Прим. № __

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

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

СТД-02-002-2026-В

ЗАХИСТ ІНФОРМАЦІЇ. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. ПОРЯДОК ВИКОНАННЯ ВИМОГ З БЕЗПЕКИ В ІНФОРМАЦІЙНИХ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ, ТЕХНОЛОГІЧНИХ СИСТЕМАХ

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

СТД-02-002-2026-В

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: **І. Навроцький**, керівник розробки; **С. Лисенко**; **М. Рибка**; **Р. Сагайдак**; **О. Дробко**; **М. Кожін**; **Ю. Россошанський**; **О. Пономарьов**.

2 ПОГОДЖЕНО: Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (лист від 14.10.2026 № 04/04/01-27718/2026/ВН).

3 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказом Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від 23.10.2026 № 130, з 30.10.2026.

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 6
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ 8
4 ПОЗНАКИ ТА СКОРОЧЕННЯ 13
5 МОДЕЛЬ ПОРЯДКУ ВПРОВАДЖЕННЯ ВИМОГ З БЕЗПЕКИ 13
6 ЗАГАЛЬНІ ПОЛОЖЕННЯ 15
6.1 Взаємодія між рівнями управління інформаційної безпеки Організації 15
6.2 Типи заходів захисту та особливості їх застосування 16
6.3 Документування заходів захисту 20
6.4 Етапи впровадження заходів захисту 23
7 ВИЗНАЧЕННЯ ЕТАПІВ ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ 28
7.1 Етап експертної оцінки інформації, вибору БПБ або ГПБ 28
7.2 Етап оцінки ризиків 28
7.3 Етап розроблення ЦПБ 30
7.4 Етап розробки та впровадження заходів захисту 30
7.5 Етап оцінювання дотримання вимог ЦПБ 31
7.6 Етап включення системи до Переліку авторизованих систем з безпеки 33
7.7 Етап постійного моніторингу безпеки 34
8 ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ НА РІЗНИХ ЕТАПАХ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМ 35
ДОДАТОК А (обов’язковий) Етапи виконання вимог з безпеки в системі у рамках до життєвого циклу засобу інформатизації 36
Бібліографія 38

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Цей стандарт визначає основи організації та порядок виконання вимог з безпеки в інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних системах (далі – системи).

1.2 Цей стандарт визначає загальну систему дій щодо проєктування, впровадження, підтримки та постійного вдосконалення заходів захисту як частини загальної системи управління організацією, яка ґрунтується на підході управління ризиками безпеки та яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення безпеки інформації у поєднанні зі стратегічними, оперативними та бюджетними процесами планування в організації відповідно до міжнародних стандартів системи менеджменту інформаційної безпеки.

1.3 Вимоги цього стандарту поширюються на системи, що розгорнуті та експлуатуються органами державної влади, органами місцевого самоврядування, а також підприємствами, установами та організаціями всіх форм власності (далі – Організації).

Цей стандарт застосовний для вибору та реалізації заходів захисту в системах, спрямованих на забезпечення:

– конфіденційності інформації (виключення неавторизованого доступу, копіювання, надання та розповсюдження);

– цілісності інформації (виключення неавторизованого знищення та модифікації);

– доступності інформації (виключення неавторизованого блокування інформації та системи);

– спостережності системи (властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій

користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності за певні дії).

Цей стандарт застосовується для вибору та реалізації заходів захисту в системах, спрямованих на забезпечення захисту персональних даних.

Досягнення належного рівня безпеки в Організації вимагає:

– чітко визначених та сформульованих вимог з безпеки для систем і Організації;

– суворого планування безпеки, а також управління життєвим циклом системи та інформації;

– використання надійних компонентів системи, сучасних апаратних засобів та програмного забезпечення для захисту інформації;

– застосування системного підходу до забезпечення безпеки;

– ефективного процесу інтеграції засобів захисту в системи;

– застосування чітко задокументованих та інтегрованих у процеси практик безпеки;

– постійного моніторингу систем для визначення поточного стану ефективності заходів захисту, необхідних змін в системах і робочих середовищах, а також стану безпеки загалом.

Організації мають оцінювати ризики безпеки для своїх функцій (процесів) і активів, фізичних осіб, інших організацій, які виникають в результаті виконання їхніх завдань і функцій (процесів). Оцінювання ризиків безпеки потребує глибокого розуміння загроз безпеки, реалізація яких ґрунтується на вразливостях систем і Організації загалом, імовірних та можливих негативних наслідків, що виникають у разі порушення конфіденційності, цілісності, доступності та інших властивостей безпеки. Вимоги з безпеки повинні бути сформульовані з урахуванням стратегії управління ризиками Організації з увагою на особливості, витрати, порядок і ефективність впровадження заходів, пов’язаних з проєктуванням, розробкою, придбанням, розгортанням, експлуатацією та підтримкою систем.

Результати оцінювань ризиків мають бути джерелом інформації для процесу налаштування та посилення базового профілю безпеки. Процес вибору призводить до формування узгодженого набору заходів захисту – цільового профілю безпеки, що відповідає конкретним потребам Організації. Цей процес має бути гнучким для того, щоб Організації могли ефективно пристосовуватися до складних і мінливих умов функціонування систем та робочого середовища.

Цей стандарт призначений для суб'єктів/осіб, пов'язаних з розробленням, розвитком, впровадженням, оцінюванням, експлуатацією, обслуговуванням та розпорядженням системи, зокрема:

– суб'єктів інформаційних відносин (власників або розпорядників та користувачів системи), діяльність яких пов'язана з обробкою інформації, що підлягає захисту;

– осіб, діяльність яких пов'язана з використанням системи в Організації, забезпеченням захисту інформації, наглядом або управлінням (наприклад, керівники процесу управління ризиками, уповноважені посадові особи, співробітники підрозділів, що експлуатують систему, адміністратори безпеки, співробітники підрозділу кіберзахисту, відповідальні за захист інформації тощо);

– осіб, відповідальних за розробку та проєктування заходів захисту, які можуть залучатися власником або розпорядником системи на договірних умовах;

– постачальників послуг з безпеки та засобів захисту;

– осіб, відповідальних за проведення оцінювання дотримання вимог цільового профілю безпеки;

– осіб, відповідальних за проведення авторизації з безпеки системи.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такі нормативні документи:

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT);

НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;

НД ТЗІ 3.6-025-24 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;

NIST Special Publication 800-30. Rev.1. Guide for Conducting Risk Assessments, 2012;

NIST Special Publication 800-37. Rev.2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018;

NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View, 2011;

NIST Special Publication 800-53. Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020;

NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems, 2011;

NIST Special Publication 800-160 Vol. 1 Rev. 1. Engineering Trustworthy Secure Systems, 2022;

NIST Special Publication 800-160 Vol. 2 Rev. 1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, 2021.

Примітка. У разі заміни нормативного документу, на який наведено посилання, слід застосовувати новий нормативний документ. У разі скасування нормативного документу, на який наведено посилання, слід застосовувати останню чинну на момент застосування редакцію нормативного документу. 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 вжито терміни, наведені в ДСТУ 2226 [6], ДСТУ 3396.2 [7].

