Прим. № __

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стандартизація криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

СТД-04-002-2026-В

ЗАХОДИ З КІБЕРЗАХИСТУ. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА НАСТАНОВИ

Київ
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
2026

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: призначеним органом стандартизації у сфері криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам Державної служби спеціального зв’язку та захисту інформації України – Державним науково-дослідним інститутом технологій кібербезпеки та захисту інформації.

РОЗРОБНИКИ: **М. Комаров**, канд. техн. наук, керівник розробки; **О. Верховець; К. Гуляєв**, канд. техн. наук, ст. наук. співроб.; **В. Гольнєв**; **Р. Цирень; О. Рущак**; **І. Писанко**; **Д. Жарук**; **Т. Грищишина**.

2 ПОГОДЖЕНО: Адміністрацією Державної служби спеціального зв’язку та захисту інформації України (лист від «____» _____ 2026 р. № _____).

3 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказом Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від «____» _____ 2026 р. № _____, з «____» _____ 2026 р.

4 Цей стандарт застосовується на добровільній основі, крім випадків, якщо обов’язковість його застосування встановлена нормативно-правовими актами.

5 Право власності на стандарти криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам належить державі в особі Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, який розповсюджує такі стандарти.

6 УВЕДЕНО ВПЕРШЕ.

ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ....4
2 НОРМАТИВНІ ПОСИЛАННЯ....5
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ....5
4 ПОЗНАКИ ТА СКОРОЧЕННЯ....7
5 ЗАГАЛЬНІ ПОЛОЖЕННЯ....8
5.1 Мета й принципи здійснення заходів з кіберзахисту....8
5.2 Загальні положення щодо оцінювання стану кіберзахисту....9
6 МОДЕЛЬ ЗАХОДІВ З КІБЕРЗАХИСТУ....10
7 КАТАЛОГ ЗАХОДІВ З КІБЕРЗАХИСТУ....12
7.1 Загальна характеристика Каталогу заходів з кіберзахисту....12
7.2 Функції та категорії заходів з кіберзахисту....12
7.3 План кіберзахисту....14
7.4 Рівні впровадження заходів з кіберзахисту....15
ДОДАТОК А (обов’язковий) КАТАЛОГ ЗАХОДІВ З КІБЕРЗАХИСТУ....17
ДОДАТОК Б (обов’язковий) ФОРМА ПЛАНУ КІБЕРЗАХИСТУ....31
БІБЛІОГРАФІЯ....34

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Цей стандарт установлює загальні положення, вимоги та уніфіковані настанови щодо формування, планування, здійснення, моніторингу та вдосконалення заходів з кіберзахисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури.

1.2 Суб’єктами застосування цього стандарту є органи державної влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від форм власності, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також секторальні органи у сфері захисту критичної інфраструктури – для розроблення галузевих вимог з кіберзахисту відповідно до Загальних вимог з кіберзахисту об’єктів критичної інфраструктури [4], оператори критичної інфраструктури, власники та/або розпорядники об’єктів критичної інформаційної інфраструктури, суб’єкти господарювання, які безпосередньо проводять у межах своєї компетенції заходи із забезпечення кібербезпеки – для розроблення політик кібербезпеки та здійснення заходів з кіберзахисту відповідно до Положення про організаційно-технічну модель кіберзахисту [5].

1.3 Об’єктами застосування цього стандарту є об’єкти кіберзахисту.

1.4 Цей стандарт не поширюється на вимоги до технічної реалізації засобів захисту інформації та криптографічних модулів, що є предметом окремих стандартів і нормативних документів у сфері технічного та криптографічного захисту інформації.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такі нормативні документи:

СТД-01-001-2026-В Вимоги до побудови, викладення, оформлення, позначення та змісту стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

Примітка. У разі заміни нормативного документа, на який наведено посилання, слід застосовувати новий нормативний документ. У разі скасування нормативного документа, на який наведено посилання, слід застосовувати останню чинну на момент застосування редакцію нормативного документа. Якщо до нормативного документа, на який наведено посилання, внесено зміни (поправки), застосовують цей нормативний документ з урахуванням усіх внесених до нього змін (поправок).

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті терміни вживаються в значенні, наведеному в Законах України «Про основні засади забезпечення кібербезпеки України» [1] (кібербезпека, кіберзахист, кіберзагроза, кібератака, кіберінцидент), об’єкт критичної інформаційної інфраструктури, технологічна система (система управління технологічними процесами), «Про захист інформації в інформаційно-комунікаційних системах» [2] (інформаційна (автоматизована) система, електронна комунікаційна система, інформаційно-комунікаційна система, криптографічний захист інформації, технічний захист інформації), «Про критичну інфраструктуру» [3] (об’єкт критичної інфраструктури, оператор критичної інфраструктури), Загальних вимогах з кіберзахисту об’єктів критичної інфраструктури [4] (ризик кібербезпеки), Положенні про організаційно-технічну модель кіберзахисту [5] (кібергігієна) та ДСТУ ISO/IEC 27005:2023 [10] (вразливість).

Нижче подано терміни, додатково вжиті в цьому стандарті, та визначення позначених ними понять.

3.1 каталог заходів з кіберзахисту (Каталог)

Систематизований перелік (довідник) організаційних та технічних заходів з кіберзахисту, призначених для формування системи захисту об’єктів кіберзахисту з урахуванням результатів управління ризиками кібербезпеки

3.2 план кіберзахисту

Документ, який описує поточний та/або цільовий стани кіберзахисту та розробляється з урахуванням результатів управління ризиками кібербезпеки на основі каталогу заходів з кіберзахисту

3.3 поточний стан кіберзахисту

Сукупність досягнутих показників захищеності об’єктів кіберзахисту, що визначається рівнем застосування заходів з кіберзахисту та їхньою здатністю протидіяти актуальним кіберзагрозам

3.4 цільовий стан кіберзахисту

Запланований рівень впровадження та ефективності заходів з кіберзахисту, обраних із каталогу заходів з кіберзахисту за результатами оцінки ризиків кібербезпеки, якого організація прагне досягти

3.5 сфера застосування заходів з кіберзахисту

Офіційно задокументований опис меж (організаційних, фізичних та технічних) і застосовності заходів з кіберзахисту в межах організації

3.6 рівень впровадження заходів з кіберзахисту

Характеристика контролю й суворості дотримання практик управління ризиками кібербезпеки, яка надає контекст того, як організацією розглядаються ризики кібербезпеки та процеси, що застосовуються для управління ними

3.7 роль

Сукупність функціональних обов’язків і повноважень щодо кібербезпеки, закріплених за посадовою особою або структурним підрозділом суб’єкта забезпечення кібербезпеки

Примітка 1. Роль не тотожна функції моделі заходів з кіберзахисту, визначеній у 6.1.

