УДК 004.056 **DOI:10.30837/rt.2024.2.217.01**

О.В. ПОТІЙ, д-р техн. наук, Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук,
Ю.К. ВАСИЛЬЄВ, М.В. ЄСІНА, канд. техн. наук

ПРОЦЕС ДЕКЛАРУВАННЯ ПРОФІЛІВ БЕЗПЕКИ ІНФОРМАЦІЇ

Вступ

Нові виклики у сфері захисту інформації та кібербезпеки вимагають від держави та власників інформаційних активів застосовувати нові технології захисту з метою підвищення ефективності впровадження та використання засобів захисту. Тому на сьогодні з'явилась нагальна потреба у модернізації вітчизняної нормативної бази у сфері захисту інформації. Модернізація нормативної бази має проводитися у напрямку гармонізації з міжнародними стандартами, а також враховувати досвід світових лідерів у цій галузі – ЄС та США.

По суті, дана робота розглядає процес реалізації експериментального проєкту з декларування відповідності комплексних систем захисту інформації (КСЗІ) в інформаційних (ІС), електронних комунікаційних та інформаційно-комунікаційних системах (ІКС), створених з використанням профілів безпеки інформації. Особливістю подання матеріалу є застосування процесного підходу щодо розкриття нормативно-правових документів, що регламентують проведення експериментального проєкту з декларування відповідності КСЗІ з використанням профілів безпеки інформації.

Вважаємо, що актуальними та необхідними питаннями, які розглянуті в статті, будуть питання надання навчально-методичної допомоги власникам (розпорядникам) систем, які в умовах ведення війни з російською федерацією готові взяти на себе відповідальність за ефективність реалізованих заходів захисту ІС, ІКС, що знаходяться під їхньою експлуатацією.

1. Аналіз стандартів, на яких побудовані системи захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах

На сьогодні для забезпечення безпеки інформації, що оброблюється у системі, зазвичай застосовуються комплексні системи захисту інформації (КСЗІ), системи управління інформаційною безпекою (СУІБ) [1] та системи безпеки інформації (СБІ) [2]. Також можна використовувати вимоги та рекомендації до забезпечення безпеки інформації, що надає NIST SP 800-53 [3]. Також розроблений інший підхід до захисту інформації, що засновується на використанні базових профілів безпеки (БПБ) [4].

Безумовно, кожен з цих підходів до забезпечення безпеки інформації має свої переваги та недоліки. Проведені авторами статті дослідження дозволили проаналізувати та зробити висновки щодо переваг, недоліків та можливостей застосування кожного з підходів до забезпечення безпеки інформації.

Створення КСЗІ є важливим кроком для забезпечення безпеки даних та відповідності законодавству, але потребує значних ресурсів та кваліфікації для ефективного впровадження та підтримки.

Створення КСЗІ має свої переваги та недоліки, які варто враховувати під час прийняття рішення щодо їх впровадження [5].

До переваг можна віднести наступне:

1. Підвищений рівень безпеки: КСЗІ забезпечують багаторівневий захист від різноманітних загроз, таких як віруси, атаки хакерів, витоки інформації та інші кіберзагрози.

2. Відповідність законодавству: впровадження КСЗІ допомагає організаціям відповідати вимогам національного та міжнародного законодавства щодо захисту інформації.

3. Захист конфіденційних даних: КСЗІ дозволяють забезпечити конфіденційність і цілісність критично важливої інформації, що знижує ризики втрати або викрадення даних.

4. Безперервність бізнесу: завдяки захищеній інфраструктурі зменшуються ризики простоїв і втрати даних, що сприяє безперервності та стабільності бізнес-процесів.

5. Підвищення довіри клієнтів і партнерів: наявність сертифікованої системи захисту інформації підвищує довіру клієнтів і партнерів, що може бути конкурентною перевагою на ринку.

До недоліків можна віднести:

1. Високу вартість впровадження та підтримки: розробка, впровадження та підтримка КСЗІ можуть бути досить витратними, особливо для малих та середніх підприємств.

2. Складність управління: управління КСЗІ вимагає високого рівня кваліфікації персоналу, що може бути викликом для компаній, які не мають відповідних ресурсів.

3. Зниження продуктивності: деякі засоби захисту можуть впливати на продуктивність систем, уповільнюючи роботу користувачів і процесів.