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

3.1 авторизація з безпеки

Рішення щодо можливості функціонування (експлуатації) відповідної інформаційної, електронної комунікаційної, інформаційно-комунікаційної, технологічної системи з урахуванням її відповідності вимогам законодавчих та інших нормативно-правових актів, стандартів і нормативних документів у сферах технічного та криптографічного захисту інформації, кіберзахисту, що приймається у встановленому законодавством порядку

3.2 базовий профіль безпеки системи (БПБ)

Мінімальні вимоги з безпеки інформації та взаємопов’язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації, що обробляється у системі (відкрита інформація чи інформація з обмеженим доступом), або функціонального призначення такої системи

3.3 вимога з безпеки

Твердження, яке виражає конкретну потребу в безпеці інформації (активу), включно із супутніми обмеженнями та умовами. Вимога з безпеки, що висувається до інформації, системи чи Організації, може походити з різних джерел, серед яких, наприклад, закони, розпорядчі документи, нормативно-правові акти, нормативні документи, державні, міжнародні та інші стандарти, накази, директиви, правила (політики), положення, а також потреби конкретної Організації

3.4 вимоги захисту персональних даних

Вимоги, спрямовані на захист особистого життя фізичних осіб, що пов’язані зі створенням, збиранням, використанням, обробкою, зберіганням, поширенням, розкриттям чи видаленням персональних даних

3.5 галузевий профіль безпеки системи (ГПБ)

Взаємопов’язана сукупність заходів щодо захисту інформації, визначених для системи органом державної влади (Організацією) у межах своїх повноважень у відповідній сфері або галузі з урахуванням мінімальних вимог щодо таких заходів із захисту (базового профілю), відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі, а також надання відповідних рекомендацій

3.6 гібридний захід захисту

Захід захисту, що реалізується для системи, частково як загальний захід, а частково як специфічний

3.7 довірений ланцюг постачання

Певний рівень довіри під час взаємодії в ланцюгу постачання, такий, що кожен учасник відносин «споживач-постачальник» забезпечує належний захист інформації, систем і послуг

3.8 додавання заходу захисту

Включення до профілю безпеки заходів захисту, які не передбачені базовим профілем безпеки системи для виконання вимог законодавства до конкретної системи, її функціонального призначення та оцінки ризиків Організації

3.9 електронна комунікаційна система

Сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб

Примітка: Далі по тексту документа для всіх систем буде використовуватися термін система

3.10 життєвий цикл інформації

Етапи, через які проходить інформація, зокрема: створення або збір, обробка, поширення, використання і зберігання, включно зі знищенням і видаленням

3.11 загальний захід захисту

Захід захисту, який успадковується (використовується) декількома системами

3.12 заходи захисту інформації

Заходи або контрзаходи, передбачені для впровадження в системі або Організації для захисту конфіденційності, цілісності та доступності інформації, що знаходиться (циркулює) в системі

3.13 зовнішні системні служби

Системна послуга, яка реалізується поза межами системи (тобто послуга, яка використовується системою, але не є її частиною) і над якою Організація, як правило, не має прямого контролю

3.14 зовнішня система

Система (або компонент системи), що перебуває поза межами, встановленими Організацією і над яким Організація, як правило, не має прямого контролю

3.15 інформаційна (автоматизована) система

Організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів

3.16 інформаційно-комунікаційна система

Сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле

3.17 концепція безпеки інформації

Документ, прийнятий на рівні Організації, який закріплює основні положення та відношення вищого керівництва щодо питань захисту інформації в Організації, закріплює вимоги безпеки, а також прийняті Організацією ризики

3.18 налаштування заходу захисту

Процес визначення параметрів заходів захисту, які повинні бути визначені Організацією

3.19 оцінювання дотримання вимог цільового профілю безпеки

Процес перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації та кіберзахисту в системах з метою встановлення стану захищеності систем або їх відповідності вимогам законодавчих та інших нормативно-правових актів, стандартів, нормативних документів у сферах криптографічного та технічного захисту інформації, кіберзахисту

3.20 перелік авторизованих з безпеки систем

Єдина електронна база даних, що містить відомості про авторизовані системи з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні підприємства (установи та/або організації), органи місцевого самоврядування

3.21 політика безпеки інформації

Документ або сукупність документів рівня системи, які містять набір вимог, правил, обмежень, рекомендацій, що регламентують порядок обробки інформації в системі та спрямовані на досягнення і підтримку стану безпеки системи та Організації в цілому

3.22 посилення заходу захисту

Розширення заходу захисту для створення додаткової, але пов’язаної з первинною, функціональності або для збільшення рівня захищеності

3.23 постійний моніторинг безпеки

Набір процедур, направлених на підтримку обізнаності (поінформованості) про поточний стан безпеки в системі та Організації для прийняття рішень щодо управління ризиками безпеки

3.24 програма безпеки інформації

Документ на рівні системи, який наслідує принципи Концепції безпеки інформації та надає їхню специфікацію для конкретної системи

3.25 робоче середовище

Фізичне оточення, в якому система отримує/створює, обробляє, зберігає та передає інформацію

3.26 роль

Визначена сукупність правил, які встановлюють рамки взаємодії між користувачем та системою

3.27 специфічні заходи захисту

Заходи захисту, що реалізуються на системному рівні та не успадковуються (використовуються) жодною іншою системою

3.28 управління доступом на основі ролей

Набір дозволів доступу, який отримує фізична особа на основі явного або неявного припущення про певну роль

3.29 успадкований захід захисту

Захід захисту, реалізований, коли система отримує результати захисту від впровадженого заходу захисту, що контролюється, впроваджується (реалізується/використовується), оцінюється суб’єктами, які не несуть відповідальності за цю систему

3.30 цільовий профіль безпеки системи (ЦПБ)

Взаємопов’язана сукупність заходів із захисту інформації, визначених органами державної влади, державними підприємствами, установами та організаціями, органами місцевого самоврядування (далі – власник або розпорядник системи) для відповідних систем з урахуванням мінімальних вимог

щодо таких заходів із захисту (базового профілю), вимог законодавчих та інших нормативно-правових актів, стандартів і нормативних документів у сферах криптографічного та технічного захисту інформації, кіберзахисту, нормативних документів системи технічного та криптографічного захисту інформації, кіберзахисту, а також галузевого профілю (за наявності), політик безпеки, призначення системи, її структурно-функціональних характеристик та особливостей функціонування системи, результатів проведеної оцінки ризиків безпеки

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

У цьому стандарті використано такі позначення та скорочення:

БІ – безпека інформації;

БПБ – базовий профіль безпеки;

ГПБ – галузевий профіль безпеки;

ІТ – інформаційна технологія;

ПВПД – цикл «Плануй – виконуй – перевіряй – дій»;

ПД – персональні дані;

ЦПБ – цільовий профіль безпеки системи.

5 МОДЕЛЬ ПОРЯДКУ ВПРОВАДЖЕННЯ ВИМОГ З БЕЗПЕКИ

5.1 Впроваджені заходи захисту мають забезпечувати задоволення вимог з безпеки. Такі вимоги можуть бути сформульовані національними, державними та міжнародними установами. Необхідною умовою забезпечення інтероперабельності національних систем з міжнародними партнерами є можливість легкого впровадження міжнародних стандартів у галузі безпеки інформації (зокрема, NIST Special Publication 800-30 [14], NIST Special Publication 800-37 [15], NIST Special Publication 800-39 [16], NIST Special Publication 800-53 [17], NIST Special Publication 800-128 [18] та NIST Special

Publication 800-160 [19, 20]). Для більш швидкого та ефективного впровадження вимог з безпеки необхідно застосовувати механізм, який здатен забезпечити легкий процес інтеграції державних, міжнародних та інших стандартів безпеки.

5.2 При впровадженні вимог з безпеки має бути забезпечена можливість «персоналізації» даного процесу для кожної системи. Під персоналізацією розуміється можливість гнучкого процесу впровадження вимог з безпеки, який максимально забезпечує задоволення потреб конкретної системи та є економічно ефективним.

5.3 Рішення щодо сукупності вимог з безпеки для розгортання в конкретній системі має прийматися залежно від типу системи та інформації, яка в ній знаходиться (циркулює) за результатами експертної оцінки інформації.

5.4 Власники або розпорядники систем мають впроваджувати вимоги з безпеки керуючись положеннями цього стандарту для впровадження відповідних заходів захисту, направлених на забезпечення цілісності та доступності інформації, яка знаходиться (циркулює) у цих системах.

5.5 Власники або розпорядники систем, які обробляють будь-які ПД, не залежно від форми власності системи, мають впроваджувати вимоги з безпеки керуючись положеннями цього стандарту, а також вимог ДСТУ EN ISO/IEC 29100:2022 «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя» (EN ISO/IEC 29100:2020, IDT; ISO/IEC 29100:2011, including Amd 1:2018, IDT) [11] для впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності ПД. Власники або розпорядники систем, які обробляють ПД та знаходяться у приватній власності додатково можуть прийняти рішення щодо впровадження відповідності системи вимогам міжнародних Регламентів (GDPR).

