтересованих сторін про кіберінциденти, кібератаки та кіберзагрози				
59.	RS.CO-03	Упроваджується надання інформації визначеним внутрішнім і зовнішнім заінтересованим сторонам				

1	2	3	4	5	6	7
60.	RS.MI-01	Забезпечується локалізація кіберінцидентів				
61.	RS.MI-02	Забезпечується ліквідація кіберінцидентів				
6.	Функція Відновлення (RC)					
62.	RC.RP-01	Забезпечується виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення одразу після їх ініціалізації в ході реагування на кіберінциденти, кібератаки та кіберзагрози				
63.	RC.RP-02	Забезпечується відбір, визначення обсягу, пріоритетність та виконання заходів з відновлення				
64.	RC.RP-03	Перевіряється цілісність резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення				
65.	RC.RP-05	Перевіряється цілісність відновлених активів, відновлених систем та служб і підтверджується їх робочий стан				
66.	RC.CO-03	Забезпечується інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей				
67.	RC.CO-04	Забезпечується інформування суспільства про відновлення після кіберінциденту, кібератаки, використовуючи затверджені методи та повідомлення, відповідно до Порядку публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх наслідків, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533				

Особа, відповідальна за заповнення плану:

(посада)

_____.2026

(підпис, власне ім'я, прізвище)