4. Необхідність регулярного оновлення: КСЗІ потребують регулярного оновлення для захисту від нових загроз, що вимагає додаткових витрат та зусиль.

5. Потенційні проблеми з інтеграцією: інтеграція КСЗІ з існуючими системами може бути складною і вимагати значних зусиль для забезпечення сумісності та коректної роботи.

Створення та застосування СУІБ є важливим для забезпечення комплексного захисту інформації та відповідності нормативним вимогам. Проте, процес впровадження та підтримки таких систем може бути складним та затратним, що вимагає ретельного планування та наявності відповідних ресурсів [1].

СУІБ є важливими для захисту даних та забезпечення безпеки інформаційних активів організацій. Розглянемо переваги та недоліки створення та застосування таких систем.

Переваги:

1. Системний підхід до безпеки: СУІБ дозволяють систематизувати та стандартизувати процеси управління безпекою інформації, що сприяє більш ефективному виявленню та реагуванню на загрози.

2. Відповідність стандартам та нормативним документам: впровадження СУІБ допомагає організаціям відповідати міжнародним стандартам, наприклад, таким як ISO/IEC 27001, та вимогам місцевого законодавства, що може бути критичним для багатьох галузей.

3. Зниження ризиків: СУІБ дозволяють ідентифікувати, оцінювати та управляти ризиками, що знижує ймовірність виникнення інцидентів інформаційної безпеки.

4. Покращення репутації: наявність сертифікованої СУІБ підвищує довіру клієнтів, партнерів та акціонерів до компанії, покращуючи її імідж на ринку.

5. Підвищення ефективності бізнес-процесів: інтеграція СУІБ може сприяти оптимізації бізнес-процесів та покращенню управління інформаційними активами.

6. Забезпечення безперервності бізнесу: СУІБ допомагають забезпечити стійкість організації до інцидентів та аварійних ситуацій, що сприяє безперервності бізнесу.

Недоліки:

1. Висока вартість впровадження та підтримки: створення та підтримка СУІБ можуть бути дорогими, що може бути суттєвим викликом для малих та середніх підприємств.

2. Складність впровадження: процес впровадження СУІБ може бути складним і вимагати значних зусиль та часу для адаптації існуючих процесів та навчання персоналу.

3. Необхідність постійного моніторингу та оновлення: СУІБ потребують регулярного моніторингу, аудиту та оновлення для забезпечення актуальності та ефективності, що потребує додаткових ресурсів.

4. Складність управління змінами: впровадження нових політик та процедур може зустріти опір з боку персоналу, що потребує додаткових зусиль для управління змінами та навчання.

5. Зниження гнучкості: деякі компанії можуть виявити, що суворе дотримання політик та процедур СУІБ знижує гнучкість і швидкість реагування на нові бізнес-можливості.

6. Високі вимоги до кваліфікації персоналу: ефективне управління СУІБ вимагає високого рівня кваліфікації та спеціалізованих знань, що може бути викликом для деяких організацій.

Створення та застосування СБІ відповідно до НД ТЗІ 3.6-004-21 є важливим для забезпечення захисту інформації та відповідності законодавчим вимогам. СБІ передбачає комплекс організаційних, технічних, програмних та інших заходів для захисту інформації. Процес впровадження та підтримки таких систем може бути складним та затратним, що потребує ретельного планування та наявності відповідних ресурсів [2].

Розглянемо переваги та недоліки створення та застосування такої системи.

Переваги:

1. Відповідність законодавчим вимогам: впровадження СБІ дозволяє організаціям відповідати вимогам національного законодавства щодо захисту інформації, що є обов'язковим для державних та деяких приватних структур.

2. Комплексний підхід до безпеки: НД ТЗІ 3.6-004-21 описує комплекс заходів, що включають організаційні, технічні, програмні та інші аспекти безпеки, забезпечуючи всебічний захист інформації.

3. Систематизація процесів безпеки: впровадження СБІ дозволяє систематизувати процеси безпеки інформації, що сприяє більш ефективному управлінню ризиками та реагуванню на загрози.

4. Підвищення довіри клієнтів та партнерів: наявність сертифікованої СБІ підвищує довіру до організації з боку клієнтів, партнерів та інших зацікавлених сторін.