Примітка 2. У цьому стандарті терміни «система», «системи» вживаються в значенні «інформаційні, електронні комунікаційні, інформаційно-комунікаційні та технологічні системи».

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

4.1 У цьому стандарті вжито такі скорочення:

АЗ – апаратне забезпечення;

Каталог – Каталог заходів з кіберзахисту;

ПЗ – програмне забезпечення;

СТД – стандарт криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;

CSF – фреймворк кібербезпеки (*cybersecurity framework*);

NIST – Національний інститут стандартів та технології Сполучених Штатів Америки (*National Institute of Standards and Technology*).

4.2 У цьому стандарті вжито такі познаки функцій та категорій заходів з кіберзахисту:

DE – виявлення (*Detect*);

DE.CM – безперервний моніторинг;

DE.AE – аналіз несприятливих подій;

GV – стратегічне керівництво (*Govern*);

GV.OC – організаційний контекст;

GV.RM – політика управління ризиками кібербезпеки;

GV.RR – ролі (функціональні обов’язки), обов’язки та повноваження;

GV.PO – політика;

GV.OV – нагляд;

GV.SC – управління ризиками ланцюга постачання;

ID – ідентифікація (*Identify*), забезпечується розуміння поточних ризиків кібербезпеки;

ID.AM – управління активами;

ID.RA – оцінювання ризиків кібербезпеки;

ID.IM – удосконалення;

PR – захист (*Protect*);

PR.AA – управління ідентифікацією, автентифікація та контроль доступу;

PR.AT – обізнаність і навчання з питань кібербезпеки;

PR.DS – безпека даних;

PR.PS – безпека платформ;

PR.IR – стійкість технологічної інфраструктури;

RS – реагування (*Respond*);

RS.MA – управління кіберінцидентами;

RS.AN – аналіз кіберінциденту;

RS.CO – звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація;

RS.MI – мінімізація наслідків кіберінцидентів;

RC – відновлення (*Recover*);

RC.RP – виконання плану відновлення після кіберінциденту;

RC.CO – комунікація з відновлення після кіберінциденту.

5 ЗАГАЛЬНІ ПОЛОЖЕННЯ

5.1 Мета й принципи здійснення заходів з кіберзахисту

5.1.1 Метою здійснення заходів з кіберзахисту є забезпечення кібербезпеки об’єктів кіберзахисту шляхом запобігання кіберінцидентам, виявлення кібератак та захисту від них, усунення їхніх наслідків, а також відновлення сталості й надійності функціонування комунікаційних і технологічних систем.

5.1.2 Суб’єкти забезпечення кібербезпеки здійснюють заходи з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки. Управління ризиками кібербезпеки здійснюють на постійній та системній основі для запобігання виникненню кіберінциденту, здійсненню кібератак і реалізації кіберзагроз та зменшення їхніх можливих наслідків.

5.1.3 Здійснення заходів з кіберзахисту ґрунтується на таких принципах:

– ризик-орієнтованість – визначення заходів з кіберзахисту та їх пріоритету з урахуванням результатів управління ризиками кібербезпеки, місії суб'єкта забезпечення кібербезпеки та очікувань заінтересованих сторін;

– безперервність – заходи функцій «Стратегічне керівництво», «Ідентифікація», «Захист» та «Виявлення» виконуються безперервно, а заходи функцій «Реагування» та «Відновлення» мають бути готовими до виконання в будь-який час у разі виникнення кіберінцидентів або кібератак;

– системність та інтеграційний характер – заходи з кіберзахисту розглядаються як єдина взаємопов'язана сукупність, що формує цикл управління кібербезпекою суб'єкта забезпечення кібербезпеки;

– гармонізація з міжнародними практиками – заходи з кіберзахисту розроблено з урахуванням NIST CSF 2.0 [11] та узгоджено з положеннями ДСТУ ISO/IEC 27001 [8] та ДСТУ ISO/IEC 27002 [9];

– технологічна нейтральність – заходи з кіберзахисту застосовують до всіх типів технологічних середовищ, зокрема хмарних і мобільних середовищ та систем штучного інтелекту.

5.2 Загальні положення щодо оцінювання стану кіберзахисту

5.2.1 Суб'єкт забезпечення кібербезпеки з метою визначення поточного стану та/або цільового стану кіберзахисту забезпечує оцінювання стану кіберзахисту. Оцінювання стану кіберзахисту здійснюють на основі рівнів впровадження заходів з кіберзахисту з урахуванням Каталогу, особливостей функціонування та архітектури систем.

5.2.2 За результатами оцінювання встановлюють значення рівнів впровадження, що характеризують контроль та суворе дотримання практик управління ризиками кібербезпеки, а також надають контекст того, як суб'єктом забезпечення кібербезпеки розглядаються ризики кібербезпеки та процеси, що застосовуються для управління цими ризиками. Результати оцінювання стану кіберзахисту використовують під час перегляду плану кіберзахисту.

6 МОДЕЛЬ ЗАХОДІВ З КІБЕРЗАХИСТУ

6.1 Модель заходів з кіберзахисту охоплює шість функцій: стратегічне керівництво (GV), ідентифікація (ID), захист (PR), виявлення (DE), реагування (RS) та відновлення (RC). Кожна функція поділяється на категорії, пов’язані із заходами з кіберзахисту, які вони охоплюють, кожна категорія поділяється на підкатегорії, які, своєю чергою, поділяються на конкретизовані заходи технічного та управлінського характеру.