6 ЗАГАЛЬНІ ПОЛОЖЕННЯ

6.1 Взаємодія між рівнями управління інформаційної безпеки Організації

6.1.1 Виконання вимог з безпеки повинні бути частиною загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки в Організації.

6.1.2 Заходи захисту повинні забезпечити безпечність та надійність виконання функцій/процесів за призначенням Організації. Впровадження та функціонування заходів захисту стосується всіх підрозділів Організації. Тому відповідальні особи повинні співпрацювати у вирішенні питань, що належать до сфери їх відповідальності, під час впровадження та функціонування заходів захисту.

6.1.3 Цілі захисту інформації, заходи захисту (існуючі або ті, що будуть впроваджені), документація, що описує функціонування заходів захисту, повинні бути зрозумілими для всіх зацікавлених сторін (стейкхолдерів).

6.1.4 Виконання в Організації вимог з безпеки:

– постійно відслідковувати та оцінювати ризики безпеки з урахуванням призначення (місії) Організації;

– ефективно виявляти ризики безпеки та знижувати ймовірність їх виникнення;

– розробити ефективну політику безпеки інформації та забезпечити її якісне виконання;

– ефективно розробляти, впроваджувати та тестувати заходи захисту інформації;

– забезпечити розуміння питань безпеки інформації керівництвом та всіма працівниками Організації.

6.1.5 Управління ризиками безпеки потребує участі посадових осіб на всіх ланках управління Організації – від керівництва, що визначає стратегічне бачення (місію), цілі та задачі для Організації, до керівників середньої ланки, які здійснюють планування, виконання та управління функціями/процесами, та осіб, які розробляють, впроваджують, використовують і підтримують системи та процеси управління ризиками. Такий підхід підтримує виконання функціональних завдань Організації та реалізації процесів. Управління ризиками є цілісною діяльністю, яка впливає на всі аспекти діяльності Організації, зокрема планування, архітектуру підприємства, процеси життєвого циклу розробки системи.

На рисунку 1 наведено багаторівневий підхід до управління ризиками безпеки. Управління ризиками здійснюється на організаційному, процесному (функціональному) та на системному рівнях.

Взаємодія між рівнями забезпечується двонаправленими інформаційними потоками. Це дозволяє обробляти ризики безпеки на всіх рівнях.

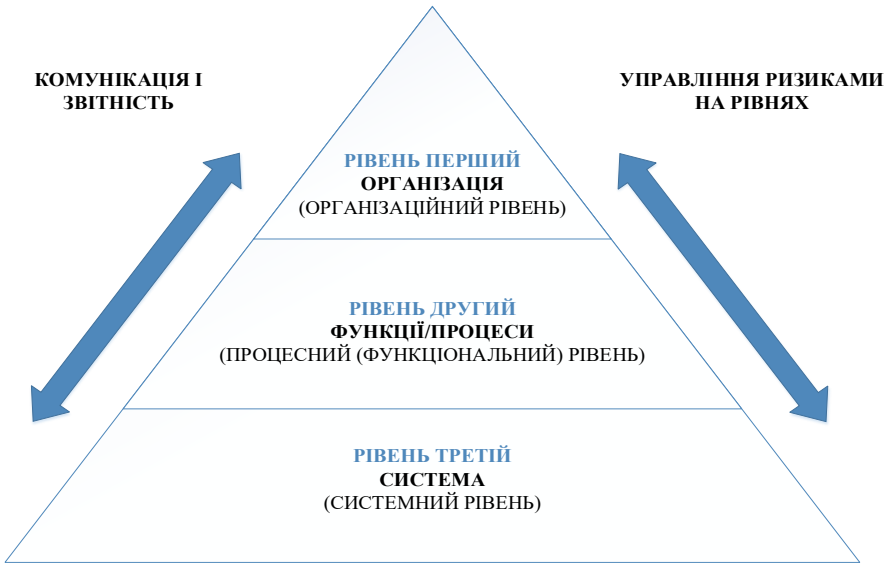


Рисунок 1 – Загальний підхід щодо управління ризиками безпеки

6.2 Типи заходів захисту та особливості їх застосування

6.2.1 Заходи, що проводяться на організаційному, процесному (функціональному) та системному рівнях (рисунок 2) є важливими для

підготовки Організації до реалізації концепції управління ризиками та впровадження вимог з безпеки. Така підготовка передбачає широкий спектр заходів.

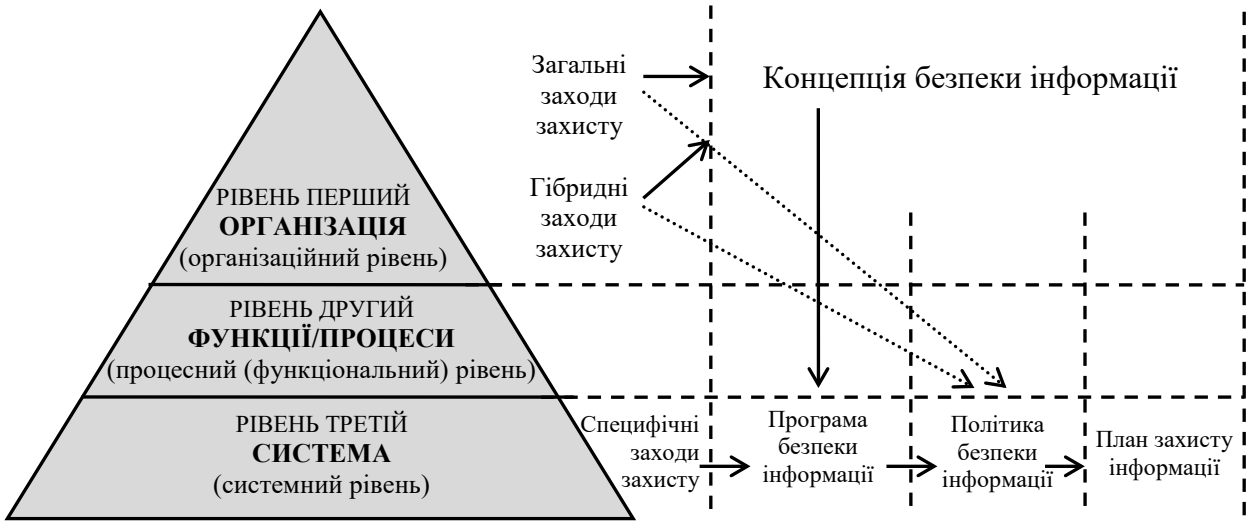


Рисунок 2 – Розподіл заходів захисту за рівнями управління ризиками в організації

6.2.2 Прийняття рішення щодо управління ризиками безпеки на системному рівні тісно пов’язане з такими аспектами:

– призначення (місія, цілі), завдання, функції та процеси Організації;

– ініціативи з модернізації систем, компонентів та послуг систем;

– архітектура Організації, зменшення складності систем шляхом інтеграції, оптимізації та стандартизації;

– розподіл ресурсів для забезпечення ефективного, результативного та економічно-вигідного виконання функцій/процесів та досягнення цілей Організації.

6.2.3 Цей стандарт визначає три типи заходів захисту інформації: загальні заходи захисту, специфічні для системи заходи захисту (далі – специфічні заходи захисту) та гібридні заходи захисту. Тип заходу захисту визначає:

– сферу застосування заходу захисту;

– спільний характер або спадковість заходів захисту;

– відповідальність за розробку (налаштування), впровадження, оцінювання та надання дозволу на впровадження заходу захисту.

6.2.4 Кожен тип заходу захисту має конкретну спрямованість і завдання, що допомагає організаціям ефективно впроваджувати його та отримувати очікувані результати в контексті виконання вимог з безпеки. Застосування певних типів заходів захисту забезпечує оптимізацію витрат (часових, матеріальних, людських) у різних системах і робочих середовищах на впровадження (реалізацію) заходів захисту та побудову системи захисту інформації загалом.

