НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.3-025-24

Том 1

Адміністрація Держспецзв'язку

Київ 2024

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Приватним акціонерним товариством "Інститут інформаційних технологій"

2 ПРИЙНЯТО НА НАДАНО ЧИННОСТІ: Адміністрацією Державної служби спеціального зв’язку та захисту інформації України

3 Цей нормативний документ розроблено згідно з правилами, установленими в національній стандартизації України

4 НА ЗАМІНУ НД ТЗІ 2.3-025-21

ЗМІСТ

ВСТУП

Цей НД ТЗІ розроблено з метою визначення методів оцінки заходів захисту визначених в НД ТЗІ 3.6-006-2024 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

НД ТЗІ 2.3-025-24
Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

Чинний від _____

1 Галузь використання

Цей НД описує систему дій щодо проведення оцінювання заходів захисту для інформаційних систем як окремий етап Порядку впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

Вимоги цього НД розповсюджуються на інформаційні, інформаційно-комунікаційні, електронні комунікаційні системи, що розгорнуті та експлуатуються державними органами та установами, органами місцевого самоврядування, а також на підприємствах та організаціях всіх форм власності (далі – Організації).

Оцінювання впроваджених заходів захисту є одним з етапів створення системи безпеки інформації (СБІ) в Організації.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі стандарти та нормативні документи:

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

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT);

НД ТЗІ 3.6-004-21 «Порядок впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці»;

НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»;

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 2.6-008-21 «Порядок авторизації безпеки інформаційних систем».

3 Визначення

У цьому НД ТЗІ подано терміни та визначення згідно із ДСТУ 3396.2, ДСТУ 2226, НД ТЗІ 1.1-003, а також НД ТЗІ 3.6-004-21.

4 Позначення та скорочення

У цьому НД використано такі позначення та скорочення:

БІ – Безпека інформації;

НД – Нормативний документ;

ПЗ – Програмне забезпечення;

ІКС – інформаційно-комунікаційна система

ІТ – Інформаційна технологія;

ЗЗ – Заходи захисту;

СБІ – система безпеки інформації;

ПВПД – «плануй-виконуй-перевіряй-дій» ;

ЦПБ – цільовий профіль безпеки.

5 Методологія оцінювання заходів захисту

5.1 Мета та завдання процедури оцінювання заходів захисту

Оцінювання впроваджених заходів захисту для інформаційних систем є одним з етапів розгортання системи безпеки інформації (СБІ) в Організації, що ґрунтується на моделі ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2015 (рисунок 5.1).

