

**НОРМАТИВНИЙ ДОКУМЕНТ**

**СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

**Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем**

**НД ТЗІ 3.6-007-21**

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Київ 2021

**НОРМАТИВНИЙ ДОКУМЕНТ**

**СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

|  |  |
| --- | --- |
|  |  ЗатвердженоНаказ Адміністрації Державної служби спеціального зв’язку тазахисту інформації України від " " 20 р. №  |

**Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем**

**НД ТЗІ 3.6-007-21**

Адміністрація Держспецзв'язку

Київ 2021

**ПЕРЕДМОВА**

1 РОЗРОБЛЕНО: Приватним акціонерним товариством "Інститут інформаційних технологій".

2. ВНЕСЕНО: Державною службою спеціального зв’язку та захисту інформації України.

УВЕДЕНО ВПЕРШЕ.

Цей документ не може бути повністю чи частково відтворений, тиражований і розповсюджений без дозволу Адміністрації Державної служби спеціального зв'язку та захисту інформації України

**ЗМІСТ**

[1 Галузь використання 1](#_Toc88130366)

[2 Нормативні посилання 1](#_Toc88130367)

[3 Визначення 1](#_Toc88130368)

[4 Позначення та скорочення 1](#_Toc88130369)

[5 Передумови впровадження заходів захисту 2](#_Toc88130370)

[5.1 Мета та завдання впровадження заходів захисту 2](#_Toc88130371)

[5.2 Порядок впровадження заходів захисту 3](#_Toc88130372)

[5.3 Рекомендації щодо налаштування базового (галузевого), уточнення та документування цільового профілю безпеки 7](#_Toc88130373)

[Додаток А 11](#_Toc88130374)

**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** |

Чинний від \_\_\_\_\_\_\_\_\_\_\_\_\_

# 1 Галузь використання

Цей нормативний документ (НД) визначає основи організації та порядок впровадження (реалізації) заходів захисту 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.

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

# 2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі закони, стандарти, політики, регламенти, директиви, інструкції 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 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»;

НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

# 3 Визначення

У цьому НД ТЗI подано терміни та визначення згідно із ДСТУ 3396.2, ДСТУ 2226, НД ТЗІ 1.1-003, а також НД ТЗІ, який описує 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.

# 4 Позначення та скорочення

У цьому НД використано такі позначення та скорочення:

БІ – Безпека інформації;

БПБ – Базовий профіль безпеки;

ГПБ – Галузевий профіль безпеки;

ЗЗ – Заходи захисту;

ІС – Інформаційна система;

НД – Нормативний документ;

ПВПД – Плануй – виконуй – перевіряй – дій;

ПД – Персональні дані;

СБІ – Система безпеки інформації;

ЦБП – Цільовий профіль безпеки;

SDLC – Життєвий цикл розробки IT-систем (System Development Life Cycle).

# 5 Передумови впровадження заходів захисту

## 5.1 Мета та завдання впровадження заходів захисту

Впровадження 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 (рис. 5.1).

Впровадження заходів захисту здійснюється у відповідності до розробленої Концепції безпеки інформації (БІ) та приватності із застосуванням методології проектування систем захисту інформації.

**Метою етапу** є впровадження (згідно з Концепцією безпеки інформації та приватності) заходів захисту, а також документування результатів впровадження заходів захисту у їх базовій конфігурації.

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

Відповідальність за впровадження заходів захисту покладається на Власника (Розпорядника) ІС. Безпосереднє виконання покладається на адміністратора безпеки або інших осіб, на яких покладено функції забезпечення безпеки інформації.