6.2.5 Загальні заходи захисту можуть бути використані для декількох систем одночасно. Захід захисту вважається успадкованим, коли система використовує результати захисту від впровадженого заходу захисту, що контролюється, впроваджується (реалізується), оцінюється суб'єктами, які не несуть відповідальності за цю систему. Загальні заходи захисту можуть впроваджуватися різними технологіями: застосування засобів захисту периметру, засобів управління доступом, засобів ідентифікації та автентифікації, а також заходів захисту, які є елементом міждоменних рішень. Витрати на розробку, впровадження (реалізацію), оцінювання, прийняття рішення про застосування та моніторинг загальних заходів захисту можуть бути амортизовані в різних системах та елементах Організації. Вибір загальних заходів захисту рекомендуються здійснювати на загальноорганізаційній основі із залученням керівництва Організації, яке розуміє цілі та завдання Організації, ризики безпеки Організації, важливість систем, що підтримують функції, процеси та активи Організації. Залучення керівництва Організації забезпечить оптимальність розподілу ресурсів і відповідальності щодо розроблення, впровадження, оцінювання, надання дозволу та моніторингу загальних заходів захисту.

6.2.6 Відповідальність за провадження загальних заходів захисту покладається на конкретних посадових осіб. Ці посадові особи розробляють, впроваджують, оцінюють, приймають рішення про застосування і контролюють вибрані Організацією для впровадження (реалізації) загальні заходи захисту. Визначення та вибір загальних заходів захисту найефективніше проводити в

співпраці з уповноваженими посадовими особами, представниками керівництва, аналітиками безпеки, власниками або розпорядниками інформації та з іншими зацікавленими сторонами. Загальні заходи захисту мають бути задокументовані в програмі (концепції) безпеки інформації Організації. Вони також можуть бути задокументовані в політиках безпеки систем, які успадковують ці заходи захисту, або в ситуаціях, коли загальні заходи захисту впроваджуються в межах конкретних систем. Загальні заходи захисту можуть бути описані в одному документі або в кількох документах з посиланнями на інші документи. Якщо програма (концепція) безпеки інформації складається з декількох документів, у кожному документі мають бути визначені посадові особи, відповідальні за розробку, реалізацію, оцінювання, прийняття рішення про застосування та моніторинг відповідних загальних заходів захисту. Якщо загальні заходи захисту включаються в окрему політику безпеки системи, концепція безпеки інформації Організації має вказувати, які окремі політики безпеки містять опис загальних заходів захисту.

6.2.7 Заходи захисту, які не визначені як загальні заходи, вважаються специфічними або гібридними. За впровадження специфічного заходу захисту, що стосується конкретної системи, відповідальність несуть власники або розпорядники системи та відповідальні особи.

6.2.8 Захід захисту може бути визначений як гібридний, якщо одна частина заходу захисту є загальною, а інша частина заходу захисту є специфічною для системи.

Організація може реалізовувати заходи планування безперервної роботи, використовуючи для всіх систем заздалегідь погоджений з власниками або розпорядниками шаблон плану, пристосовуючи план для конкретного використання. Розподіл гібридних заходів захисту на загальні та специфічні може залежати від Організації, типів використовуваних інформаційних технологій, розподілу обов’язків і методів (механізмів), що використовуються Організацією для реалізації заходів захисту.

6.2.9 Визначення того, чи є захід захисту загальним, гібридним або специфічним, залежить від контексту його впровадження (реалізації). Захід захисту не можна визначити загальним, гібридним або специфічним, лише ґрунтуючись на його формулюванні.

Захід захисту може бути специфічним для однієї системи, і водночас може бути загальним заходом для іншої системи (тобто успадкованим від першої системи). Одним з методів визначення того, чи може специфічний захід бути загальним заходом для інших систем, є розгляд того, хто чи що залежить від функціональності цього заходу захисту. Якщо певна частина системи, що є зовнішньою для цієї системи, залежить від заходу захисту, то цей захід може бути загальним.

6.2.10 Розмежування заходів захисту на загальні, гібридні та специфічні може допомогти оптимізувати витрати на впровадження та оцінювання заходів захисту, а також забезпечити гнучкість і послідовність застосування засобів захисту у межах усієї Організації. Хоча розподіл заходів захисту на загальні, гібридні й специфічні є простим та інтуїтивно зрозумілим, фактично застосування зазначених заходів потребує планування та координації діяльності із захисту інформації.

6.3 Документування заходів захисту

6.3.1 Даний розділ надає рекомендації щодо порядку документування основних вимог з безпеки, а також впроваджених заходів захисту інформації на організаційному та системному рівнях.

6.3.2 До основних документів, які можуть бути сформовані та затверджені в Організації на систему належать такі:

- концепція безпеки інформації (розробляється за необхідності);
- опис системи;
- програма безпеки інформації (розробляється за необхідності);
- політики безпеки інформації;

– плани захисту інформації;

– результати експертної оцінки інформації;

– результати оцінки ризиків;

– цільовий профіль безпеки системи;

– документи, які передбачені ЦПБ (плани, політики, інструкції, журнали тощо);

– звіт з оцінювання реалізації ЦПБ;

– авторизаційний лист.

6.3.3 Даний перелік не є вичерпним і може доповнюватися на розсуд власника або розпорядника Організації та/або системи, виходячи із особливостей Організації/системи та/або нормативних вимог, сформованих уповноваженим органом або галузевим уповноваженим органом з авторизації.

У таблиці 1 наведені рекомендовані розділи відповідних документів. Кожен із цих документів може бути представлений як окремий документ або сукупність документів.

Таблиця 1 – Рекомендовані документи та їхній стислий зміст

Назва документу	**Рекомендований зміст**
1	**2**
Концепція безпеки інформації	Концепція безпеки інформації не є обов'язковою та розробляється за необхідністю в довільній формі. Концепція безпеки інформації визначає загальну політику Організації стосовно управління ризиками, а саме визначає загальні стандарти які Організація використовує для проведення оцінки ризиків в різних сферах, відповідальних осіб або функціональні ролі Організації відповідальні за оцінку ризиків а також може включати проведену оцінку ризиків рівня всієї Організації з визначенням загальної позиції Організації стосовно тих чи інших ризиків та заходи захисту, які впроваджуються на всю Організацію.
Опис системи	1. Загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв’язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо); 2. Види і характеристики каналів зв’язку; 3. Особливості взаємодії окремих компонентів, їх взаємний вплив один на одного; 4. Тощо.

Продовження таблиці

1	2
	Опис технології обробки інформації повинен виявити особливості обігу електронних даних (документів), мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Описуються види носіїв інформації та порядок їх використання під час функціонування системи. Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елемента) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.
Програма безпеки інформації	Програма безпеки інформації не є обов'язковою та розробляється за необхідністю в довільній формі. Програма безпеки інформації повністю або частково наслідує Концепцію безпеки інформації для конкретної системи. У ній зазначаються відповідальні особи або функціональні ролі Організації відповідальні за проведення оцінки ризиків функціонування конкретної системи, стандарт або методологія, за яким проводиться оцінка ризиків для конкретної системи, а також заходи захисту рівня Організації, які розповсюджуються на систему.
Експертна оцінка інформації	Обґрунтування вибору базового або галузевого профілю безпеки системи залежно від інформації, що обробляється (оброблятиметься) у системі, здійснюється власником або розпорядником системи з урахуванням проведеної експертної оцінки інформації, яка обробляється (оброблятиметься) у системі. При проведенні експертної оцінки інформації слід керуватися вимогами «Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затвердженому постановою Кабінету Міністрів України № 939 від 18.12.2013 [2] та «Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», затвердженої постановою Кабінету Міністрів України № 736 від 19.10.2016 [3].
Результати оцінки ризиків	Стандарти, які можуть бути використанні при оцінці ризиків обираються власником або розпорядником системи самостійно, проте орієнтовна загальна структура звіту за результатами оцінювання ризиків повинна мати такий вигляд: 1. Мета проведення оцінювання; 2. Методологія оцінювання; 3. Критерії оцінювання; 4. Допустимий рівень ризику; 5. Перелік виявлених загроз; 6. Опис вразливих місць; 7. Оцінка наслідків від реалізації ризиків; 8. Перелік уже існуючих заходів протидії ризикам;