5. Захист від різноманітних загроз: НД ТЗІ 3.6-004-21 включає заходи для захисту від різноманітних загроз, включаючи кібератаки, витоки інформації та ін.

6. Підвищення загального рівня безпеки: впровадження заходів, описаних у документі, допомагає підвищити загальний рівень інформаційної безпеки в організації, знижуючи ризики втрат інформації.

Недоліки:

1. Висока вартість впровадження: комплексний підхід до безпеки може вимагати значних фінансових витрат на закупівлю обладнання, програмного забезпечення та навчання персоналу.

2. Складність впровадження: впровадження СБІ може бути складним процесом, що вимагає значного часу та ресурсів, особливо для великих організацій.

3. Необхідність постійного моніторингу та оновлення: СБІ потребує регулярного моніторингу, аудиту та оновлення для забезпечення актуальності та відповідності новим загрозам, що вимагає додаткових ресурсів.

4. Зниження гнучкості бізнес-процесів: впровадження суворих заходів безпеки може знижувати гнучкість бізнес-процесів, уповільнюючи реакцію на зміни ринкових умов або нові бізнес-можливості.

5. Високі вимоги до кваліфікації персоналу: управління та підтримка СБІ вимагають високого рівня кваліфікації та спеціалізованих знань, що може бути проблемою для деяких організацій.

6. Потенційні проблеми з інтеграцією: інтеграція нових систем безпеки з існуючими інформаційними системами може бути складною і вимагати додаткових зусиль для забезпечення сумісності та коректної роботи.

Застосування та реалізація вимог NIST SP 800-53 rev. 5 можуть значно підвищити рівень безпеки інформаційних систем і управління ризиками в організації. NIST SP 800-53 rev. 5 є важливим документом для забезпечення безпеки інформаційних систем і мереж. Він описує контрольні заходи та процедури для оцінки ефективності систем управління безпекою

інформації. Але його процес впровадження може бути складним і витратним, що потребує ретельного планування, наявності кваліфікованого персоналу та достатніх ресурсів [3].

Розглянемо переваги та недоліки застосування та реалізації вимог цього документа на практиці.

Переваги:

1. Комплексний підхід до безпеки: документ охоплює широкий спектр контрольних заходів і процедур для забезпечення всебічного захисту інформаційних систем, включаючи технічні, організаційні, адміністративні та фізичні аспекти.

2. Відповідність міжнародним стандартам: NIST SP 800-53 rev. 5 базується на міжнародно визнаних практиках і стандартах, що допомагає організаціям відповідати вимогам міжнародного ринку та регуляторів.

3. Гнучкість і адаптивність: документ пропонує гнучкий підхід до впровадження контрольних заходів, що дозволяє адаптувати їх до специфічних потреб і умов кожної організації.

4. Підвищення рівня безпеки: виконання вимог NIST SP 800-53 rev. 5 підвищує загальний рівень безпеки інформаційних систем, знижуючи ризики інцидентів безпеки та витоку даних.

5. Покращення процесів управління ризиками: документ допомагає організаціям краще ідентифікувати, оцінювати та управляти ризиками, що сприяє більш ефективному захисту інформаційних активів.

6. Підвищення довіри клієнтів і партнерів: дотримання вимог NIST SP 800-53 rev. 5 підвищує довіру клієнтів і партнерів до організації, покращуючи її репутацію та конкурентоспроможність на ринку.

Недоліки:

1. Високі витрати на впровадження: реалізація вимог документа може бути дорогим процесом, що включає закупівлю обладнання, програмного забезпечення та навчання персоналу.

2. Складність впровадження: впровадження контрольних заходів NIST SP 800-53 rev. 5 може бути складним процесом, що вимагає значних зусиль і ресурсів, особливо для організацій з обмеженими можливостями.

3. Високі вимоги до кваліфікації персоналу: ефективне впровадження та підтримка вимог документа вимагають високого рівня кваліфікації та спеціалізованих знань від персоналу.

4. Часові витрати: процес впровадження вимог NIST SP 800-53 rev. 5 може зайняти багато часу, що може впливати на загальну продуктивність організації.

5. Потенційна бюрократизація процесів: виконання детальних вимог і процедур може призвести до збільшення бюрократичних процесів в організації, що може уповільнити прийняття рішень і реалізацію проєктів.