6.2 Функція «Стратегічне керівництво» (GV) є наскрізною та розташована в центрі моделі. Вона визначає результати, які допомагають суб’єкту забезпечення кібербезпеки обрати підхід до використання заходів інших п’яти функцій та визначити їхню пріоритетність з урахуванням місії суб’єкта забезпечення кібербезпеки й очікувань заінтересованих сторін. Реалізація функції «Стратегічне керівництво» забезпечує інтеграцію питань кібербезпеки до загальної системи управління ризиками суб’єкта забезпечення кібербезпеки та охоплює: розуміння організаційного контексту (GV.OC); політику управління ризиками кібербезпеки (GV.RM); ролі, обов’язки та повноваження (GV.RR); політику кібербезпеки (GV.PO); нагляд за виконанням політики (GV.OV); управління ризиками кібербезпеки ланцюга постачання (GV.SC).

6.3 Функція «Ідентифікація» (ID) забезпечує розуміння поточних ризиків кібербезпеки суб’єкта забезпечення кібербезпеки. Розуміння активів (даних, апаратного та програмного забезпечення, систем, об’єктів, послуг, персоналу), постачальників і пов’язаних із ними ризиків кібербезпеки дає суб’єктам змогу визначати пріоритетність своїх зусиль відповідно до політики управління ризиками та потреб місії, визначених у функції «Стратегічне керівництво». Функція охоплює визначення можливостей для вдосконалення політик, планів, процесів, процедур і практик суб’єкта, що підтримують управління ризиками кібербезпеки, для інформування діяльності за всіма шістьма функціями.

6.4 Функція «Захист» (PR) забезпечує застосування засобів захисту для управління ризиками кібербезпеки суб’єкта забезпечення кібербезпеки. Після

того як активи та ризики визначені й пріоритезовані за функцією «Ідентифікація», ця функція підтримує здатність суб’єкта забезпечення кібербезпеки захистити ці активи, щоб запобігти несприятливим подіям у сфері кібербезпеки або знизити їх ймовірність і наслідки. Функція охоплює: управління ідентичностями, автентифікацію та контроль доступу; підвищення обізнаності та навчання персоналу; безпеку даних; безпеку платформ (апаратного та програмного забезпечення й сервісів фізичних та віртуальних платформ); стійкість технологічної інфраструктури.

6.5 Функція «Виявлення» (DE) забезпечує своєчасне виявлення та аналіз аномалій, індикаторів компрометації й інших потенційно несприятливих подій, які можуть свідчити про те, що відбуваються кібератаки та кіберінциденти. Функція охоплює успішне реагування на кіберінциденти та відновлення після них.

6.6 Функція «Реагування» (RS) забезпечує здатність суб’єкта забезпечення кібербезпеки локалізувати наслідки кіберінцидентів та кібератак. Функція охоплює управління кіберінцидентами, їх аналіз, зменшення наслідків, звітування та комунікацію

6.7 Функція «Відновлення» (RC) забезпечує відновлення активів та операцій суб’єкта забезпечення кібербезпеки, що постраждали від кіберінциденту або кібератаки, з метою своєчасного повернення до стабільного функціонування та усунення наслідків кіберінцидентів і кібератак. Функція охоплює виконання плану відновлення після кіберінциденту та комунікацію під час відновлення.

6.8 Усі шість функцій мають здійснюватися одночасно, функції «Стратегічне керівництво», «Ідентифікація», «Захист» та «Виявлення» здійснюються безперервно, а функції «Реагування» та «Відновлення» мають бути готовими до виконання в будь-який час, у разі виникнення кіберінцидентів або кібератак. Функції «Стратегічне керівництво», «Ідентифікація» та «Захист» сприяють запобіганню кіберінцидентам і готовності до них, а функції

«Стратегічне керівництво», «Виявлення», «Реагування» та «Відновлення» допомагають суб’єкту забезпечення кібербезпеки виявляти кіберінциденти та кібератаки, реагувати на них і відновлюватися після них.

6.9 Шість функцій, їх категорії та підкатегорії застосовуються в межах сфери, визначеної суб’єктом забезпечення кібербезпеки.

6.10 Здійснення заходів з кіберзахисту за моделлю, наведеною в цьому розділі, сприяє зниженню ризиків кібербезпеки та підвищенню рівня кібербезпеки суб’єкта забезпечення кібербезпеки. Модель інтегрується із загальним управлінням ризиками суб’єкта та підтримує безперервне вдосконалення. Вона слугує основою для обміну інформацією між вищим керівництвом, яке зосереджується на пріоритетах і стратегічних напрямах функціонування суб’єкта, менеджерами, які управляють конкретними ризиками кібербезпеки, та фахівцями, які впроваджують і експлуатують технології.

7 КАТАЛОГ ЗАХОДІВ З КІБЕРЗАХИСТУ

7.1 Загальна характеристика Каталогу заходів з кіберзахисту

7.1.1 Каталог визначає необхідну взаємопов’язану сукупність організаційних та технічних заходів з кіберзахисту.

7.1.2 Каталог застосовують під час оцінювання поточного стану кіберзахисту, визначенні цільового стану кіберзахисту та розробленні плану кіберзахисту. Каталог наведено в додатку А.

7.2 Функції та категорії заходів з кіберзахисту

7.2.1 Заходи з кіберзахисту Каталогу згруповано за шістьма функціями моделі заходів з кіберзахисту, які поділяються на 22 категорії та 106 заходів. Перелік функцій та категорій заходів з кіберзахисту наведено в таблиці 1.

Таблиця 1 – Назви та ідентифікатори основних функцій і категорій

Функція й категорія	Ідентифікатор
СТРАТЕГІЧНЕ КЕРІВНИЦТВО (GV)	
Організаційний контекст	GV.OC
Політика управління ризиками кібербезпеки	GV.RM
Ролі, обов’язки та повноваження	GV.RR
Політика	GV.PO
Нагляд	GV.OV
Управління ризиками ланцюга постачання	GV.SC
ІДЕНТИФІКАЦІЯ (ID)	
Управління активами	ID.AM
Оцінювання ризиків кібербезпеки	ID.RA
Удосконалення	ID.IM
ЗАХИСТ (PR)	
Управління ідентифікацією, автентифікація та контроль доступу	PR.AA
Обізнаність і навчання з питань кіберзахисту	PR.AT
Безпека даних	PR.DS
Безпека платформ	PR.PS
Стійкість технологічної інфраструктури	PR.IR
ВИЯВЛЕННЯ (DE)	
Безперервний моніторинг	DE.CM
Аналіз несприятливих подій	DE.AE
РЕАГУВАННЯ (RS)	
Управління кіберінцидентами	RS.MA
Аналіз кіберінциденту	RS.AN
Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація	RS.CO
Мінімізація наслідків кіберінцидентів	RS.MI
ВІДНОВЛЕННЯ (RC)	
Виконання плану відновлення після кіберінциденту	RC.RP
Комунікація з відновлення після кіберінциденту	RC.CO

7.2.2 Розподіл заходів з кіберзахисту за функціями є таким: функція «Стратегічне керівництво» (GV) – 31 захід; функція «Ідентифікація» (ID) – 21 захід; функція «Захист» (PR) – 22 заходи; функція «Виявлення» (DE) –

11 заходів; функція «Реагування» (RS) – 13 заходів; функція «Відновлення» (RC) – 8 заходів.