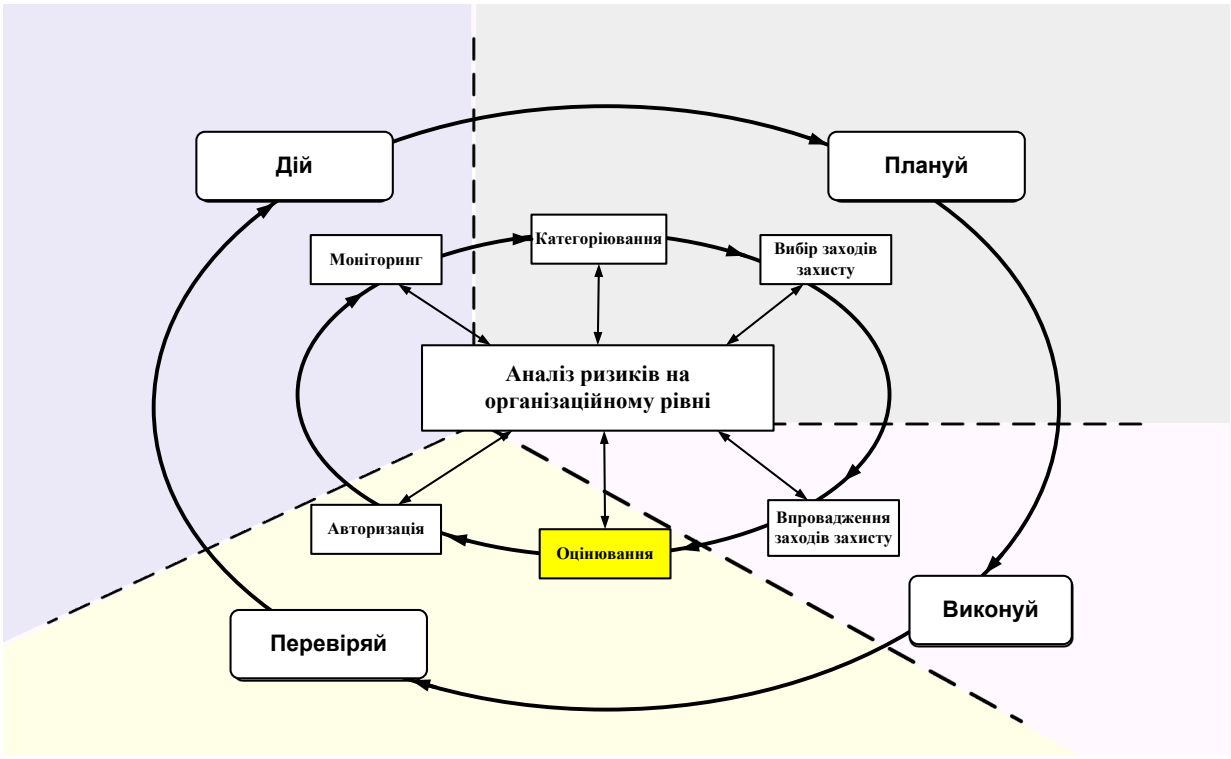


Рисунок 5.1 – Відповідність етапів впровадження СБІ моделі ISO/IEC 27001

Впровадження заходів захисту здійснюється у відповідності до розробленого та затвердженого ЦПБ, БІ та Планів захисту ЗЗ із застосуванням методики оцінювання, яка подається у цьому НД ТЗІ.

Метою оцінювання заходів захисту є підвищення рівня безпеки інформаційних систем на основі аналізу потенційних недоліків та вразливих точок, а також забезпечення економічної ефективності розгорнутих заходів захисту.

У таблиці 5.1 наведено короткий опис **завдань та очікуваних результатів етапу** оцінювання впроваджених заходів захисту.

Таблиця 5.1 – Завдання та результати оцінювання впроваджених заходів захисту

Завдання	Результати
Завдання О-1 Підготовка до оцінювання впроваджених заходів захисту в ІС	***Розроблений та затверджений*** План проведення оцінювання заходів захисту
Завдання О-2 Оцінювання впроваджених заходів захисту в ІС	***Проведене оцінювання*** відповідно до методики оцінювання та затвердженого плану. Оцінювачем сформульований висновок щодо результатів.
Завдання О-3 Документування звітів з оцінювання впроваджених заходів захисту в ІС	Звіт оцінювача ***задокументований та переданий*** Власнику (Розпоряднику) ІС.

Для забезпечення комплексності, всеосяжності та послідовності процедури оцінювання, а також для її економічної ефективності, організації мають прагнути розробити загально організаційну стратегію проведення процедури оцінювання. До важливих передумов розгортання такої загально організаційної стратегії відносяться налагоджені процеси категоріювання безпеки, а також процеси вибору та впровадження заходів захисту.

При впроваджені заходів захисту слід звертати увагу, що впровадження загально організаційних заходів заходу сприяє:

– зменшенню витрат на розробку, впровадження та оцінювання;

– централізації та автоматизації процесів оцінювання;

– узгодженості заходів захисту.

У випадках, коли архітектура системи не дозволяє розгортати загально організаційні заходи захисту, з метою забезпечення загально організаційної стратегії проведення оцінювання, необхідно організувати обмін інформацією щодо результатів оцінювання між відповідальними особами інформаційних систем, які входять до складу організації. Це забезпечить:

– можливість перегляду результатів оцінювання для всіх інформаційних систем організації, а також прийняття рішень, щодо розгорнутих заходів захисту на основі повних результатів оцінювання, що сприятиме зменшенню ризику для організації в цілому;

– формування більш глобального уявлення про слабкі місця та недоліки, що виникають в інформаційних системах, а також можливість розробити загально організаційні рішення щодо політики інформаційної безпеки організації;

– збільшення бази знань організації щодо загроз та вразливостей для більш економічно ефективних рішень загальних проблем безпеки інформації та приватності.

5.2 Методика оцінювання заходів захисту

5.2.1 Підготовка до оцінювання заходів захисту

Проведення оцінювання заходів захисту в сучасних умовах складних інфраструктур інформаційних технологій може бути складним та ресурсномістким процесом. Оцінювання заходів захисту може проводитися різними організаційними структурами, однак для успіху потрібна співпраця між усіма сторонами, котрі зацікавлені в забезпечені безпеки інформації в організації, включаючи власників інформаційних систем, постачальників засобів захисту, уповноважених осіб за забезпечення захисту інформації. Встановлення відповідного набору очікувань до, під час та після процесу оцінювання має першочергове значення для

досягнення прийнятного результату - тобто отримання інформації, необхідної для прийняття вмотивованих рішень, в тому числі, на основі оцінки ризиків.

Процес підготовки до оцінювання заходів захисту є важливим аспектом проведення ефективного оцінювання. Заходи, впроваджені на етапі підготовки, вирішують цілий ряд питань, що стосуються вартості, графіка та результатів оцінювання.