6. Необхідність постійного моніторингу та оновлення: вимоги документа потребують регулярного моніторингу та оновлення для забезпечення актуальності та відповідності новим загрозам, що вимагає додаткових ресурсів.

2. Нормативно-правові акти щодо декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації

Нормативні документи (НД) системи технічного захисту інформації (ТЗІ), на яких ґрунтується КСЗІ, визначають процес створення певного підґрунтя для власників ІС, електронних комунікаційних та ІКС. Така система забезпечує власників ІС, електронних комунікаційних та ІКС чітким механізмом та допомагає в його реалізації. Вихідним документом, що регламентує порядок впровадження експериментального проєкту з декларування є Постанова Кабінету Міністрів України від 30.05.2024 № 627 (рис. 1) [4].

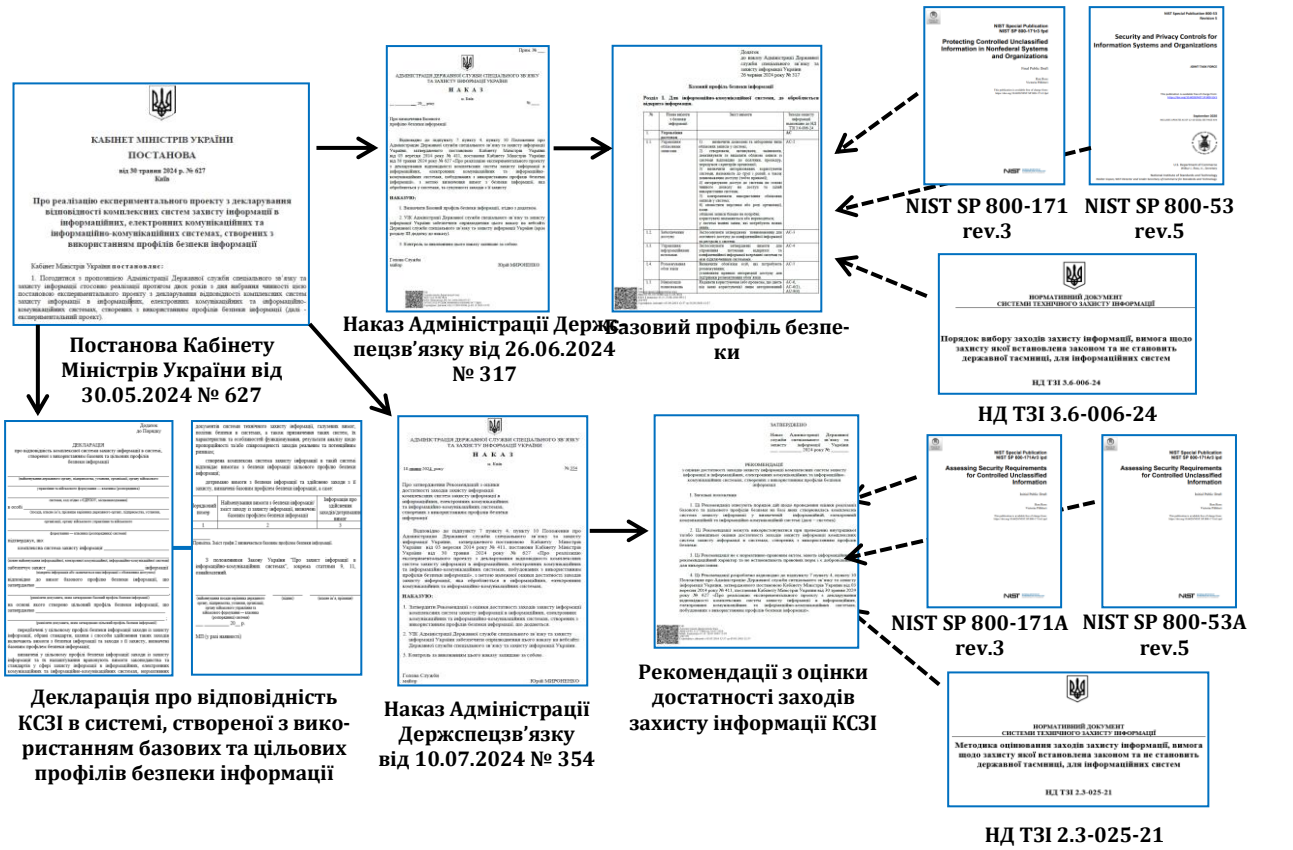

Рис. 1. Нормативно-правові акти щодо реалізації проєкту з декларування відповідності КСЗІ в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації

Метою експериментального проєкту є підвищення рівня захисту державних інформаційних ресурсів (ДІР) та інформації, вимога щодо захисту якої встановлена законом, оптимізація процесу державної експертизи та підтвердження відповідності комплексних систем захисту інформації в системах.