Продовження таблиці

1	2
	9. Рекомендації щодо усунення залишкових ризиків.
Цільовий профіль безпеки системи	Розробляється відповідно до Рекомендацій з розроблення, які затверджуються Адміністрацією Держспецзв'язку.
План захисту інформації	План захисту інформації – це документ, у якому наводяться технічні засоби, відповідальні особи та ресурси, які реалізують вимоги ЦПБ та необхідні для забезпечення захисту інформації в системі або в Організації загалом. Розробляється відповідно до вимог заходу захисту PL-2, який наведений у НД ТЗІ 3.6-006-24 [12].
Політики безпеки інформації	Політики безпеки інформації – це сукупність затверджених керівництвом Організації правил, вимог та обмежень, які визначають порядок забезпечення захисту інформації, використання систем і відповідальність користувачів та адміністраторів. 1. Ціль/цілі політики БІ; 2. Сфера застосування Політики БІ; 3. Ролі в системі та сфера їхньої відповідальності; 4. Порядок перегляду Політики БІ.
Документи, які передбачені ЦПБ (плани, політики, інструкції, журнали тощо)	Розробляються в довільній формі у відповідності до вимог реалізації заходів захисту, які визначаються згідно НД ТЗІ 3.6-006-24 [12].
Звіт з оцінювання реалізації ЦПБ	Розробляється з урахуванням Рекомендацій з оцінювання дотримання вимог ЦПБ, які затверджуються Адміністрацією Держспецзв'язку.
Авторизаційний лист	Форма авторизаційного листа наведена в Додатку 1 до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України № 712 від 18.06.2025 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» [5].

6.4 Етапи впровадження заходів захисту

6.4.1 Розгортання та подальше функціонування заходів захисту здійснюється як безперервна цілеспрямована діяльність Організації, яка складається з етапів та завдань (рисунок 3).

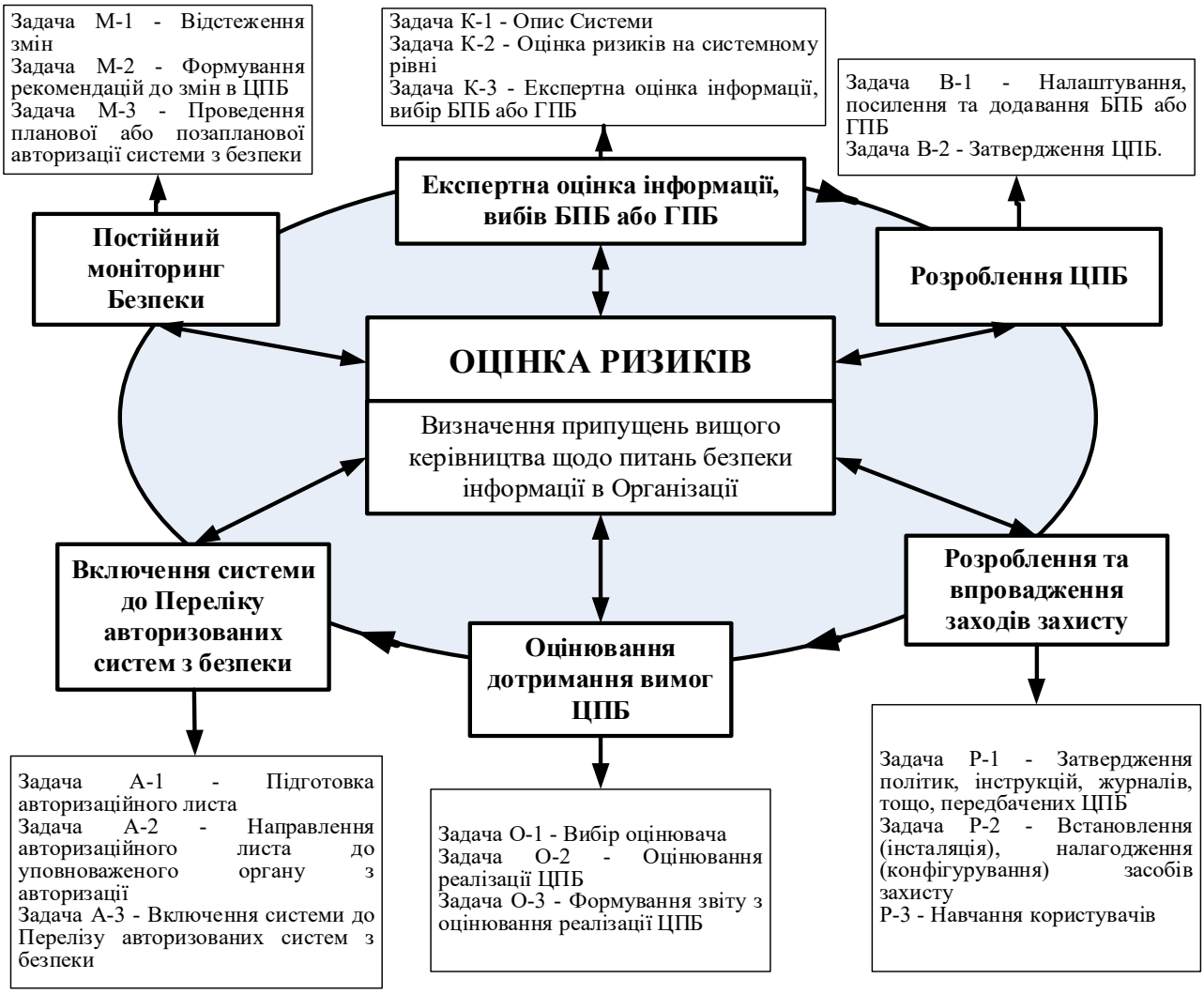


Рисунок 3 – Етапи впровадження заходів захисту в Організації

6.4.2 Організації під час впровадження заходів захисту слід дотримуватися послідовного підходу, який застосовується до всіх етапів управління ризиками у масштабах всієї Організації (від організаційного до системного рівня). Відповідальні особи в Організації визначають необхідні ресурси для виконання завдань щодо управління ризиками та забезпечують доступність цих ресурсів для відповідного персоналу.

6.4.3 Діяльність з впровадження заходів захисту складається з семи етапів:

– експертна оцінка інформації, вибір БПБ або ГПБ;

– оцінка ризиків;

– розроблення ЦПБ;

– розробка та впровадження заходів захисту (впровадження вимог ЦПБ);
– оцінювання дотримання вимог ЦПБ;
– включення системи до Переліку авторизованих систем з безпеки;
– постійний моніторинг безпеки.

6.4.4 Усі виконані дії щодо виконання вищезазначених етапів повинні документуватися відповідальними особами в частині, яка регулюється їхніми повноваженнями (обов'язками). За своїми ролями та впливом при виконанні на процес оцінки ризиків на організаційному рівні, результати експертної оцінки інформації, вибір, впровадження заходів захисту та оцінювання їх реалізації, а також авторизації з безпеки системи та процесів постійного моніторингу безпеки, усі особи можна розподілити на такі:

а) Власник або розпорядник системи.

б) Розробник (проєктувальник) заходів захисту. За необхідності для виконання цієї ролі можуть залучатися сторонні фахівці та/або суб'єкти господарювання на договірній основі.

в) Постачальник товарів, робіт і послуг.

г) Підрозділ із кіберзахисту або призначена особа чи особи, на яких покладається забезпечення захисту інформації та контролю за ним.

д) Оцінювач дотримання вимог ЦПБ. Для виконання цієї ролі повинні залучатися фахівці або Організації які відповідають вимогам, встановлених законодавством.

е) Уповноважений орган з авторизації.

ж) Галузевий уповноважений орган.

6.4.5 В свою чергу, кожний з етапів складається із завдань. Кожне завдання розглядається як функціональний блок, який містить мету, вхідні дані, вихідні дані та перелік ролей, що відповідають за виконання завдання.