З організаційної точки зору процес підготовки до оцінювання заходів захисту включає такі ключові заходи:

– забезпечення того, щоб політика оцінювання заходів захисту була розроблена та зрозуміла всім задіяним відповідальним особам;

– забезпечення того, щоб усі етапи, які передбачені в процесі оцінювання заходів захисту були успішно виконані. А результати оцінювання кожної інформаційної системи, яка входить до складу організації були представлені на розгляд керівника організації;

– встановлення мети та обсягу оцінювання;

– забезпечення того, щоб загальні заходи захисту, а також загальна частина гібридних заходів захисту, були впроваджені в ІС організації, а також в ІС постачальників;

– інформування ключових організаційних посадових осіб про майбутнє оцінювання, а також виділення необхідних ресурсів для їх проведення;

– встановлення відповідних каналів комунікації між відповідальними за процес оцінювання посадовими особами різних інформаційних систем, які входять до складу організації;

– встановлення часових рамок для завершення процесу оцінювання та ключових етапів прийняття рішень, необхідних організації для ефективного управління оцінками;

– визначення та вибір компетентних оцінювачів / груп оцінювачів, які будуть відповідати за проведення оцінювання, а також розгляд питань щодо незалежності оцінювачів / груп оцінювачів;

– збір матеріалів, які нададуть можливість оцінити коректність реалізації;

– встановлення механізму взаємодії між організацією та оцінювачами та / або групами оцінювачів для мінімізації двозначності або непорозуміння щодо впровадження заходів захисту, а також слабких місць / недоліків.

На етапі підготовки оцінювачами / групами оцінювачів заходів захисту проводяться наступні дії:

– отримання загального розуміння діяльності організації (включаючи місію, функції та процеси) та те, як інформаційна система, яка є предметом конкретного процесу оцінювання, підтримує ці організаційні операції;

– отримання розуміння структури інформаційної системи (тобто архітектури системи) та впроваджених заходів захисту (включаючи системні, гібридні та загальні заходи захисту);

– визначення організаційних структур, відповідальних за розробку та впровадження загальних заходів (або загальної частини гібридних заходів);

– проведення зустрічей із відповідальними за процес оцінювання посадовими особами організації для забезпечення спільного розуміння цілей та глибини процесу оцінювання;

– збір матеріалів, які нададуть можливість оцінити коректність реалізації;

– отримання попередніх результатів оцінювання, які можуть бути використані для поточного оцінювання (наприклад, звіти, результати планових аудитів, звіти сканування вразливостей, результати тестування тощо);

– розробка плану оцінювання заходів захисту, які можуть бути інтегровані в один план або розроблені окремо.

5.2.2 Розробка плану оцінювання заходів захисту

План (плани) оцінювання заходів захисту має містити цілі оцінювання, а також детальну дорожню карту проведення оцінювання. Ці плани можуть бути розроблені як один інтегрований план або як окремі плани, залежно від організаційних потреб. На рисунку 5.2 зображені основні кроки розробки планів проведення оцінювання заходів захисту.

У таблиці 5.2 наведені основні завдання кожного із етапів підготовки планів оцінювання заходів захисту.

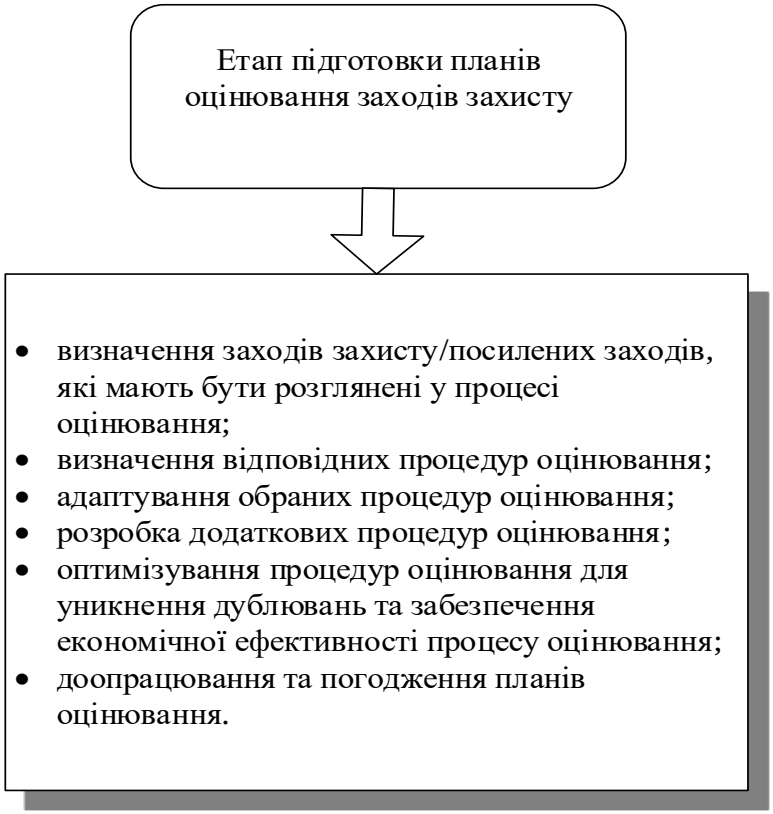


Рисунок 5.2 – Кроки розробки планів оцінювання заходів захисту

Таблиця 5.2 – Основні завдання етапів підготовки плану оцінювання заходів захисту