Новий проєкт дозволить децентралізувати та спростити процеси оцінки та впровадження КСЗІ, підвищити відповідальність власника (розпорядника) системи. Нормативно-правові акти, що розроблені в рамках проєкту, враховують положення:

- посібника із заходів безпеки та приватності для інформаційних систем і організацій (NIST SP 800-53 rev. 5: Security and Privacy Controls for Information Systems and Organizations [3]), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);
- методології та набору процедур для проведення оцінки засобів захисту та конфіденційності, які застосовуються в системах і організаціях у рамках ефективного управління ризиками (NIST SP 800-53A rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations [6]);
- посібника із захисту контрольованої несекретної інформації в нефедеральних системах і організаціях (NIST SP 800-171 rev. 3. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [7]);
- процедури оцінки та методології, які можна використовувати для проведення оцінки вимог безпеки в спеціальній публікації NIST 800-171 (NIST SP 800-171A rev. 3. Assessing Security Requirements for Controlled Unclassified Information [8]);
- порядку вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 3.6-006-24 [9]);

- методики оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 2.3-025-24 [10]).

Основним поняттям, на якому побудовані вказані нормативно-правові документи є поняття профілю безпеки. Профіль безпеки (ПБ) – набір заходів захисту, які застосовуються до інформації або ІС для задоволення вимог чинної нормативної бази, а також спрямовані на захист потреб з метою управління ризиками безпеки [2].

Створення комплексних систем захисту інформації в системах з використанням базових та цільових профілів та декларування відповідності таких комплексних систем здійснюється за рахунок налаштування базового профілю безпеки (БПБ).

Базовим профілем безпеки інформації є вимоги з безпеки інформації та взаємопов'язана сукупність заходів з її захисту, визначені Адміністрацією Держспецзв'язку для відкритої інформації та інформації з обмеженим доступом, яка обробляється у системах.

Базовий профіль безпеки є простим і доступним варіантом для організацій з обмеженими ресурсами та невисокими вимогами до безпеки. Він забезпечує мінімальний рівень захисту та може бути швидко впроваджений. Однак для організацій з високими вимогами до безпеки або специфічними загрозами, більш комплексні системи, такі як КСЗІ, СУІБ або СБІ, можуть бути більш відповідними, хоча і потребують значних ресурсів для впровадження та підтримки.

Цільовий профіль безпеки (ЦПБ) – представляє собою взаємопов'язану сукупність заходів із захисту інформації та їх налаштування, визначених для системи її власником (розпорядником) відповідно до базового профілю з урахуванням вимог законодавства та стандартів у сфері захисту інформації в ІС, електронних комунікаційних та ІКС, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки в системах, а також призначення системи, її характеристик та особливостей функціонування, результатів проведеної оцінки ризиків [4].

БПБ є корисним інструментом для встановлення мінімальних стандартів захисту інформації в організації. Він забезпечує швидке впровадження та зниження ризиків від найпоширеніших загроз, проте для повного захисту інформаційних активів може вимагати подальшого посилення та адаптації до специфічних потреб організації.

Основні характеристики базового профілю безпеки:

1. Мінімальні вимоги до безпеки: визначає мінімальний набір заходів, які повинні бути впроваджені для забезпечення базового рівня безпеки.

2. Стандартні контрольні заходи: включає стандартні контрольні заходи, такі як управління доступом, шифрування даних, безпека мережі, моніторинг та аудит, захист від шкідливого програмного забезпечення.

3. Універсальність: може бути застосований до різних типів організацій та інформаційних систем, забезпечуючи базовий рівень захисту незалежно від специфіки.

4. Спрощене впровадження: базовий профіль безпеки розроблений таким чином, щоб бути легким для впровадження, навіть для організацій з обмеженими ресурсами та технічними можливостями.