7.3 План кіберзахисту

7.3.1 План кіберзахисту є інструментом, який допомагає суб'єкту оцінити достатність ресурсів, визначити пріоритетні заходи з кіберзахисту, забезпечити поінформованість про результати (з метою обізнаності всіх співробітників суб'єкта), враховуючи місії функціонування систем, очікування заінтересованих сторін, актуальні виклики та загрози, а також законодавчі вимоги у сферах кіберзахисту та захисту інформації.

7.3.2 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.

7.3.3 План кіберзахисту розробляють з урахуванням результатів управління ризиками кібербезпеки на основі Каталогу та описує поточний та/або цільовий стани кіберзахисту. Форма плану кіберзахисту наведена в додатку Б.

7.3.4 План кіберзахисту містить опис сфери застосування заходів з кіберзахисту, визначеної суб'єктом. Опис сфери застосування в плані кіберзахисту має охоплювати: перелік і межі підрозділів та основних операційних процесів суб'єкта, перелік систем, електронних комунікаційних мереж та ПЗ, на які поширюються заходи з кіберзахисту, а також географічне розташування систем, приміщень, 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.

7.3.5 Суб'єкти поетапно та послідовно досягають цільового стану кіберзахисту шляхом здійснення заходів з кіберзахисту, передбачених планом кіберзахисту. Під час розроблення та оновлення плану кіберзахисту

рекомендовано враховувати результати проведення аналізу ефективності реагування на кіберінциденти, кібератаки або кіберзагрози.

7.4 Рівні впровадження заходів з кіберзахисту

7.4.1 Суб’єкт, для формування поточного та цільового станів кіберзахисту, використовує рівні впровадження заходів з кіберзахисту. Рівні відображають практики суб’єкта з управління ризиками кібербезпеки як часткові (Рівень 1), ризико-орієнтовані (Рівень 2), повторювані (Рівень 3) та адаптивні (Рівень 4) і описують перехід від неформальних, ситуативних заходів реагування до підходів, які є гнучкими, заснованими на оцінці ризиків кібербезпеки та постійно вдосконалюються.

7.4.2 Рівень 1 – частковий. Застосування організаційної політики ризиків кібербезпеки управляється в індивідуальному порядку. Визначення пріоритетності є випадковим (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.

7.4.3 Рівень 2 – поінформований про ризик. Методи управління ризиками затверджуються керівництвом суб’єкта як окрема організаційна політика. Існує усвідомлення ризиків кібербезпеки на організаційному рівні, але загальноорганізаційного підходу до управління ризиками кібербезпеки не встановлено. Оцінка ризиків кібербезпеки організаційних та зовнішніх активів здійснюється, але зазвичай не є повторюваною або періодичною.

7.4.4 Рівень 3 – повторюваний. Практика управління ризиками офіційно затверджена керівництвом суб’єкта та визначена як політика. Політики, процеси та процедури з урахуванням ризиків визначаються, впроваджуються за призначенням і переглядаються. Існує загальноорганізаційний підхід до управління ризиками кібербезпеки: інформація про кібербезпеку регулярно

поширюється, персонал суб’єкта володіє знаннями та навичками для виконання своїх ролей і обов’язків.

7.4.5 Рівень 4 – адаптивний. Загальноорганізаційний підхід до управління ризиками кібербезпеки, який використовує політику, процеси та процедури з урахуванням ризиків. Процес управління ризиками кібербезпеки є частиною організаційної культури суб’єкта. Суб’єкт адаптує свої практики кібербезпеки на основі попередньої та поточної діяльності з кіберзахисту, включаючи отримані дані та прогнозні показники, і своєчасно й ефективно реагує на складні кіберзагрози, що розвиваються.

7.4.6 Під час оцінювання ступеня відповідності документації та повноти впровадження заходів з кіберзахисту додатково застосовується Рівень 0 – «відсутній», за якого документальне забезпечення заходу відсутнє, процедури не описані та не затверджені керівництвом суб’єкта, захід не впроваджено, а дії щодо його реалізації не проводяться.

Примітка. Рівні впровадження заходів з кіберзахисту побудовано на основі орієнтовних описів ярусів (CSF Tiers), наведених у додатку B NIST CSF 2.0 [11], з такими адаптаціями: додано Рівень 0 «відсутній» та передбачено застосування рівнів до заходів Каталогу. Можливість адаптації описів ярусів передбачено NIST SP 1302 [12]. Каталог розроблено з урахуванням NIST CSF 2.0 [11].

ДОДАТОК А
(обов’язковий)
КАТАЛОГ ЗАХОДІВ З КІБЕРЗАХИСТУ

А.1 GV (СТРАТЕГІЧНЕ КЕРІВНИЦТВО): визначення стратегій, політик, ролей та обов’язків, проведення моніторингу щодо управління ризиками кібербезпеки.

А.1.1 GV.OC (Організаційний контекст): розуміння обставин, у яких суб'єкт ухвалює рішення щодо управління ризиками кібербезпеки, а саме місії, очікувань заінтересованих сторін, залежностей, а також законодавчих, нормативних та договірних вимог.

А.1.1.1 GV.OC-01: забезпечити розуміння місії суб’єкта та її врахування під час управління ризиками кібербезпеки.

А.1.1.2 GV.OC-02: визначити внутрішніх та зовнішніх заінтересованих сторін, забезпечити розуміння та врахування їхніх потреб і очікувань щодо управління ризиками.

А.1.1.3 GV.OC-03: визначити та забезпечити виконання співробітниками чинних законодавчих та інших нормативно-правових актів, нормативних документів та договірних вимог, а також вимог суб’єкта щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав і свобод.