Назва етапу	Завдання етапу	Відповідальні особи
Визначення заходів захисту/посилених заходів, які мають бути розглянуті у процесі оцінювання	Аналіз плану (планів) захисту Визначення переліку розгорнутих (або таких, що плануються) заходів захисту Класифікація заходів захисту за типом (загальні, специфічні для організації, гібридні, успадковані) Визначення мети оцінювання для кожного заходу захисту	Оцінювач / група оцінювачів. Адміністратор безпеки або інша посадова особа, відповідальна за безпеку інформації.
Визначення відповідних процедур оцінювання	Визначення алгоритму проведення оцінювання	Оцінювач / група оцінювачів
Адаптування обраних процедур оцінювання	Обрання відповідних методик оцінювання Визначення об’єктів оцінювання Обрання значень атрибутів Визначення глибини оцінювання Визначення загальних заходів безпеки, які були оцінені раніше, а також (за необхідності) аналіз раніше проведених оцінок Розробка організаційних процедур оцінювання.	Оцінювач / група оцінювачів
Розробка додаткових процедур оцінювання	Розробка процедур оцінювання для специфічних для організації заходів захисту.	Оцінювач / група оцінювачів
Оптимізація процедур оцінювання для уникнення дублювань та забезпечення економічної ефективності	Перегляд обраних процедур оцінювання та за можливості їхньої комбінація для різних класів заходів захисту (наприклад організація загальних співбесід із ключовими організаційними посадовими особами, відповідальним за безпеку інформації) організація груп відповідних політик та процедур, які можуть розглядатися як єдине ціле	Оцінювач / група оцінювачів
Доопрацювання та погодження планів оцінювання	Встановлення графіку проведення процедур оцінювання Погодження графіку процедур оцінювання із відповідальними організаційними посадовими особами Перевірка плану проведення процедури оцінювання за критеріями повноти, актуальності, відповідності цілям оцінювання та економічної доцільності Погодження плану проведення процедури оцінювання із відповідальними організаційними посадовими особами	Оцінювач / група оцінювачів. Відповідальна організаційна посадова особа.

5.2.3 Процес оцінювання заходів захисту

Завданнями методики оцінювання заходів захисту є забезпечення послідовних оцінок заходів захисту з відтворюваними результатами, сприяння кращому розумінню ризиків для операцій та активів організації, приватних осіб, інших організацій, що виникають внаслідок функціонування та використання інформаційних систем, забезпечення економічної ефективності процесів оцінювання заходів захисту, а також створення повної, надійної інформаційної бази для підтримки рішень щодо управління ризиками, взаємності результатів оцінки, обміну інформацією та дотримання національного законодавства в галузі безпеки інформації.

Для реалізації зазначених завдань необхідно послідовна побудова схем алгоритмів та таблиць у відповідності до Каталогу заходів захисту, наведеному у НД ТЗІ, який визначає порядок вибору заходів захисту. Оцінкам підлягають всі впроваджені в інформаційній системі заходи захисту/посилені заходи захисту. Кожен захід захисту/посилений захід захисту розглядається окремо.

Загальний порядок оцінювання класу заходів захисту (рисунок 5.3) може бути представлена наступним чином:

1. Виділення групи заходів захисту у класі заходів захисту відповідно до нумерації в Каталозі заходів захисту;
2. Виділення заходу захисту (посиленого заходу захисту) в групі заходів захисту відповідно до нумерації в Каталозі заходів захисту;
3. Встановлення параметрів конкретного (посиленого) заходу захисту, якщо вони присутні;
4. Виділення завдань конкретного (посиленого) заходу захисту;
5. Виділення часткових заходів захисту, якщо вони наявні;
6. Встановлення параметрів часткових заходів захисту, якщо вони присутні;
7. Виділення завдань часткових заходів захисту;
8. Виділення характеристик часткових (посилених) заходів захисту, якщо вони присутні;
9. Виділення уточнених характеристик часткових (посилених) заходів захисту, якщо вони присутні.

Додаток А містить таблиці для реалізації методики оцінювання заходів захисту, які містяться в Каталозі.

Відповідно до Каталогу захід захисту може поділятися на часткові заходи захисту, які необхідні для більшої деталізації. Аналогічно, часткові/посилені заходи захисту можуть мати додаткові характеристики, а якщо це необхідно – уточнені характеристики. В процесі оцінювання оцінювачам / групам оцінювачів слід дотримуватися встановленої в Каталозі структури заходів захисту.

До параметрів конкретного (посиленого/часткового) заходу захисту, а також параметрів часткових заходів захисту можуть відноситися:

- встановлені організацією відповідно до діючих політик конкретні числові значення часових проміжків часу, протягом яких мають бути виконані обумовлені дії;
- конкретно задана частота проведення аудитів, перевірок, надання звітів тощо;
- визначені організацією посадові особи або ролі, відповідальні за конкретні дії щодо безпеки інформації;

– конкретно названі політики, процедури або умови, які впливають на реалізацію заходів захисту.

Такі параметри мають бути встановлені до моменту початку процедури оцінювання. Їхні значення обираються відповідно до діючих поточних політик безпеки інформації, а також планів захисту, впроваджених у організації. Параметри формулюють додаткові завдання заходів (посилених) захисту.