6.4.6 Впровадження вимог цього та інших стандартів з питань управління безпекою інформації є безперервним процесом розроблення, впровадження,

функціонування, моніторингу, перегляду, підтримування та вдосконалення заходів захисту.

6.4.7 Цей стандарт щодо виконання вимог з безпеки інформації конкретизує вимоги міжнародного стандарту ДСТУ ISO/IEC 27003:2018 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова» (ISO/IEC 27003:2017, IDT) [9] з урахуванням особливостей діяльності підприємств, установ та організацій з питань безпеки інформації. Модель, що впроваджується цим стандартом, конкретизує модель ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2022 [8] (рисунок 4).

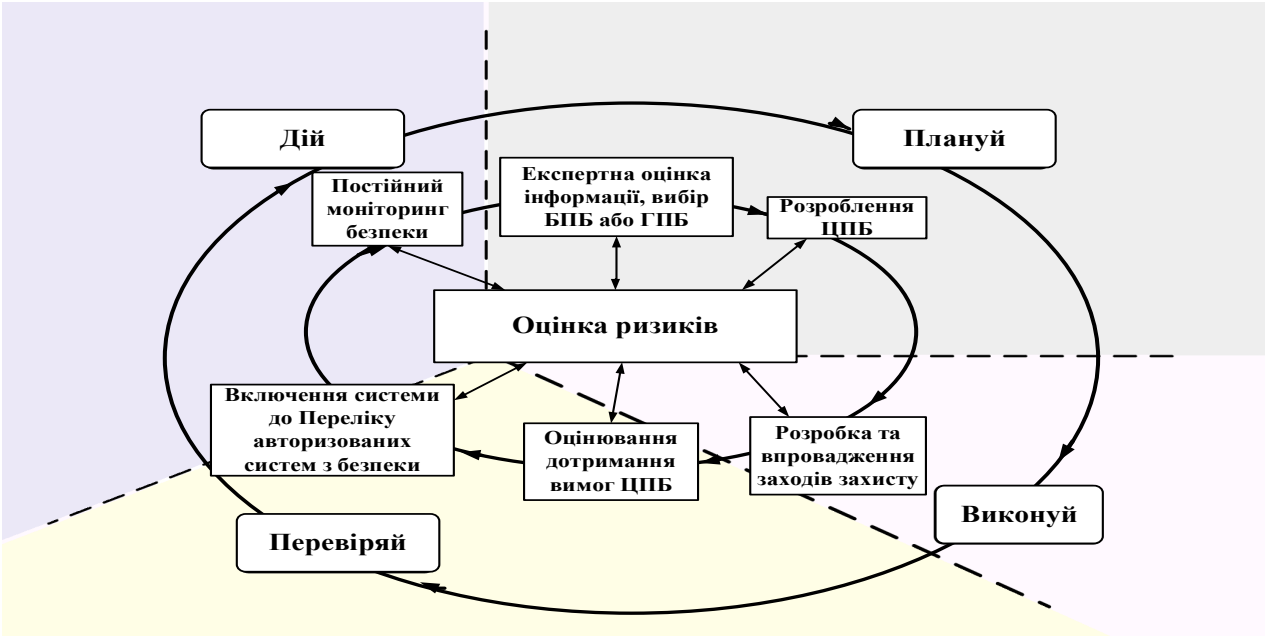


Рисунок 4 – Відповідність етапів впровадження вимог з безпеки моделі ПВПД, яка визначена у ISO/IEC 27001

Кожний із етапів має перелік вхідних та вихідних даних (рисунок 5). Вихідні дані кожного із етапів можуть бути вхідними для подальших.

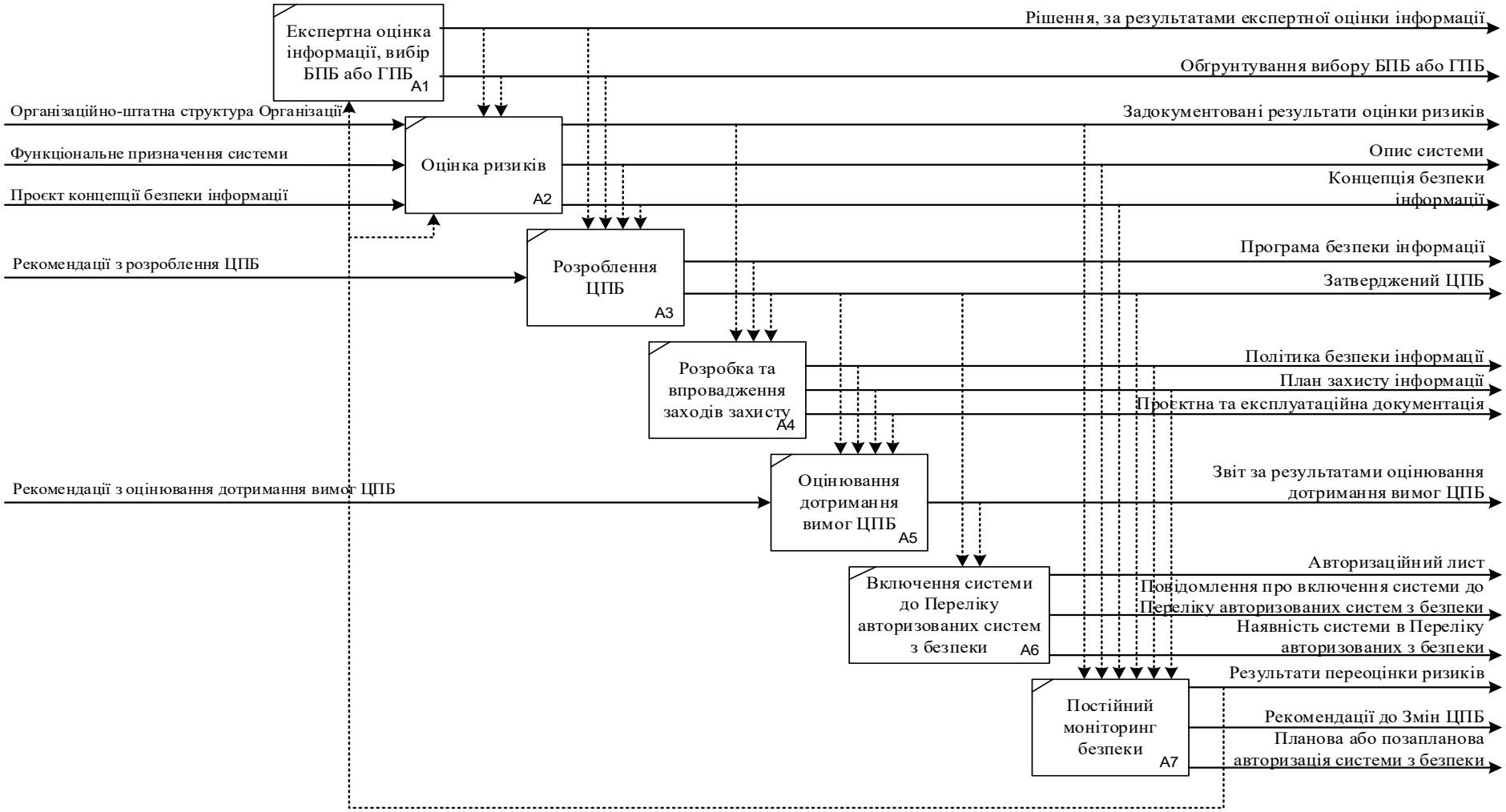


Рисунок 5 – Взаємозв’язок етапів впровадження заходів захисту

7 ВИЗНАЧЕННЯ ЕТАПІВ ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ

7.1 Етап експертної оцінки інформації, вибору БПБ або ГПБ

7.1.1 Відповідно до «Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», затверджених постановою Кабінету Міністрів України № 373 від 29.03.2006 [1] обрання базового або галузевого профілю безпеки системи залежно від інформації, що обробляється (оброблятиметься) у системі, здійснюється власником або розпорядником системи з урахуванням проведеної експертної оцінки інформації, яка обробляється (оброблятиметься) у системі та з урахуванням функціонального призначення системи.