А.1.1.4 GV.OC-04: визначити та довести до відома співробітників ключові цілі, критичні послуги та спроможності суб’єкта.

А.1.1.5 GV.OC-05: визначити наслідки, спроможності та послуги, від яких залежить діяльність суб’єкта, забезпечити їх усвідомлення співробітниками.

А.1.2 GV.RM (Політика управління ризиками кібербезпеки): визначення, документування та доведення до відома заінтересованих сторін політики управління ризиками кібербезпеки, яка встановлює мету, сферу діяльності, ролі, відповідальність, зобов’язання керівництва, координацію між

структурними підрозділами та відповідність; визначає пріоритети, обмеження та рівні ризику кібербезпеки, втрати, яких суб’єкт може зазнати, з урахуванням факторів ризику для кожного з видів діяльності, для підтримки рішень щодо операційних ризиків; а також процедури, що сприяють впровадженню цієї політики. Політика відповідає чинним законам, нормативно-правовим актам, політикам, стандартам і вказівкам. Для управління розробленням, документуванням і розповсюдженням політики та процедур призначається відповідальна посадова особа. Політика та процедури переглядаються й оновлюються з визначеною суб’єктом періодичністю та за настання визначених суб’єктом подій.

A.1.2.1 GV.RM-01: визначити та узгодити із заінтересованими сторонами суб’єкта цілі управління ризиками кібербезпеки.

A.1.2.2 GV.RM-02: визначити допустимий рівень ризику кібербезпеки, який суб’єкт може прийняти, довести до відома всіх співробітників та заінтересованих сторін і підтримувати таку інформацію в актуальному стані.

A.1.2.3 GV.RM-03: додати до загальних процесів управління ризиками суб’єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей.

A.1.2.4 GV.RM-04: визначити та довести до відома співробітників стратегічні напрями, які описують відповідні варіанти реагування на ризики кібербезпеки.

A.1.2.5 GV.RM-05: визначити та довести до відома співробітників способи обміну інформацією всередині суб’єкта щодо ризиків кібербезпеки, включаючи ризики, які несуть постачальники товарів, робіт, послуг та інші треті сторони.

A.1.2.6 GV.RM-06: визначити та довести до відома співробітників стандартизовані методи розрахунку, документування, ідентифікації та визначення пріоритетності ризиків кібербезпеки.

A.1.2.7 GV.RM-07: визначити, охарактеризувати та забезпечувати обговорення зі співробітниками суб’єкта стратегічних можливостей щодо управління ризиками кібербезпеки.

А.1.3 GV.RR (Ролі, обов’язки та повноваження): визначення та доведення до відома співробітників суб’єкта ролей щодо кібербезпеки, відповідальності, уповноважених суб’єкта для інформування, оцінки ефективності та постійного вдосконалення.

А.1.3.1 GV.RR-01: визначити із числа керівництва суб’єкта посадову особу, яка звітує про ризики кібербезпеки та підтримання культури поведінки щодо усвідомлення ризиків та етики, її постійне вдосконалення, а також відповідає за них.

А.1.3.2 GV.RR-02: встановити, забезпечити комунікацію, розуміння та дотримання ролей та повноважень щодо управління ризиками.

А.1.3.3 GV.RR-03: визначити необхідні ресурси відповідно до політики управління ризиками кібербезпеки, ролей, відповідальності та політик.

А.1.3.4 GV.RR-04: включити питання кібербезпеки в практики управління персоналом.

А.1.4 GV.PO (Політика): затвердження та сприяння реалізації політики кібербезпеки суб’єкта.

А.1.4.1 GV.PO-01: розробити та довести до відома співробітників суб’єкта політику управління ризиками кібербезпеки, яка визначена з урахуванням структури суб’єкта, стратегії кібербезпеки та пріоритетів.

А.1.4.2 GV.PO-02: забезпечити періодичний перегляд, оновлення та виконання політики управління ризиками кібербезпеки з урахуванням змін нормативних вимог, стандартів, загроз, технологій та місії суб’єкта.

А.1.5 GV.OV (Нагляд): результати комплексної діяльності з управління ризиками кібербезпеки використовуються для інформування, покращення ефективності та коригування політики управління ризиками.

А.1.5.1 GV.OV-01: забезпечити врахування результатів політики управління ризиками кібербезпеки для вдосконалення та коригування її напрямів.

А.1.5.2 GV.OV-02: забезпечити перегляд і коригування політики управління ризиками кібербезпеки для врахування вимог суб’єкта та можливих ризиків.

А.1.5.3 GV.OV-03: забезпечити оцінювання продуктивності управління ризиками кібербезпеки для перегляду, внесення необхідних коригувань відповідно до поточних потреб.

А.1.6 GV.SC (Управління ризиками ланцюга постачання): ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки, пов’язаних з ланцюгами постачання, та їх покращення постачальниками товарів, робіт, послуг суб’єкта.

А.1.6.1 GV.SC-01: розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки, пов’язаними з ланцюгами постачання, погодити їх із заінтересованими сторонами суб’єкта.

А.1.6.2 GV.SC-02: розробити, довести, здійснювати внутрішню та зовнішню координацію ролей з кібербезпеки під час їх виконання постачальниками товарів, робіт, послуг, користувачами та партнерами суб’єкта.

А.1.6.3 GV.SC-03: забезпечити інтеграцію управління ризиками ланцюга постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки суб’єкта, оцінку ризиків та їх вдосконалення.

А.1.6.4 GV.SC-04: визначити та пріоритизувати постачальників товарів, робіт, послуг за ступенем критичності.

А.1.6.5 GV.SC-05: встановити вимоги, пов’язані з ризиками кібербезпеки у ланцюгах постачання, та впровадити їх у договори/контракти або інші типи договорів з постачальниками товарів, робіт, послуг та відповідними третіми сторонами.

А.1.6.6 GV.SC-06: забезпечити планування та комплексну перевірку постачальників товарів, робіт, послуг або інших третіх сторін для зменшення ризиків кібербезпеки перед початком договірних відносин з ними.

А.1.6.7 GV.SC-07: визначити ризики кібербезпеки, пов’язані з постачальником товарів, робіт, послуг, його продукцією та послугами, які він надає, з іншими третіми сторонами, врахувати їх, зареєструвати, пріоритизувати та забезпечити реагування на них і контроль протягом всієї співпраці.