Переваги:

1. Швидке впровадження: набір мінімальних вимог дозволяє швидко розгорнути базові заходи безпеки, забезпечуючи початковий рівень захисту.

2. Зниження ризиків: реалізація БПБ знижує ризики від найпоширеніших загроз та вразливостей, забезпечуючи фундаментальний рівень захисту інформації.

3. Підвищення обізнаності: допомагає підвищити обізнаність організацій щодо необхідності забезпечення інформаційної безпеки та встановлення основних стандартів захисту.

Недоліки:

1. Обмежений рівень захисту: БПБ забезпечує лише мінімальний рівень захисту, що може бути недостатнім для організацій з високими вимогами до безпеки.

2. Необхідність подальшого розширення: організації, які впровадили БПБ, можуть потребувати подальшого розширення та посилення заходів безпеки для забезпечення захисту від більш складних та специфічних загроз.

Під час визначення цільового профілю власник (розпорядник) системи самостійно обирає стандарти у сфері захисту інформації в ІС, електронних комунікаційних та ІКС, які використовуються під час здійснення заходів із захисту інформації, шляхи і способи здійснення таких заходів відповідно до цільового профілю, а також визначає наявність у ньому інформації з обмеженим доступом та забезпечує дотримання встановлених правил роботи з документами, які містять інформацію з обмеженим доступом (рис. 2).

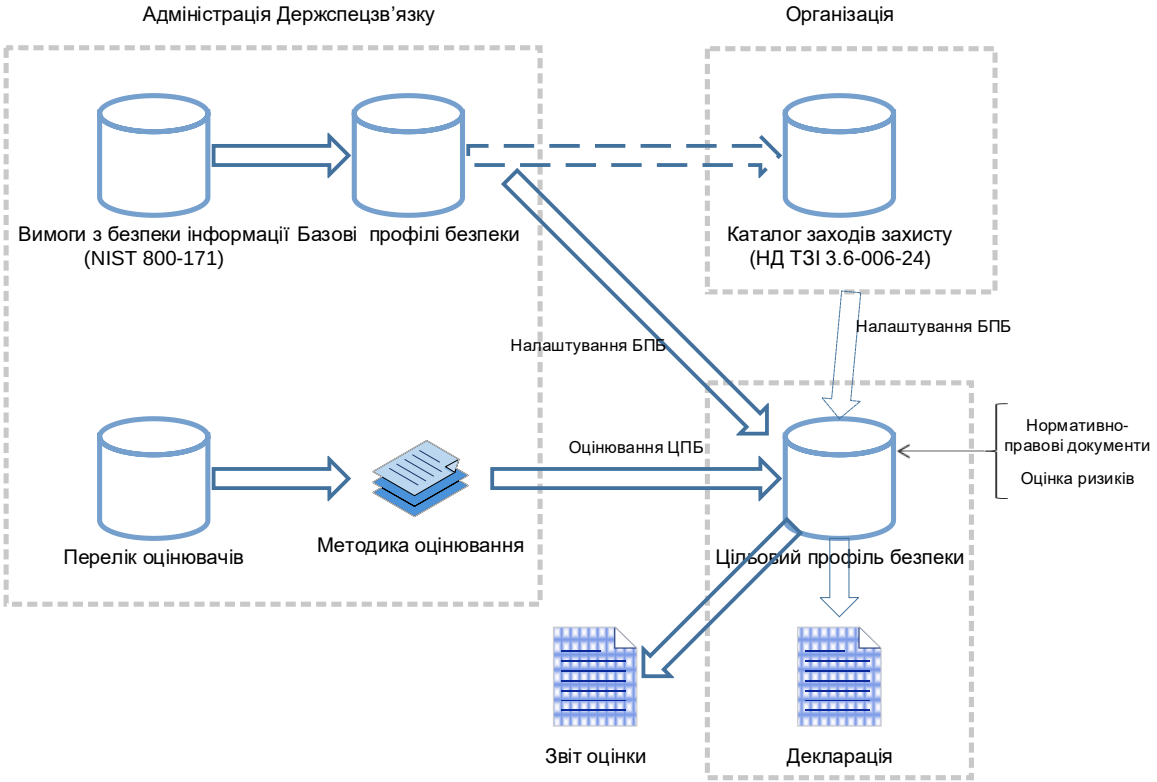

Рис. 2. Застосування профілів безпеки інформації

Передбачені у цільовому профілі заходи із захисту інформації, обрані стандарти, шляхи і способи здійснення таких заходів повинні включати відповідні вимоги та заходи, визначені базовим профілем.