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

Таблиця 5.1 – Завдання та результати етапу впровадження (реалізації) заходів захисту

| Завдання | Результати |
| --- | --- |
| **Завдання Р-1**Налаштування обраного БПБ (ГПБ) | ***Встановлені параметри*** (часткові параметри) заходів захисту, характеристики часткових ЗЗ, уточнених характеристик.До БПБ (ГПБ) ***додані*** або ***виключені*** заходи захисту для актуалізації профілю безпеки відповідно до ІС |
| **Завдання Р-2**Уточнення цільового профілю безпеки | ***Проведено*** аналіз ризиків на системному рівні, результати аналізу задокументовані.***Встановлені параметри відкореговані*** |
| **Завдання Р-3**Затвердження розробленого цільового профілю безпеки | ЦПБ ***затверджений*** у встановленому порядку |
| **Завдання Р-4** Документування заходів захисту в затвердженому цільовому профілю безпеки | ***Розроблені***, ***затверджені*** та ***задокументовані*** Політики безпеки інформації та приватності |
| **Завдання Р-5**Встановлення (інсталяція), налагодження (конфігурування) засобів захисту ІС | ***Сформовані***, ***задокументовані*** та ***затверджені*** в порядку, встановленому в Організації, плани заходів захисту.***Встановлені*** засоби захисту ІС з налаштованою конфігурацією у відповідності до вимог політик безпеки, проектної та експлуатаційної документації. |
| **Завдання Р-6**Навчання користувачів ІС | ***Проведені*** навчання, тренування (в т.ч. підвищення кваліфікації) користувачів ІС |

## 5.2 Порядок впровадження заходів захисту

Впровадження заходів захисту здійснюється в порядку, який визначений на рисунку 5.2.

Вхідними даними для етапу впровадження заходів захисту виступають наступні дані. (перелік не є вичерпним):

1. Програма БІ та приватності ІС сформована на етапі вибору заходів захисту відповідно до НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».
2. БПБ (ГПБ) обраний на етапі вибору заходів захисту відповідно до НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».
3. Проектна документація на ІС.
4. Задокументована на Організаційному рівні стратегія управління ризиками.
5. Задокументовані результати оцінювання ризиків на Організаційному рівні.

Перелік вхідних даних не є вичерпним і може бути доповнений в разі необхідності для врахування особливостей ІС.

Для досягнення поставленої мети при проведенні процедур реалізації (впровадження) заходів захисту слід враховувати циклічний та комплексний характер виконання впровадження заходів захисту.

**Етап Р**

**Реалізація (впровадження)**

**заходів захисту**

**Етап О**

**Оцінювання заходів захисту**

Результати аналізу ризиків на Організаційному рівні

Програма БІ та приватності

Проектна документація на ІС

План заходів захисту

Аналіз ризиків на системному рівні

Навчання користувачів ІС

Встановлення (інсталяція), налагодження (конфігурування) засобів захисту ІС

**Етап В**

**Вибір заходів захисту**

Документування заходів захисту в затвердженому ЦПБ

БПБ (ГПБ)

Уточнений ЦПБ

Політики БІ

Затвердження цільового профілю безпеки

Визначення та впровадження заходу (посиленого) захисту

Встановлення параметрів заходу (посиленого) захисту

Встановлення параметрів часткових заходів захисту (за потребою)

Встановлення уточнених характеристик часткових заходів захисту (за потребою)

Вибір заходу (посиленого) захисту з БПБ

Налаштування базового (галузевого) профілю безпеки

Коригування встановлених параметрів (часткових параметрів) заходів захисту

Уточнення ЦБП

Рисунок 5.2 – Порядок реалізації (впровадження) заходів захисту

Вибір заходів захисту відбувається в порядку встановленим НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»

Оцінювання заходів захисту відбувається в порядку, встановленим НД ТЗІ «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»

До важливих передумов проведення впровадження заходів захисту організація повинна мати чітку загальну стратегію проведення процедури впровадження, яка повинна сприяти:

* зменшенню витрат на розробку, впровадження та оцінювання заходів захисту;
* централізації та автоматизації процесів впровадження заходів захисту;
* узгодженості заходів захисту.

Впровадження (Реалізація) заходів захисту відбувається в рамках моделі проектування ІС, яка була сумісно обрана Власником ІС (Розпорядником) та керівництвом Організації, до якої відноситься ІС. Впровадження (Реалізація) заходів захисту відбувається після узгодження між власником ІС (Розпорядником) та розробником (проектувальником) системи захисту інформації проектної документації на ІС.