А.1.6.8 GV.SC-08: забезпечити залучення відповідних постачальників товарів, робіт, послуг та інших третіх сторін до діяльності щодо планування, реагування на кіберінциденти, кібератаки, кіберзагрози та відновлення після них.

А.1.6.9 GV.SC-09: інтегрувати практичні заходи щодо забезпечення безпеки ланцюга постачання в програми суб’єкта щодо кібербезпеки та управління ризиками кібербезпеки, контролювати їх ефективність протягом всього життєвого циклу користування продуктами та послугами, які суб’єкт отримує від постачальника товарів, робіт, послуг чи інших третіх сторін.

А.1.6.10 GV.SC-10: передбачити в планах управління ризиками кібербезпеки, пов’язаними з ланцюгами постачання, порядок дій, які необхідно виконати після завершення (припинення) партнерських відносин або договору про надання послуг.

А.2 ID (ІДЕНТИФІКАЦІЯ): забезпечується розуміння поточних ризиків кібербезпеки.

А.2.1 ID.AM (Управління активами): ідентифікація активів (у тому числі даних, ПЗ, систем, засобів, послуг, осіб), які необхідні суб’єкту для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі суб’єкта та політики управління ризиками кібербезпеки.

А.2.1.1 ID.AM-01: забезпечити періодичне проведення інвентаризації обладнання, яким керує суб’єкт.

А.2.1.2 ID.AM-02: забезпечити періодичне проведення інвентаризації ПЗ, послуг і систем, якими керує суб’єкт.

А.2.1.3 ID.AM-03: забезпечити підтримку використання авторизованих мережевих з’єднань та визначити внутрішні й зовнішні мережеві потоки.

А.2.1.4 ID.AM-04: забезпечити періодичне проведення інвентаризації послуг, що надаються постачальниками товарів, робіт, послуг.

А.2.1.5 ID.AM-05: провести розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта.

А.2.1.6 ID.AM-07: забезпечити інвентаризацію даних і пов'язаних з ними метаданих відповідно до визначених типів даних.

А.2.1.7 ID.AM-08: забезпечити управління системами, АЗ та ПЗ, послугами та даними протягом усього їх життєвого циклу.

А.2.2 ID.RA (Оцінювання ризиків кібербезпеки): усвідомлення суб'єктом ризиків кібербезпеки для нього, його активів і ризиків, які пов'язані з людським фактором.

А.2.2.1 ID.RA-01: ідентифікувати, підтверджувати та вести записи/журналювати вразливі місця активів.

А.2.2.2 ID.RA-02: організувати отримання інформації про кіберзагрози та вразливості з платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з репозитарію інформації про кіберінциденти, інших офіційних джерел.

А.2.2.3 ID.RA-03: визначити та задокументувати внутрішні та зовнішні кіберзагрози.

А.2.2.4 ID.RA-04: визначити та задокументувати потенційні наслідки та вірогідні загрози, пов'язані з експлуатацією вразливостей.

А.2.2.5 ID.RA-05: забезпечити використання інформації про вірогідні кіберзагрози, вразливості та можливі наслідки від їх настання для розуміння невід'ємного ризику кібербезпеки та інформування про пріоритетність реагування на ризики.

А.2.2.6 ID.RA-06: визначити заходи реагування на ризики кібербезпеки та встановити їх пріоритетність, забезпечити їх відслідковування та комунікацію щодо них.

А.2.2.7 ID.RA-07: забезпечити управління, оцінювання на предмет ризику кібербезпеки, реєстрацію та відстеження змін та винятків до затвердженої документації.

А.2.2.8 ID.RA-08: визначити процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості.

А.2.2.9 ID.RA-09: проводити перевірку автентичності й цілісності обладнання та ПЗ перед його придбанням і використанням.

А.2.2.10 ID.RA-10: забезпечити проведення оцінювання постачальників товарів, робіт, послуг перед придбанням у них критично важливих для суб'єкта товарів, робіт і послуг.

А.2.3 ID.IM (Удосконалення): удосконалення організаційних процесів, процедур і діяльності з управління ризиками кібербезпеки, які визначено в класах заходів кіберзахисту.

А.2.3.1 ID.IM-01: визначити напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту.

А.2.3.2 ID.IM-02: визначити напрями удосконалення за результатами тестування безпеки та навчальних вправ, включаючи їх виконання у взаємодії з постачальниками товарів, робіт, послуг та відповідними третіми сторонами.

А.2.3.3 ID.IM-03: визначати покращення з управління ризиками кібербезпеки під час виконання операційних процесів, процедур і дій.

А.2.3.4 ID.IM-04: розробити, затвердити, довести до відома співробітників, переглядати й удосконалювати план реагування на кіберінциденти, кібератаки або кіберзагрози відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози [6], внутрішні політики кібербезпеки, план кіберзахисту та інші регламентуючі документи, які впливають на діяльність суб'єкта.

А.3 PR (ЗАХИСТ): розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталого та надійного функціонування об'єктів кіберзахисту, удосконалення систем реагування на

кіберінциденти, кібератаки, кіберзагрози з урахуванням необхідності забезпечення пропорційності можливостей таких систем реальним і потенційним ризикам кібербезпеки.

А.3.1 PR.AA (Управління ідентифікацією, автентифікація та контроль доступу): доступ до фізичних і логічних активів надається лише авторизованим користувачам, службам та обладнанню й управляється відповідно до оціненого ризику неавторизованого доступу.

А.3.1.1 PR.AA-01: забезпечити на рівні суб'єкта керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

А.3.1.2 PR.AA-02: забезпечити перевірку автентичності особи (identity proofing) та прив'язку облікових записів до засобів автентифікації на основі контексту взаємодії.

А.3.1.3 PR.AA-03: забезпечити автентифікацію користувачів, служб та апаратного забезпечення.

А.3.1.4 PR.AA-04: забезпечити захист, передавання та перевірку електронних тверджень ідентичності.

А.3.1.5 PR.AA-05: визначити в політиці, дотримуючись принципів найменших привілеїв і розподілу обов'язків, дозволи доступу, повноваження та авторизації, керувати ними, застосовувати та переглядати.

А.3.1.6 PR.AA-06: здійснювати управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки.

А.3.2 PR.AT (Обізнаність і навчання з питань кіберзахисту): суб'єкт здійснює систематичне проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо проводять заходи з кіберзахисту.