Переваги та недоліки застосування базового профілю безпеки у порівнянні з КСЗІ, СУІБ та СБІ:

Переваги:

1. Простота впровадження: легше впровадити, оскільки він передбачає мінімальні вимоги та контрольні заходи.

2. Низька вартість: зазвичай вимагає менше фінансових та ресурсних витрат порівняно з більш комплексними системами.

3. Швидкість реалізації: може бути швидко розгорнутий, забезпечуючи базовий рівень захисту за короткий час.

4. Зниження ризиків: забезпечує захист від найпоширеніших загроз, що є корисним для організацій з обмеженими ресурсами.

Недоліки:

1. Обмежений рівень захисту: забезпечує лише мінімальний рівень безпеки, що може бути недостатнім для організацій з високими вимогами до безпеки.

2. Необхідність подальшого розширення: для повного захисту інформаційних активів може знадобитися впровадження додаткових заходів безпеки.

3. Менша гнучкість: менше адаптований до специфічних потреб організації порівняно з більш комплексними системами.

3. Процес створення КСЗІ в системах з використанням базових та цільових профілів та декларування відповідності таких комплексних систем

Загальна схема створення КСЗІ в системах з використанням базових та цільових профілів та декларування відповідності таких комплексних систем здійснюється за такими етапами (рис. 3) [4]:

1. Розробка профілів безпеки.
2. Впровадження вимог безпеки.
3. Оцінювання достатності.
4. Декларування відповідності КСЗІ в системах, створених з використанням профілів безпеки.