7.1.2 При проведенні експертної оцінки інформації слід керуватися вимогами «Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затвердженого постановою Кабінету Міністрів України № 939 від 18.12.2013 [2] та «Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», затвердженої постановою Кабінету Міністрів України № 736 від 19.10.2016 [3].

7.2 Етап оцінки ризиків

7.2.1 На цьому етапі здійснюється визначення мети функціонування системи, аналіз умов її експлуатації та оцінювання потенційних ризиків для інформації й ресурсів системи. Проводиться ідентифікація активів, джерел загроз, можливих вразливостей та потенційних наслідків порушення конфіденційності, цілісності й доступності інформації.

7.2.2 Оцінка ризиків виконується з урахуванням:

- архітектури системи;
- виду інформації, що обробляється;

- особливостей середовища функціонування;
- наявних зовнішніх і внутрішніх підключень;
- технологічних та організаційних особливостей експлуатації системи.

7.2.3 У межах етапу визначаються можливі сценарії реалізації загроз, оцінюється рівень їх впливу на діяльність Організації або системи та встановлюється допустимий рівень ризику. Отримані результати використовуються для формування вимог до захисту інформації, вибору необхідних заходів захисту та подальшого формування профілю безпеки системи.

7.2.4 Оцінка ризиків на рівні Організації ґрунтується на узагальнених даних, отриманих у результаті оцінки ризиків на рівні систем, безперервного моніторингу та оцінки будь-яких стратегічних ризиків, що мають значення для Організації. Організація враховує сукупність ризиків, пов’язаних з експлуатацією та використанням своїх систем, з обміном інформацією та взаємодією з іншими системами, що належать їй або зовнішнім суб’єктам, а також із залученням зовнішніх постачальників послуг.

Організація може переглянути ризики, пов’язані з архітектурою підприємства та системами різного рівня впливу, що знаходяться в одній мережі, а також перевірити, чи відокремлені системи з вищим рівнем впливу від систем з нижчим рівнем впливу або систем, що експлуатуються та обслуговуються зовнішніми постачальниками. Організація може також врахувати різноманітність середовищ, що можуть існувати в Організації (наприклад, різні локації, що виконують різні завдання або функції), та необхідність врахування такої різноманітності в оцінках ризиків. Результати оцінки ризиків використовуються при створенні ЦПБ та профілю кібербезпеки.

Примітка. Як приклад, стандарти з питань оцінювання ризиків, але не обмежуючись: ISO/IEC 27005 [10] або NIST SP 800-30 [14].

7.3 Етап розроблення ЦПБ

7.3.1 На цьому етапі розробляється ЦПБ, який визначає конкретний перелік заходів захисту, необхідних для забезпечення встановленого рівня безпеки інформації та прийнятного рівня ризику.

7.3.2 Цільовий профіль формується на основі:

- обраного базового або галузевого профілю безпеки;
- вимог нормативних документів у сфері захисту інформації та кіберзахисту;
- особливостей архітектури та умов функціонування системи;
- результатів оцінки ризиків.

7.3.3 У межах етапу здійснюється уточнення та адаптація заходів захисту БПБ або ГПБ до конкретної системи:

- за необхідності посилюються наявні заходи захисту;
- за необхідності додаються додаткові заходи захисту;
- здійснюється налаштування параметрів заходів захисту;
- за необхідності враховуються базові вимоги з кіберзахисту.

7.3.4 Результатом етапу є документально визначений ЦПБ, який містить перелік організаційних та технічних заходів захисту інформації та є основою для їх подальшого впровадження.

7.4 Етап розробки та впровадження заходів захисту

7.4.1 На цьому етапі здійснюється практична реалізація заходів захисту інформації, визначених у ЦПБ. Метою етапу є створення та впровадження організаційних, апаратних, програмно-апаратних та програмних механізмів, необхідних для забезпечення встановленого рівня захищеності системи.

7.4.2 У межах етапу виконуються:

- розробка політик, процедур, інструкцій та регламентів з питань захисту інформації та кіберзахисту;

– впровадження механізмів ідентифікації, автентифікації та розмежування доступу;

– налаштування засобів реєстрації та аудиту подій безпеки;

– реалізація криптографічного захисту інформації;

– впровадження антивірусного захисту, резервного копіювання та відновлення інформації;

– забезпечення мережевого та фізичного захисту;

– налаштування процедур управління конфігурацією та змінами в системі;

– тощо.

7.4.3 Також визначаються відповідальні особи за адміністрування, супроводження та контроль функціонування заходів захисту. Реалізація заходів повинна відповідати вимогам внутрішніх політик Організації та ЦПБ.

7.4.4 Під час впровадження перевіряється сумісність заходів захисту з архітектурою системи, умовами її експлуатації та технологічними особливостями функціонування.

7.4.5 Результатом етапу є впроваджені в системі заходи захисту інформації та комплект організаційно-розпорядчої і технічної документації, необхідної для подальшого оцінювання ефективності реалізованих заходів та експлуатації системи.

7.5 Етап оцінювання дотримання вимог ЦПБ

7.5.1 На цьому етапі здійснюється перевірка повноти, коректності та ефективності реалізації заходів захисту інформації, визначених у ЦПБ. Метою оцінювання є підтвердження того, що впроваджені механізми захисту функціонують відповідно до встановлених вимог та забезпечують необхідний рівень захищеності системи.

7.5.2 У межах етапу проводяться:

– аналіз організаційно-розпорядчої та технічної документації;

– перевірка налаштувань засобів захисту;

- оцінювання правильності реалізації механізмів безпеки;
- перевірка обізнаності персоналу щодо експлуатації системи;
- виявлення невідповідностей, недоліків та потенційних вразливостей.

7.5.3 Оцінювання дотримання вимог ЦПБ здійснюється з урахуванням рекомендацій з оцінювання дотримання вимог ЦПБ, затверджених уповноваженим органом з авторизації.

7.5.4 Суб'єкти господарювання, фізичні особи – підприємці або фізичні особи, що проводять оцінювання, повинні відповідати вимогам до суб'єктів оцінювання, що передбачають сукупність кваліфікаційних та інших обов'язкових умов і критеріїв. Вимоги до суб'єктів оцінювання затверджуються Адміністрацією Держспецзв'язку.

7.5.5 Заходи щодо організації та проведення оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки проводяться з дотриманням таких принципів:

– неупередженість у прийнятті рішень: рішення та висновки оцінювання формуються виключно на підставі перевірених матеріалів (доказів). Жоден оцінювач не може допускати впливу особистих інтересів, тиску з боку керівництва, клієнта або третіх осіб;

– відсутність конфлікту інтересів: оцінювання не може проводити Організація, яка володіє або розпоряджується об'єктом оцінювання або брала участь у його створенні, щоб уникнути будь-якого конфлікту інтересів і забезпечити повну незалежність оцінювання;

– об'єктивність матеріалів (доказів): висновки базуються лише на перевірених і задокументованих фактах, отриманих шляхом дослідження, опитування, випробування;

– прозорість процесу: усі етапи оцінювання, критерії оцінки, методи та рішення документуються та є доступними для зацікавлених сторін у межах встановлених правил конфіденційності;

– відповідальність оцінювача: кожен оцінювач несе персональну відповідальність за дотримання принципів незалежності, професійної етики та об’єктивності.

7.5.6 Результати етапу оформлюються у вигляді звіту з оцінки у якому міститься висновки щодо реалізації заходів захисту ЦПБ, а також перелік виявлених невідповідностей із рекомендаціями щодо їх усунення. Отримані результати використовуються для прийняття рішення щодо готовності системи до авторизації з безпеки та введення в експлуатацію.

7.5.7 Організації перед укладенням договору на проведення оцінювання дотримання вимог ЦПБ та під час експлуатації системи можуть проводити самооцінювання. При визначенні оцінювача в межах Організації необхідно враховувати як технічну компетенцію, так і незалежність при відборі оцінювачів заходів захисту. Організації забезпечують, щоб оцінювачі заходів захисту володіли необхідними навичками та технічною компетенцією для розробки ефективних планів оцінювання та проведення оцінювання заходів.