Усі виконані дії щодо формування цільового профілю безпеки повинні документуватися відповідальними особами в частині, яка регулюється їхніми повноваженнями. За своїми ролями та впливом при виконанні на процеси уточнення цільового профілю безпеки усі особи можливо розподілити на наступні:

1. Власник ІС (Розпорядник).
2. Розробник (Проектувальник) системи захисту інформації. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як проектувальник системи безпеки, проектувальник системи приватності.
3. Постачальник послуг безпеки та засобів захисту. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як інженер з безпеки системи, інженер з приватності системи.
4. Адміністратор безпеки. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як службова особа з безпеки, службова особа з приватності, системний адміністратор.

5.2.1 Налаштування обраного базового (галузевого) профілю безпеки

Налаштування представляє собою циклічну реалізацію заходів захисту, що входять до складу визначених груп заходів захисту.

На першому етапі при виборі групи захисту потрібно визначитися з наявністю в ній з кількістю та переліком заходів захисту та посилених заходів захисту.

Цей вибір обумовлює послідовність дій щодо розгляду заходу захисту або посилені заходи захисту. Так, якщо буде обрано гілку в алгоритмі, спрямовану на визначення заходів захисту, то надалі слід розглянути параметри заходів захисту.

Заходи захисту мають змінні параметри, які необхідно визначити або обрати зі списку запропонованих під час налаштування профілю безпеки з урахуванням конкретних умов діяльності організації та застосування інформаційної системи, структурно-функціональних характеристик інформаційної системи, результатів аналізу ризиків безпеки. Цей механізм надає організаціям можливість налаштувати заходи захисту з урахуванням вимог безпеки та приватності конкретних зацікавлених сторін.

Для всіх параметрів заходів захисту (циклічно обираючи один за одним) проводиться вибір часткових заходів захисту. Розгляд часткових заходів захисту супроводжується формуванням в якості параметрів завдань часткових заходів захисту. У випадку, коли таких завдань декілька, то проводиться циклічно перегляд усіх завдань та оцінювання характеристик часткових заходів захисту й уточнених характеристик часткових заходів захисту. В наслідок цього, отримується два вкладених один в одного циклу. По завершенні циклу проводиться перехід до наступної групи класу заходів захисту.

У випадку, коли клас захисту має посилені заходи захисту, то в них завдання часткових заходів захисту відсутні. Тому надається можливість використати лише один цикл розгляду – безпосередньо по завданням посиленого заходу захисту.

5.2.2 Уточнення цільового профілю безпеки

Уточнення ЦПБ відбувається за результатами проведеного аналізу ризиків на системному рівні. Уточнення передбачає коригування встановлених параметрів (часткових параметрів) заходів захисту або зміну переліку впроваджених заходів захисту.

Для коректного уточнення ЦПБ на рівні ІС має бути проведений аналіз ризиків. Вибір методики аналізу ризиків покладається на Власника (Розпорядника) ІС та залежить від обраної Організацією стратегії управління ризиків. Вхідними даними для уточнення ЦПБ виступають:

* затверджена стратегія управління ризиками;
* задокументовані результати аналізу ризиків на Організаційному рівні;

обрана методика аналізу ризиків на системному рівні.

5.2.3 Затвердження цільового профілю безпеки

ЦПБ затверджується на рівні ІС, Організації, а також (за необхідності) на рівні уповноваженого органу з авторизації безпеки.

5.2.4 Документування заходів захисту в розробленому цільовому профілю безпеки

Порядок документування впроваджених заходів захисту встановлюється на рівні Організації та має відповідати вимогам чинного законодавства в галузі безпеки інформації. Рекомендації щодо документування надані в цьому НД ТЗІ, а також в НД ТЗІ, який описує 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.

5.2.5 Встановлення (інсталяція), налагодження (конфігурування) засобів захисту ІС

Інсталяція та налагодження заходів захисту відбувається у порядку встановленому у Організації та ІС. Результати документування відображаються у Планах ЗЗ.

Розроблення, оформлення та затвердження робочої та експлуатаційної документації на реалізовані заходи захисту для ІС та, у разі необхідності, її окремих складових частин, здійснюється по завершенню заходів. Робоча документація містить детальні щодо забезпечення управління ЦПБ і взаємодії його компонентів, а також документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань. Також, в разі необхідності на цьому етапі відбувається налаштування засобів захисту у відповідності до визначених вимог безпеки.