А.3.2.1 PR.AT-01: систематично проводити інструктажі та тренінги з кібергігієни, а також забезпечити обізнаність і навченість співробітників (підвищення їх кваліфікації) таким чином, щоб вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки.

А.3.2.2 PR.AT-02: забезпечити обізнаність та навченість співробітників (підвищення їх кваліфікації), які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту таким чином, щоб вони мали знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки.

А.3.3 PR.DS (Безпека даних): управління даними здійснюється відповідно до політики ризиків кібербезпеки суб'єкта для захисту конфіденційності, цілісності та доступності інформації.

А.3.3.1 PR.DS-01: забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб'єкта.

А.3.3.2 PR.DS-02: забезпечити конфіденційність, цілісність і доступність даних, що передаються.

А.3.3.3 PR.DS-10: забезпечити конфіденційність, цілісність і доступність даних, що використовуються: до яких є доступ; які обробляються та регулярно оновлюються застосунками, користувачами або пристроями суб'єкта.

А.3.3.4 PR.DS-11: забезпечити створення, захист, підтримку та тестування резервних копій даних.

А.3.4 PR.PS (Безпека платформ): керування АЗ і ПЗ (наприклад, мікропрограми, операційні системи, застосунки), службами фізичних і віртуальних платформ відповідно до політики ризиків кібербезпеки суб'єкта для захисту їх конфіденційності, цілісності та доступності.

А.3.4.1 PR.PS-01: встановити та застосовувати методи керування конфігурацією.

А.3.4.2 PR.PS-02: забезпечити належне обслуговування, заміну та видалення ПЗ відповідно до ризику кібербезпеки.

А.3.4.3 PR.PS-03: забезпечити обслуговування, заміну та видалення обладнання відповідно до ризику кібербезпеки.

А.3.4.4 PR.PS-04: створити записи журналів подій та забезпечити доступність записів журналів подій для постійного моніторингу.

А.3.4.5 PR.PS-05: заборонити встановлення та виконання несанкціонованого ПЗ.

А.3.4.6 PR.PS-06: інтегрувати практики безпечної розробки ПЗ та контролювати їх виконання протягом життєвого циклу розробленого ПЗ.

А.3.5 PR.IR (Стійкість технологічної інфраструктури): керування архітектурою безпеки відповідно до політики ризиків кібербезпеки суб'єкта для захисту конфіденційності, цілісності та доступності активів, а також забезпечення стійкості суб'єкта.

А.3.5.1 PR.IR-01: забезпечити захист мережі та середовища від неавторизованого логічного доступу та використання.

А.3.5.2 PR.IR-02: забезпечити захист технологічних активів від загроз навколишнього середовища.

А.3.5.3 PR.IR-03: реалізувати механізми для досягнення вимог стійкості в нормальних і несприятливих ситуаціях.

А.3.5.4 PR.IR-04: забезпечити управління пропорційністю та адекватністю застосування ресурсів для їх доступності.

А.4 DE (ВИЯВЛЕННЯ): проведення ідентифікації, збору та обробки кіберінцидентів, кібератак та кіберзагроз.

А.4.1 DE.CM (Безперервний моніторинг): моніторинг активів з метою виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій у кіберпросторі.

А.4.1.1 DE.CM-01: проводити постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій.

А.4.1.2 DE.CM-02: проводити постійний моніторинг фізичного середовища для виявлення потенційно несприятливих подій.

А.4.1.3 DE.CM-03: проводити постійний моніторинг діяльності співробітників і використання ними технологій для виявлення потенційно несприятливих подій.

А.4.1.4 DE.CM-06: проводити постійний моніторинг діяльності й послуг зовнішнього постачальника товарів, робіт, послуг для виявлення потенційно несприятливих подій.

А.4.1.5 DE.CM-09: проводити постійний моніторинг використання комп'ютерного обладнання та ПЗ, середовища їх виконання та даних для виявлення потенційно несприятливих подій.

А.4.2 DE.AE (Аналіз несприятливих подій): аналіз аномалій, індикаторів компрометації та інших потенційно несприятливих подій, щоб їх охарактеризувати та виявити кіберінциденти або кібератаки.

А.4.2.1 DE.AE-02: впровадити періодичне проведення аналізу потенційно несприятливих подій для кращого розуміння пов'язаних подій.

А.4.2.2 DE.AE-03: впровадити періодичне проведення пошуку та зіставлення інформації з кількох джерел.

А.4.2.3 DE.AE-04: забезпечити усвідомлення очікуваного впливу й масштабу несприятливих подій.

А.4.2.4 DE.AE-06: забезпечити передавання інформації про несприятливі події до уповноважених суб'єктів для використання відповідного інструментарію.

А.4.2.5 DE.AE-07: забезпечити збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації.

А.4.2.6 DE.AE-08: запровадити належну ідентифікацію кіберінцидентів та кібератак за визначеними характеристиками.

А.5 RS (РЕАГУВАННЯ): запобігання кіберінцидентам, кібератакам та кіберзагрозам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення.

А.5.1 RS.MA (Управління кіберінцидентами): керування процесом реагуванням на виявлені кіберінциденти, кібератаки та кіберзагрози.

A.5.1.1 RS.MA-01: упровадити виконання плану реагування на кіберінциденти, кібератаки або кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту.

A.5.1.2 RS.MA-02: упровадити сортування звітів про кіберінциденти після їх підтвердження.

A.5.1.3 RS.MA-03: упровадити таксономію та пріоритизацію кіберінцидентів.

A.5.1.4 RS.MA-04: упровадити інформування та підвищення рівнів критичності кіберінцидентів (за потреби).

A.5.1.5 RS.MA-05: упровадити застосування критеріїв для ініціювання відновлення після кіберінциденту.

A.5.2 RS.AN (Аналіз кіберінциденту): проведення розслідувань/перевірок для забезпечення ефективного реагування на кіберінциденти, кібератаки та кіберзагрози, експертизи кіберінцидентів, а також заходів з відновлення після них.

A.5.2.1 RS.AN-03: запровадити проведення аналізу для встановлення того, що відбулося під час кіберінциденту та які джерела виникнення кіберінциденту.

A.5.2.2 RS.AN-06: запровадити здійснення запису дій, які виконуються під час розслідування/перевірки кіберінциденту, та забезпечити цілісність і збереження таких записів.