До завдань заходів (посилених/часткових) захисту відносяться конкретні дії, які потребують виконання в залежності від сфери дії (посиленого / часткового) заходу захисту та встановлених параметрів. Один захід (посилений / частковий) захисту може включати декілька завдань. Завдання заходів (посилених / часткових) захисту визначаються оцінювачем / групою оцінювачів в процесі оцінювання. Необхідно зазначити, що можливі випадки, коли завдання заходу захисту повністю відповідає його формулюванню, в такому разі оцінювач/ група оцінювачів можуть не виділяти завдання окремо.

На рисунку 5.4 наведено приклад реалізації методики для випадку другої групи заходів класу СА.

Реалізація (впровадження) заходів захисту відбувається у порядку, встановленим НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

Атворизація безпеки інформаційної системи відбувається в порядку, встановленим НД ТЗІ «Порядок авторизації безпеки інформаційних систем».

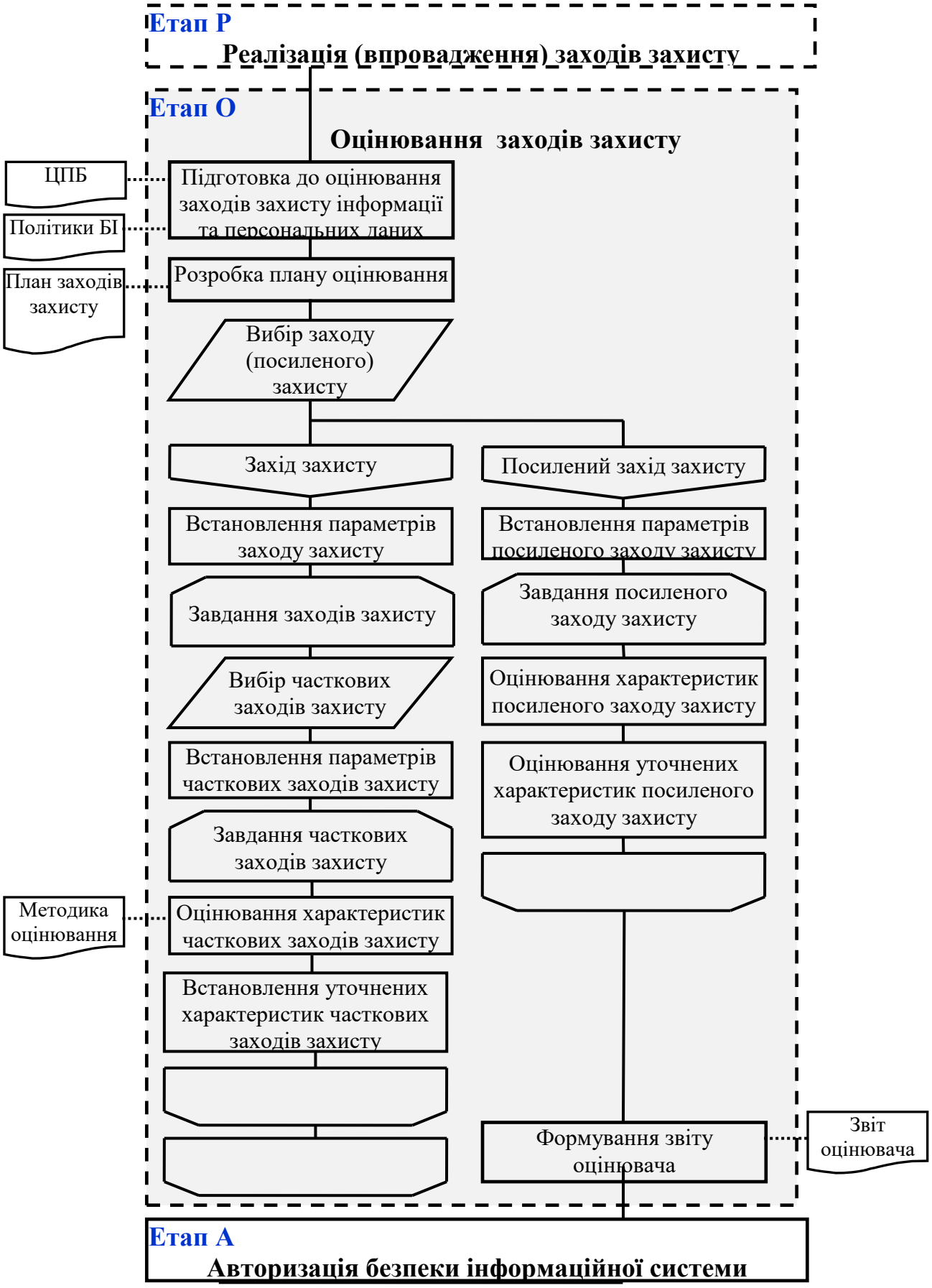


Рисунок 5.3 – Порядок проведення оцінювання заходу (посиленого) захисту

Рисунок 5.4 – Приклад реалізації методики для CA-2

Для зручності реалізації методології вводиться відповідна система маркування, яка містить обов'язкові та додаткові елементи (таблиця 5.3).