5.2.6 Навчання користувачів ІС

Порядок проведення тренувань та навчання (в т.ч. підвищення кваліфікації за необхідності) встановлюється на Організаційному рівні та на рівні ІС. Навчання проводиться користувачів ІС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами ІС та ін.) в частині, що їх стосується, основним положенням документів планів заходів захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, На цьому етапі також проводиться перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

## 5.3 Рекомендації щодо налаштування базового (галузевого), уточнення та документування цільового профілю безпеки

5.3.1 Загальні положення

Після вибору відповідного базового профілю безпеки необхідно здійснити його налаштування з метою узгодження заходів захисту з конкретними потребами організації щодо захисту інформації. Процес налаштування є елементом процесу управління ризиками організації. Рішення щодо визначення параметрів заходів захисту мають враховувати різни фактори управління ризиками безпеки.

Процес розробки цільового профілю безпеки може охоплювати такі дії:

• визначення загальних заходів захисту;

• визначення сфери застосування заходів захисту;

• вибір компенсаційних заходів захисту;

• присвоєння значень визначеним організацією параметрам заходів захисту;

• доповнення базового профілю безпеки додатковими заходами захисту та посиленими заходами захисту.

Ці рекомендації доцільно застосовувати організаціям у процесі управління ризиками безпеки для ухвалення рішення щодо налаштування та уточнення базових профілів безпеки з урахування результатів аналізу ризиків. Це дозволить також ухвалити економічно обґрунтовані рішення на основі результатів аналізу ризиків, що підтримують функції/завдання організації та потреби в захисті інформації. Не рекомендується довільно видаляти заходи захисту з базових (галузевих) профілів безпеки. Розробка цільового профілю безпеки має відповідати призначенню інформаційної системи та функцій/завдання організації, що підтримує інформаційна система.

Результати розробки цільового профілю безпеки документуються в політиці/політиках безпеки інформації системи. Кожний захід захисту, вибраний з базового (галузевого) профілю безпеки, обліковується. Якщо до цільового профілю безпеки вводяться нові заходи безпеки, їх обґрунтування вноситься до політики/політик безпеки інформації в системі, які затверджуються відповідальними посадовими особами.

Документування рішень щодо управління ризиками в процесі розробки цільового профілю безпеки є обов’язковим. Посадові особи повинні мати необхідну інформацію для ухвалення достовірних рішень на основі ризику безпеки та приватності. Ухвалення таких рішень має бути прозорим і підзвітним.

5.3.2. Визначення загальних заходів захисту

Загальні заходи захисту — це заходи захисту, які можуть бути успадковані однією чи декількома інформаційними системами організації. Якщо система успадковує загальний захід захисту, немає потреби здійснювати управління цим заходом у цій системі. Функцію безпеки чи приватності забезпечує або інша система, або інша організація. Організаційні рішення, щодо яких захід захисту позначається як загальний захід, можуть впливати на обов’язки власників системи щодо впровадження заходів захисту. Вибір загального заходу захисту може також вплинути на видатки ресурсів організації. Тобто чим більша кількість впроваджених загальних заходів захисту, тим більша потенційна економія витрат, оскільки заходи захисту амортизуються в багатьох інформаційних системах.

5.3.3 Сфера застосування заходів захисту

Рішення щодо сфери застосування заходів захисту, разом з рішеннями щодо управління ризиками, забезпечують організації додаткову інформацію для ухвалення рішень щодо застосування заходів захисту. Це дозволить обґрунтувати вилучення заходів захисту з базового профілю безпеки й вибирати лише ті заходи захисту, які необхідні для забезпечення відповідного рівня захисту. Організації можуть застосовувати описані нижче рекомендації щодо визначення сфери застосування заходів захисту в процесі ухвалення рішень на основі ризику щодо вибору та специфікації заходів захисту.