7.6 Етап включення системи до Переліку авторизованих систем з безпеки

7.6.1 За результатами позитивного оцінювання виконання вимог ЦПБ, що наведено у відповідному звіті, Організація готує авторизаційний лист та надсилає його на адресу уповноваженого органу з авторизації. За результатами успішного включення системи до переліку авторизованих систем з безпеки уповноважений орган з авторизації направляє на адресу власника або розпорядника системи повідомлення про включення системи до переліку авторизованих систем з безпеки.

7.6.2 Порядок ведення переліку авторизованих систем з безпеки визначається уповноваженим органом з авторизації.

7.7 Етап постійного моніторингу безпеки

7.7.1 На цьому етапі здійснюється постійний контроль стану захищеності системи після її введення в експлуатацію. Метою моніторингу є своєчасне виявлення змін, подій безпеки, нових загроз і вразливостей, які можуть вплинути на рівень захисту інформації та призвести до зростання ризиків.

7.7.2 У межах етапу проводиться моніторинг:

- функціонування заходів захисту;
- подій інформаційної безпеки та журналів аудиту;
- змін конфігурації системи;
- нових загроз, вразливостей і ризиків;
- оновлень програмного забезпечення та засобів захисту;
- змін нормативно-правових актів, вимог БПБ або ГПБ та політик Організації.

7.7.3 Також проводиться періодичне оцінювання ефективності реалізованих заходів захисту.

7.7.4 Особлива увага приділяється виявленню змін у середовищі функціонування системи, які можуть вплинути на її безпеку, зокрема змінам архітектури, складу програмного забезпечення, порядку обробки інформації або режиму доступу користувачів.

7.7.5 У разі виявлення недоліків або змін, що впливають на рівень захищеності системи, Організація здійснює коригування заходів захисту, повторне оцінювання реалізації ЦПБ в частині змін а також проведення планової або позапланової авторизації.

7.7.6 Результати моніторингу документуються та використовуються для підтримання актуального стану безпеки системи протягом усього життєвого циклу її експлуатації.

7.7.7 Ефективна стратегія безперервного моніторингу на рівні системи розробляється та впроваджується у взаємодії зі стратегією безперервного моніторингу на рівні Організації. Стратегія безперервного моніторингу на рівні

системи відповідає стратегії безперервного моніторингу для Організації та доповнює її. Стратегія на рівні системи стосується моніторингу тих заходів захисту, для яких моніторинг не передбачений у рамках стратегії безперервного моніторингу на рівні Організації. Стратегія на рівні системи визначає частоту моніторингу заходів захисту, не охоплених стратегією на рівні Організації, та визначає підхід, який слід використовувати для оцінки цих заходів захисту, а також визначає, як слід здійснювати моніторинг змін у системі та середовищі функціонування, як слід проводити оцінку ризиків; а також вимоги до звітності щодо стану захищеності інформації.

8 ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ НА РІЗНИХ ЕТАПАХ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМ

8.1 З метою підвищення ефективності виконання вимог з безпеки, вони мають бути інтегровані до життєвого циклу розробки систем на всіх етапах.

8.2 У Додатку А наведено етапи впровадження заходів захисту на етапах життєвого циклу засобу інформатизації. Додатком 1 до Обов’язкових вимог до створення (модернізації, модифікації, розвитку), адміністрування та забезпечення функціонування засобу інформатизації, що затверджені постановою Кабінету Міністрів України від 21.02.2025 № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» [4] наведено Матрицю дій відповідно до життєвого циклу засобу інформатизації (далі – Матриця дій). Далі наведено відображення етапів 7 розділу цього стандарту на Матриці дій.

ДОДАТОК А

(обов’язковий)

ЕТАПИ ВИКОНАННЯ ВИМОГ З БЕЗПЕКИ В СИСТЕМІ У РАМКАХ ДО ЖИТТЄВОГО ЦИКЛУ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

Найменування стадії життєвого циклу	**Етап**	**Процес**					
		створення	**модернізація**	**модифікація**	**розвиток**	**адміністрування**	**забезпечення функціонування**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Ініціювання	...	...	...	...	...	...	...
	експертної оцінки інформації, вибору БПБ або ГПБ	**виконується**	**виконується**	**виконується**	**виконується**	**не застосовується**	**виконується**
	розроблення технічних вимог*	виконується	виконується	за потреби	за потреби	не застосовується	не застосовується
2. Проєктування	...	...	...	...	...	...	...
	оцінки ризиків	**виконується**	**виконується**	**виконується**	**виконується**	**не застосовується**	**не застосовується**
	розроблення ЦПБ	**виконується**	**за потреби**	**за потреби**	**за потреби**	**не застосовується**	**не застосовується**
3. Створення та впровадження	...	...	...	...	...	...	...
	розробки та впровадження заходів захисту (виконання вимог ЦПБ)	**виконується**	**за потреби**	**за потреби**	**за потреби**	**не застосовується**	**не застосовується**
	проведення попередніх випробувань засобу інформатизації або його компонентів*	виконується	виконується	за потреби	за потреби	не застосовується	не застосовується

Продовження таблиці

1	2	3	4	5	6	7	8
	...	...	...	...	...	...	...
	оцінювання дотримання вимог ЦПБ	**виконується**	**за потреби**	**за потреби**	**за потреби**	**не застосовується**	**не застосовується**
	включення системи до переліку авторизованих систем з безпеки	**виконується**	**виконується**	**виконується**	**виконується**	**не застосовується**	**не застосовується**
4. Промислова експлуатація	...	...	...	...	...	...	...
	постійного моніторингу безпеки	**виконується**	**виконується**	**виконується**	**виконується**	**виконується**	**виконується**
5. Виведення з промислової експлуатації	...	...	...	...	...	...	...
	виключення системи з переліку авторизованих систем з безпеки	**не застосовується**	**не застосовується**	**не застосовується**	**не застосовується**	**не застосовується**	**виконується**
	списання засобу інформатизації та/або його компонентів*	не застосовується	не застосовується	не застосовується	не застосовується	виконується	не застосовується
	...	...	...	...	...	...	...

Примітки:

1. Значення процесів наведених в А1

«**Застосовується**» – процес характерний для етапу, але може мати варіативність

«**Виконується**» – процес обов’язковий для відповідного етапу

«**Не застосовується**» – процес не передбачений на відповідному етапі

«**За потреби**» – виконується у випадках, передбачених проєктною документацією або нормативними вимогами

2. Етапи виконання вимог з безпеки повинні виконуватися до етапів життєвого циклу засобів інформатизації, наведених у таблиці.

БІБЛІОГРАФІЯ

1 Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»;

2 Постанова Кабінету Міністрів України від 18.12.2013 № 939 «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях»;

3 Постанова Кабінету Міністрів України від 19.10.2016 № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»;

4 Постанова Кабінету Міністрів України від 21.02.2025 № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»;

5 Постанова Кабінету Міністрів України від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;

6 ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

7 ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

8 ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT);

9 ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT);

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

11 ДСТУ EN ISO/IEC 29100:2022 Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (EN ISO/IEC 29100:2020, IDT; ISO/IEC 29100:2011, including Amd 1:2018, IDT);

12 НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;

13 НД ТЗІ 3.6-025-24 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;

14 NIST Special Publication 800-30. Rev.1. Guide for Conducting Risk Assessments, 2012;

15 NIST Special Publication 800-37. Rev.2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018;

16 NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View, 2011;

17 NIST Special Publication 800-53. Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020;

18 NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems, 2011;

19 NIST Special Publication 800-160 Vol. 1 Rev. 1. Engineering Trustworthy Secure Systems, 2022;

20 NIST Special Publication 800-160 Vol. 2 Rev. 1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, 2021.

СТД-02-002-2026-В

Коди згідно з КСД 001: 02.01
НК 004: 35.030

Ключові слова: технічний захист інформації, порядок виконання вимог з безпеки, інформаційні системи, електронні комунікаційні системи, інформаційно-комунікаційні системи, технологічні системи