Таблиця 5.3 – Система маркування (елементи)

Тип	Зміст	Позначання	Обов'язковий/ додатковий
1	2	3	4
Клас заходів захисту	Складається із двох літер латинського алфавіту відповідно до Каталогу	Позначається без дужок	Обов'язковий елемент
Група заходів захисту всередині класу	Складається із порядкового номеру відповідно до Каталогу	Позначається без дужок	Обов'язковий елемент
Позначення посиленого заходу захисту	Складається із порядкового номеру посиленого заходу захисту відповідно до Каталогу	Позначається у круглих дужках	Додатковий елемент
Захід захисту	Складається із маленьких літер латинського алфавіту відповідно до Каталогу	Позначається у круглих дужках	Обов'язковий елемент

Закінчення таблиці 5.3

1	2	3	4
Завдання заходу захисту	Складається із порядкового номеру завдання в рамках заходу захисту визначеного оцінювачем/групою оцінювачів	Позначається у квадратних дужках	Додатковий елемент
Частковий захід захисту	Складається із порядкового номеру часткового заходу захисту відповідно до Каталогу	Позначається у круглих дужках	Додатковий елемент
Завдання часткового заходу захисту	Складається із порядкового номеру завдання в рамках часткового заходу захисту, визначеного оцінювачем/групою оцінювачів	Позначається у квадратних дужках	Додатковий елемент
Характеристики часткового заходу захисту	Складається із маленьких латинських літер відповідно до Каталогу	Позначається у круглих дужках	Додатковий елемент
Уточнені характеристики часткового заходу захисту	Складається із порядкового номеру уточненої характеристики, визначеного оцінювачем/групою оцінювачів	Позначається у квадратних дужках	Додатковий елемент

Завдання заходу захисту, завдання часткового заходу захисту та уточнені характеристики часткового заходу захисту можуть бути комбінацією двох або більше частин. У випадках, коли для надійної та коректної реалізації даних елементів достатньо впровадження не повного переліку складових частин, а, наприклад, однієї частини елементу, вона позначається у фігурних дужках.

В якості прикладу розглянемо процес оцінювання групи заходів захисту класу СА.

1. Обираємо групу заходів у класі – друга група.
2. Обираємо другий захід захисту (рисунок 5.5).
3. Конкретний захід захисту не потребує встановлення параметрів.
4. Виділяємо завдання конкретного заходу захисту (рисунок 5.5):

Розробити план оцінювання безпеки та приватності.

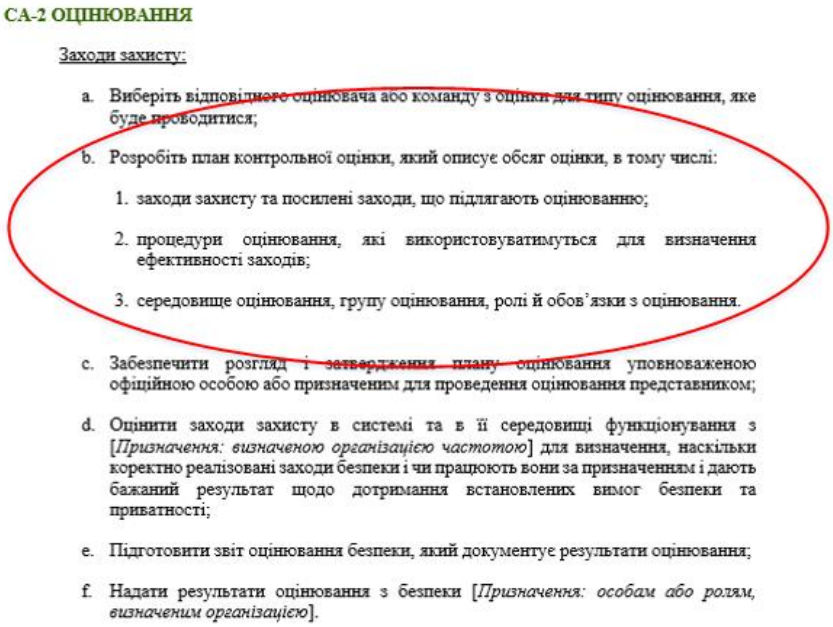
5. Відповідно до Каталогу виділяємо три часткові заходи захисту, які розкривають детальніше зміст заходу захисту (рисунок 5.6).
6. Параметри для часткових заходів захисту відсутні.
7. Завдання часткових заходів захисту відсутні.
8. Характеристики часткових заходів захисту відсутні.
9. Уточнені характеристики часткових заходів захисту відсутні.

Таким чином для першого заходу захисту в групі СА-2 можемо побудувати таблицю 5.4.