1. Рекомендації щодо впровадження, застосування та розміщення заходів захисту

Складність інформаційних систем, що постійно зростає вимагає ретельного аналізу способів і методів впровадження заходів захисту. Заходи захисту, що внесені до базового (галузевого) профілю безпеки, можуть не застосовуватися до кожного компонента системи. Заходи захисту застосовуються лише до тих компонентів системи, які забезпечують або підтримують функції безпеки чи приватності. Організації ухвалюють явні, засновані на оцінюванні ризику рішення про те, де застосовувати чи розподіляти заходи захисту в інформаційних системах для досягнення необхідної функції або можливостей безпеки чи приватності та задоволення конкретних вимог безпеки та приватності.

2) Рекомендації щодо операційного та робочого середовища

Впровадження окремих засобів захисту базового (галузевого) профілю безпеки висувають умови до операційного та робочого середовищ. Якщо ці умови не можуть бути виконані, доцільно уточнити заходи захисту базового профілю та пристосувати умови впровадження заходу захисту до наявних умов операційного та робочого середовищ. Прикладами таких обмежень операційних/робочих середовищ є: використання мобільних пристроїв; однокористувацькі системи; системи радіозв’язку; системи, що мають дуже обмежену пропускну здатність, наприклад, тактичні системи, що підтримують функції військових чи правоохоронних органів; кіберфізичні системи, датчики та пристрої; системи з обмеженою функціональністю або компоненти системи, такі як факсимільні машини, принтери, сканери, смартфони, планшети, електронні зчитувачі та цифрові камери; системи, що обробляють, зберігають або передають нестійку інформацію, або системи, що використовують методи віртуалізації для встановлення нестійких даних про операційні системи та програми; відкриті системи.

3) Рекомендації щодо технічної реалізації

Заходи захисту, що належать до конкретних технологій, наприклад, бездротова мережа, криптографія та інфраструктура відкритих ключів, застосовуються лише в тому разі, якщо ці технології використовуються або є вимога щодо їх використання в інформаційних системах організації. Заходи захисту, які можуть ефективно підтримуватися автоматизованими механізмами (технічними засобами), не вимагають розробки механізмів, якщо таких механізмів ще немає або вони не є доступними в комерційних чи сертифікованих продуктах. Якщо автоматизовані механізми недоступні, доцільно впроваджувати компенсаційні заходи захисту, які можуть бути реалізовані за допомогою неавтоматизованих механізмів або процедур.

4) Рекомендації щодо врахування призначення, функцій і завдань організації

Певні заходи захисту можуть виявитися недоцільними, якщо їх упровадження в системі чи компоненті системи можуть погіршувати, послаблювати чи іншим чином ускладнювати виконання функцій і завдань організації, включно із загрозою або заподіянням шкоди особам. Рішення щодо доцільності впровадження таких заходів захисту треба ухвалювати, враховуючи будь-які законодавчі, нормативні чи політичні вимоги.

5.3.4 Вибір компенсаційних заходів захисту

Компенсаційні заходи захисту застосовуються організаціями замість конкретних заходів захисту базового (галузевого) профілю безпеки. Це відбувається, коли заходи захисту необхідні та важливі для зниження ризику, але їх впровадження неможливе. Компенсаційний захід захисту вибирається найчастіше тоді, коли реалізація заходу захисту з базового профілю безпеки технічно неможлива, нерентабельна або реалізація негативно впливає на організаційні функції. Компенсаційні заходи захисту часто є тимчасовими до оновлення інформаційної системи. Компенсаційні заходи захисту призначені для забезпечення рівноцінного або порівняльного захисту систем, організацій і осіб. Компенсаційні заходи вибираються після визначення сфери застосування заходів захисту в процесі налаштування базового (галузевого) профілю безпеки.

Компенсаційні заходи захисту можуть вибиратися за такими правилами:

- організація вибирає компенсаційний захід захисту з каталогу заходів захисту цього нормативного документа, якщо відповідні компенсаційні заходи захисту відсутні, організація вибирає відповідні компенсаційні заходи захисту з інших джерел;

- організація надає обґрунтування того, яким чином компенсаційний захід захисту забезпечує належні функції безпеки або приватності та чому захід захисту з базового (галузевого) профілю не може бути здійснений;

- організація оцінює і приймає ризик безпеки та приватності, який пов’язано з упровадженням компенсаційного заходу захисту.