A.5.2.3 RS.AN-07: запровадити здійснення збору та забезпечити цілісність і збереження даних про кіберінциденти та метаданих.

A.5.2.4 RS.AN-08: запровадити оцінювання масштабу кіберінциденту або кібератаки та документально його підтверджувати.

A.5.3 RS.CO (Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація): координація заходів реагування з внутрішніми та зовнішніми заінтересованими сторонами відповідно до законів, нормативно-правових актів та нормативних документів або політик.

А.5.3.1 RS.CO-02: запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про кіберінциденти, кібератаки та кіберзагрози.

А.5.3.2 RS.CO-03: запровадити надання інформації визначеним внутрішнім і зовнішнім заінтересованим сторонам.

А.5.4 RS.MI (Мінімізація наслідків кіберінцидентів): виконання дій щодо запобігання розширенню подій та усунення їх наслідків.

А.5.4.1 RS.MI-01: забезпечити локалізацію кіберінцидентів.

А.5.4.2 RS.MI-02: забезпечити усунення першопричин кіберінцидентів.

А.6 RC (ВІДНОВЛЕННЯ): поновлення штатного режиму функціонування об’єктів кіберзахисту після кіберінциденту, кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування/перевірки кібератаки та кіберінциденту.

А.6.1 RC.RP (Виконання плану відновлення після кіберінциденту): проведення відновлювальних заходів для забезпечення доступності систем і служб, які постраждали від кіберінцидентів.

А.6.1.1 RC.RP-01: забезпечити виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення одразу після їх ініціалізації в ході реагування на кіберінциденти, кібератаки та кіберзагрози.

А.6.1.2 RC.RP-02: забезпечити відбір, визначення обсягу, пріоритетність та виконання заходів з відновлення.

А.6.1.3 RC.RP-03: переконатися у цілісності резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення.

А.6.1.4 RC.RP-04: критичні функції діяльності та система управління кіберризиками переглядаються для формування режиму роботи після кіберінцидентів і кібератак.

А.6.1.5 RC.RP-05: переконатися в цілісності відновлених активів, відновленні систем та служб і підтвердити їх робочий стан.

А.6.1.6 RC.RP-06: задекларувати завершення відновлення після кіберінциденту, кібератаки й підтвердження критеріїв та пов’язаної з кіберінцидентом документації.

А.6.2 RC.CO (Комунікація з відновлення після кіберінциденту): координація заходів щодо відновлення з внутрішніми та зовнішніми сторонами.

А.6.2.1 RC.CO-03: забезпечити інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей.

А.6.2.2 RC.CO-04: запровадити інформування суспільства та/або заінтересованих сторін 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 [7].

СТД-04-002-2026-В

ДОДАТОК Б

(обов’язковий)

ФОРМА ПЛАНУ КІБЕРЗАХИСТУ

Гриф обмеження доступу

(зазначається після заповнення, за необхідності)

ЗАТВЕРДЖЕНО

_____

(найменування посади керівника суб’єкта або особи, яка його заміщує)

_____

(підпис) (власне ім’я та прізвище)

МП

(за наявності)

___.___.20__ р.

ПЛАН КІБЕРЗАХИСТУ

_____

(найменування суб’єкта)

І. Загальні відомості

1. Відомості про орган державної влади, орган місцевого самоврядування, підприємство, установу та організацію незалежно від форм власності, 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 суб’єкти господарювання, які залучені до забезпечення функціонування систем суб’єкта.

_____
_____
_____

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

_____
_____
_____

3. Опис сфери застосування заходів з кіберзахисту.

_____
_____
_____

ІІ. Описи поточного та/або цільового стану кіберзахисту

№ з/п	Ідентифікатор	Заходи з кіберзахисту	Опис поточного стану кіберзахисту	Опис цільового стану кіберзахисту (конкретні заходи для досягнення цільового стану)	Відповідальна особа	Запланований термін виконання заходів
Назва функції						
1						
2						
3						
…						
N						

Посадова особа, відповідальна за заповнення плану:

(посада) (підпис, власне ім’я, прізвище)

___.____.20__ р.

БІБЛІОГРАФІЯ

1 Закон України «Про основні засади забезпечення кібербезпеки України»;

2 Закон України «Про захист інформації в інформаційно-комунікаційних системах»;

3 Закон України «Про критичну інфраструктуру»;

4 Загальні вимоги з кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518 (в редакції постанови Кабінету Міністрів України від 13.11.2025 № 1470);

5 Положення про організаційно-технічну модель кіберзахисту, затверджене постановою Кабінету Міністрів України від 29.12.2021 № 1426;

6 Національний план реагування на кіберінциденти, кібератаки та кіберзагрози, затверджений постановою Кабінету Міністрів України від 26.11.2025 № 1533;

7 Порядок публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх наслідків, затверджений постановою Кабінету Міністрів України від 26.11.2025 № 1533;

8 ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT);

9 ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT);

10 ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT);

11 NIST CSF 2.0. National Institute of Standards and Technology, USA, 2024;

12 NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers. NIST SP 1302, National Institute of Standards and Technology, 2024

СТД-04-002-2026-В

Коди згідно з КСД 001: 04.01, 04.02;

НК 004: 35.030

Ключові слова: кіберзахист, заходи з кіберзахисту, каталог заходів з кіберзахисту, базові заходи з кіберзахисту, план кіберзахисту, модель заходів з кіберзахисту, оцінювання стану кіберзахисту, рівень впровадження, кібербезпека, ризик кібербезпеки.

Начальник ДержНДІ
технологій кібербезпеки Володимир ПАВЛІКОВ

Начальник 8 наукового центру
галузевої стандартизації
ДержНДІ технологій кібербезпеки Роман ЦИРЕНЬ

Заступник начальника центру –
начальник 1 наукового відділу
8 наукового центру галузевої
стандартизації ДержНДІ
технологій кібербезпеки Тетяна МАСЛЕННИКОВА

Молодший науковий співробітник
за рахунок посади старшого
наукового співробітника
1 наукового відділу
8 наукового центру
галузевої стандартизації
ДержНДІ технологій кібербезпеки Олексій ПОНОМАРЬОВ

Старший юрисконсульт
юридичного відділу
ДержНДІ технологій кібербезпеки _____