Таблиця 5.4 – Оцінювання першого заходу захисту в групі СА-2

СА-02	**ОЦІНЮВАННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	CA-02(b)[01]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи заходи захисту та посилені заходи, що підлягають оцінюванню.
	CA-02(b)[02]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи процедури оцінювання, які використовуватимуться для визначення ефективності заходів.
	CA-02(b)[03][01]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи середовище оцінювання.
	CA-02(b)[03][02]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи групу оцінювання.
	CA-02(b)[03][03]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи ролі й обов'язки з оцінювання.



CA-2 ОЦІНЮВАННЯ

Заходи захисту:

a. Виберіть відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися;

b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі:

1. заходи захисту та посилені заходи, що підлягають оцінюванню;
2. процедури оцінювання, які використовуватимуться для визначення ефективності заходів;
3. середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання.

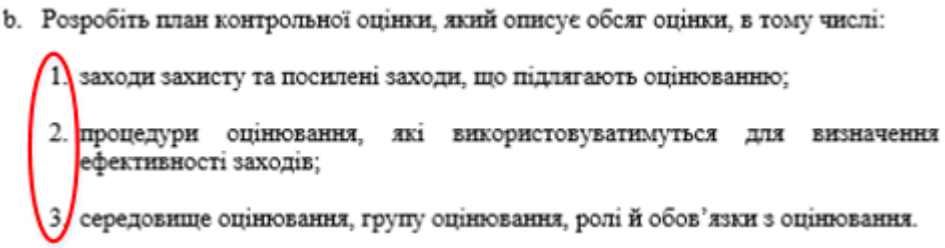
c. Забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником;

d. Оцінити заходи захисту в системі та в її середовищі функціонування з [*Призначення: визначеною організацією частотою*] для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності;

e. Підготовити звіт оцінювання безпеки, який документує результати оцінювання;

f. Надати результати оцінювання з безпеки [*Призначення: особам або ролям, визначеним організацією*].

Рисунок 5.5 – Вибір заходу захисту в групі



b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі:

1. заходи захисту та посилені заходи, що підлягають оцінюванню;
2. процедури оцінювання, які використовуватимуться для визначення ефективності заходів;
3. середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання.

Рисунок 5.6 – Виділення часткових заходів захисту

Після цього необхідно переходити до іншого заходу захисту. В рамках заходу захисту в групі CA-2, наприклад, перейдемо до заходу захисту d.

Виділяємо третій захід захисту в групі CA-2 (рисунок 5.7).

Встановлюємо параметр на рівні трьох місяців. Параметр формулює завдання:

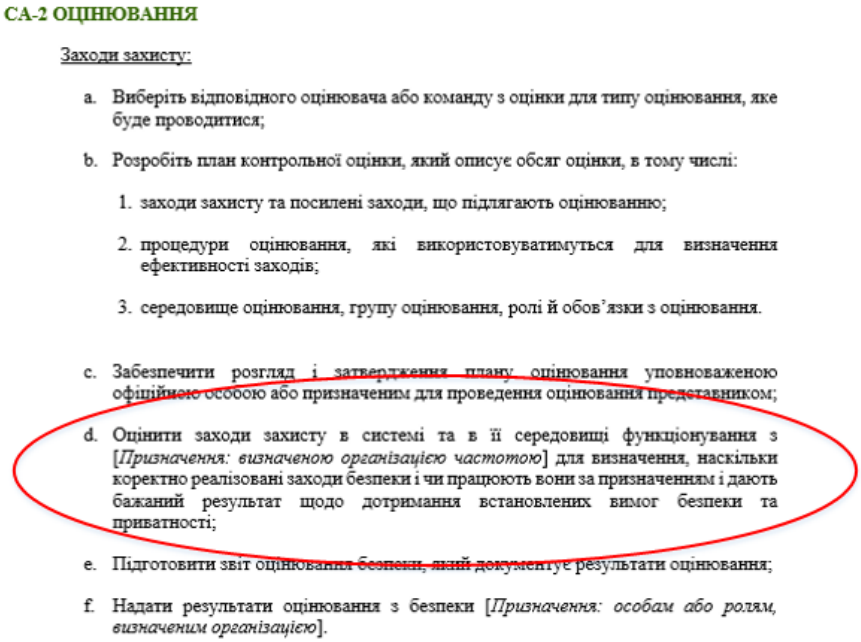
– [1] Визначити частоту оцінювання заходів захисту в системі;

– [2] Визначити частоту оцінювання заходів захисту в середовищі функціонування системи.

Виділяємо завдання конкретного заходу захисту:

– [3] Оцінити заходи захисту в системі;

– [4] Оцінити заходи захисту в середовищі функціонування системи.



CA-2 ОЦІНЮВАННЯ

Заходи захисту:

a. Виберіть відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися;

b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі:

1. заходи захисту та посилені заходи, що підлягають оцінюванню;
2. процедури оцінювання, які використовуватимуться для визначення ефективності заходів;
3. середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання.

c. Забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником;

d. Оцінити заходи захисту в системі та в її середовищі функціонування з [*Призначення: визначеною організацією частотою*] для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності;

e. Підготовити звіт оцінювання безпеки, який документує результати оцінювання;

f. Надати результати оцінювання з безпеки [*Призначення: особам або ролям, визначеним організацією*].