5.3.5 Призначення значень параметрів заходів захисту

Заходи захисту, що містять вбудовані параметри (тобто призначення та вибір), дають організаціям можливість визначати їх значення для підтримки конкретних організаційних вимог. Після визначення сфери застосування та вибору компенсаційних заходів захисту здійснюється перегляд заходів захисту для визначення параметрів.

Обґрунтування конкретних значень параметрів заходів захисту здійснюється з урахування таких факторів:

* вимог чинного законодавства, нормативних документів, директив, правил, політик безпеки, стандартів, кращих галузевих практик;
* призначення, функцій і завдань організації та інформаційної системи.

Значення параметрів можуть також визначатися місією або бізнес-вимогами.

Після визначення значень параметрів заходів захисту, вони стають постійною частиною заходів захисту, задокументуються в планах захисту інформації. Організації можуть визначати значення параметрів перед вибором компенсаційних заходів захисту, оскільки специфікація параметрів завершує визначення заходу захисту й може впливати на вимоги до компенсаційних заходів захисту. Співпраця також надає переваги щодо визначення значень параметрів заходів захисту. Для організацій, які часто працюють разом, може бути корисним розробити взаємоприйнятний набір однакових значень для параметрів заходів захисту.

5.3.6 Уточнення цільового профілю безпеки

Визначення того, які заходи захисту необхідні для забезпечення адекватної безпеки інформаційних систем і організації, захисту персональних даних, є функцією оцінювання ризиків організації. У певних ситуаціях для усунення конкретних загроз організаціям, функціям/процесам та інформаційним системам потрібні додаткові заходи захисту, крім тих заходів захисту, що внесені до базових (галузевих) профілів безпеки. Оцінювання ризику надає важливу інформацію для визначення необхідності та достатності заходів захисту в базових профілях безпеки. Організаціям рекомендується максимально використовувати каталог заходів захисту, щоб доповнити свої цільові профілі безпеки додатковими заходами захисту.

5.3.7. Надання додаткової технічної інформації для впровадження заходів захисту

Оскільки заходи захисту є абстрактними заявами про функції чи можливості безпеки або приватності, можуть виникати ситуації, коли не вистачає інформації для реалізації (впровадження) заходів захисту. Отже, можуть знадобитися додаткові деталі, щоб повністю визначити мету заходу захисту для цілей реалізації та гарантування, що вимоги безпеки та приватності, пов’язані з цим заходом захисту, задоволені. Наприклад, додаткова інформація може містити уточнення деталей реалізації, уточнення сфери застосування або ітерацію для застосування одного й того ж заходу захисту по-різному до різних сфер застосувань. Така ситуація виникає зазвичай, коли заходи захисту використовуються в процесі проєктування системи як частина вимог до розробки. Організації забезпечують надання такої інформації, якщо наявної інформації недостатньо для визначення передбачуваного застосування заходу захисту. При наданні додаткової інформації організаціям рекомендується не змінювати призначення заходу захисту та не змінювати шаблон надання заходу захисту. Додаткова інформація про реалізацію надається в розділі «Рекомендації з реалізації» та документується в планах захисту інформації.

# Додаток А

**Моделювання процесу впровадження (реалізації) заходів захисту**

Процедуру впровадження (реалізації) заходів захисту можливо зобразити в нотації стандарту Business Process Management Notation (BPMN), кий дозволяє моделювати процеси у вигляді послідовності елементарних дій (рис. А.1) з метою демонстрування можливого розподілу ролей на даному етапі.

В режимі моделювання Bizagi Modeler дозволяє здійснити чотири види аналізу: валідності послідовності процесів; процесів за часовими показниками; за розподілом ресурсів та за графіком. Така симуляція дозволить виявити помилки, зациклення, зайві розгалуження тощо. Так на рисунку А.2 показано, що були згенеровані умовні замовлення на обробку, які всі були оброблені та надійшли до фінішної вершини.



Рисунок А.1 – Порядок реалізації (впровадження) заходів захисту в нотації BPMN



Рисунок А.2 – Приклад моделювання реалізації (впровадження) заходів захисту в нотації BPMN