Рисунок 5.7 – Виділення наступного заходу захисту

При цьому, з Каталогу видно, що часткові заходи заходу відсутні. Таким чином, таблиця 5.3 доповнюється оцінюванням третього заходу захисту в групі CA-2 (таблиця 5.5).

Аналогічно оцінювач / група оцінювачів розглядає кожен впроваджений захід захисту. Захід захисту вважається коректно реалізованим, якщо повністю реалізовані всі його елементи.

В процесі оцінювання можуть бути використані наступні методи: дослідження, співбесіда або перевірка. Вибір методу та об'єктів залежить від конкретного заходу захисту. У таблиці 5.6 наведено приклади об'єктів та методи їх оцінювання.

Таблиця 5.5 – Оцінювання третього заходу захисту в групі CA-2

CA-02	**ОЦІНЮВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-02_ODP[01]	**визначено частоту, з якою слід оцінювати заходи захисту в системі та середовищі її функціонування;**
	CA-02(b)[01]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи заходи захисту та посилені заходи, що підлягають оцінюванню.

	CA-02(b)[02]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи процедури оцінювання, які використовуватимуться для визначення ефективності заходів.
	CA-02(b)[03][01]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи середовище оцінювання.
	CA-02(b)[03][02]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи групу оцінювання.
	CA-02(b)[03][03]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи ролі й обов'язки з оцінювання.
	CA-02(d)[01]	заходи захисту оцінюються в системі та середовищі її функціонування **<CA-02_ODP[01] частота оцінки>**, щоб визначити, наскільки коректно реалізовані заходи захисту, чи працюють вони за призначенням і чи дають бажаний результат щодо дотримання встановлених вимог до безпеки;
	CA-02(d)[02]	заходи захисту оцінюються в системі та середовищі її функціонування **<CA-02_ODP[01] частота оцінки>**, щоб визначити, наскільки коректно реалізовані заходи захисту, чи працюють вони за призначенням і чи дають бажаний результат щодо дотримання встановлених вимог до конфіденційності;

Таблиця 5.6 – Потенційні об'єкти та методи оцінювання

Метод оцінювання	Об'єкти	Коментар
Дослідження	Політики та процедури, проєктна та супутня документація, налаштування конфігурацій, журнали аудиту тощо	Оцінювач має ознайомитися та вивчити об'єкт та прийняти вмотивоване рішення щодо коректності реалізації відповідного заходу захисту. Рішення має бути відображене у звіті оцінювача.
Співбесіда	Відповідальні посадові особи та уповноважений персонал	Оцінювач може проводити співбесіди із залученими працівниками для кращого розуміння реалій впровадження заходів захисту. Рішення за результатами співбесіди має бути відображене у звіті оцінювача.
Перевірка	Автоматизовані механізми	Оцінювач проводить тестові випробування автоматизованих механізмів. розгорнутих для забезпечення реалізації заходів захисту. Результати тестування мають бути відображені у звіті оцінювача.

Результат оцінювання є позитивним у випадку коли в процесі оцінювання встановлена та підтверджена коректна реалізація кожного із впроваджених заходів захисту в ІС.

Методика оцінювання груп заходів захисту, які містяться у каталозі відповідно до положень НД ТЗІ, який визначає порядок вибору заходів захисту, наведено у додатках А та Б

цього НД ТЗІ.

5.2.4 Документування звітів з оцінювання впроваджених заходів захисту в ІС

Результати оцінювання заходів захисту оформлюються у вигляді Звіту. В такому Звіті повинні міститися результати оцінювання впроваджених заходів захисту із позначенням документів, які підтверджують коректну та повну реалізацію заходів захисту. Результати оцінювання заходів захисту впливають на подальшу їхню реалізацію, зміст планів заходів захисту. Власники інформаційних систем мають переглядати звіти про результати оцінювання заходів захисту, а також оновлену оцінку ризиків та за згодою призначених посадових осіб організації (наприклад, адміністратор безпеки) визначати відповідні кроки, необхідні для реагування на ті слабкі місця та недоліки, які були виявлені під час оцінки.

Після ознайомлення із результатними звіту про оцінювання заходів захисту, власники систем можуть вирішити, що певні висновки, є суттєвими, і вони вимагають негайних заходів з виправлення. І навпаки, проконсультувавшись із призначеними посадовими особами організації, можуть вирішити, що певні результати оцінки, мають несуттєвий характер і не становлять суттєвого ризику для організації.

Організація може залучати більше одного оцінювача / групи оцінювачів для проведення оцінювання. В такому випадку необхідне окреме проведення аналізу результатів оцінювання кожного оцінювача / групи оцінювачів.

Додаток А

В додатку А подається зміст НД ТЗІ 2.3-025-24 Том 2 та НД ТЗІ 2.3-025-24 Том 3.