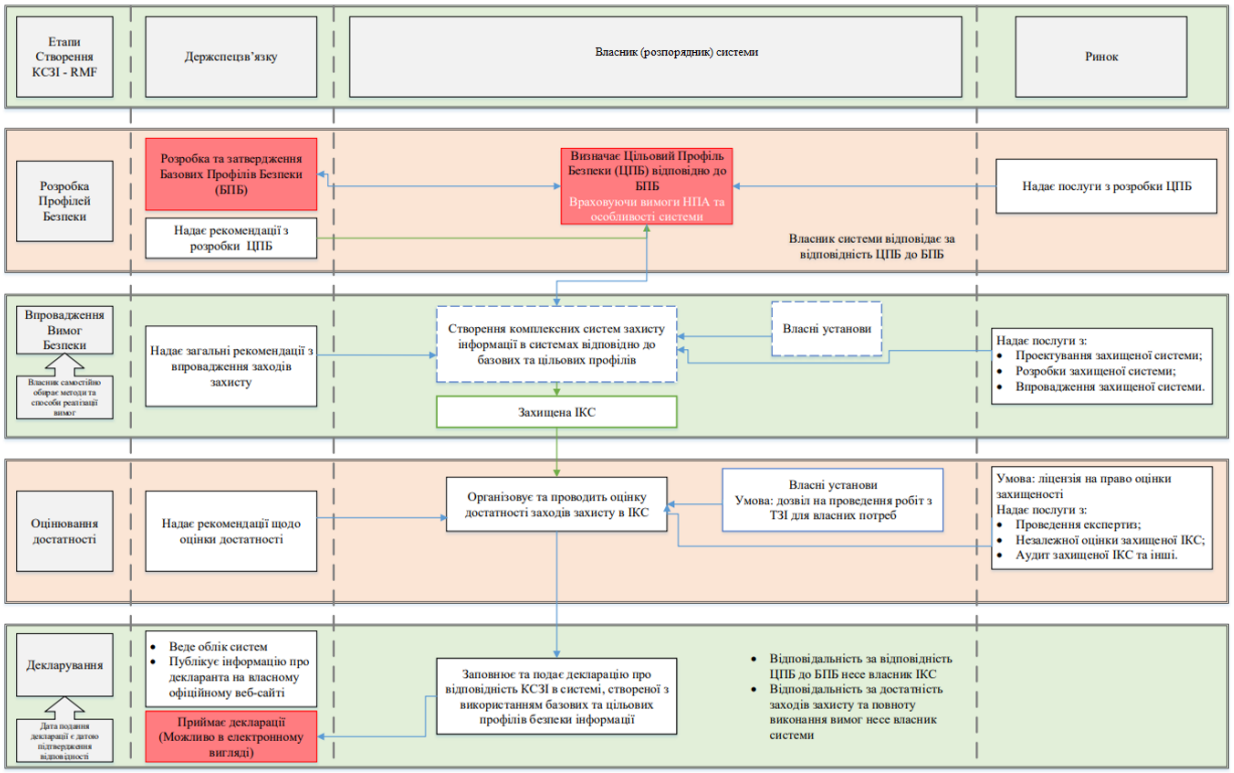

Рис. 3. Порядок реалізації експериментального проєкту

Процес створення КСЗІ в системах з використанням базових та цільових профілів та декларування відповідності таких комплексних систем передбачає виділення трьох ролей: Держспецзв'язку, власника (розпорядника) системи та ринку. В якості останньої ролі мають-ся на увазі державні та приватні підприємства, які надають свої послуги зі створення КСЗІ, наприклад, IT Engineering [11], Державна ІТ-компанія "ІНФОТЕХ" [12], АТ "ІІТ" [13], H-X Technologies [14] та багато інших.

Перший етап – розробка профілів безпеки. На цьому етапі передбачається формування вимог безпеки до системи відповідно до певного виду інформації (відкрита, службова або інформація, що становить державну таємницю) у вигляді базового профілю. Як показано на рис. 1, в першій редакції Адміністрація Держспецзв'язку таку місію виконала у вигляді відповідного наказу від 26.06.2024 № 317 [15]. Важливо також відмітити універсальність, яка закладена в БПБ цього наказу. Важливо також зазначити, що цей БПБ є універсальним та у ньому не буде поділу на АС класу 1, 2, 3. Розроблений БПБ надається власнику системи. У залежності від виду інформації, БПБ містить заходи захисту відповідно до НД ТЗІ 3.6-006-24 [9]. Під час визначення заходів захисту також враховуються профілі

безпеки засобів захисту, вимоги міжнародних та галузевих стандартів. Так, в наказі Адміністрації Держспецзв'язку від 26.06.2024 № 317 [15] надається посилання на 127 заходів захисту (посилених заходів захисту) для відкритої інформації та 153 заходів захисту (посилених заходів захисту) для службової інформації. Таким чином, власник (розпорядник) системи отримує розроблений БПБ. Після цього, власник (розпорядник) системи, враховуючи вимоги нормативно-правових актів певної галузі та особливостей самої ІС, електронної комунікаційної системи та ІКС проводить налаштування ЦПБ на основі БПБ (як показано на рис. 2). Власник (розпорядник) системи для налаштування ЦПБ може звернутися до послуг третьої сторони, але відповідальність покладається виключно на нього. Слід зазначити, що Адміністрація Держспецзв'язку при налаштуванні ЦПБ здійснює лише функції консультаційного характеру та ніякого впливу на власника (розпорядника) системи не проводить. Тому, розроблений на першому етапі ЦПБ затверджується керівником організації, до якої належить система. Саме на керівника покладається юридична відповідальність за правильність налаштування ЦПБ та впровадження заходів захисту інформації певного виду.

Другий етап – впровадження вимог безпеки. Цей етап має суттєве практичне значення для створення КСЗІ на основі налаштованого ЦПБ. Слід зазначити, що наказом визначається мінімально допустимий набір заходів захисту, впровадження яких в КСЗІ є обов'язковим. Але власник (розпорядник) системи самостійно може визначити додаткові вимоги з безпеки та заходи захисту для системи, враховуючи її специфіку. Таким чином, ЦПБ буде містити усі вимоги до певного виду інформації, що прописані в БПБ, а також додаткові вимоги, обумовлені специфікою використання системи. Також на цьому етапі ринок може приймати участь в проєктуванні (розробці) самої захищеної системи та впровадженні вимог безпеки. Знов слід зазначити, що Адміністрація Держспецзв'язку при створенні КСЗІ безпосередньої участі не приймає, лише, за потреби, може надавати консультаційні поради й ніякого впливу на власника (розпорядника) системи не проводить.

Третій етап – оцінювання достатності. Це дуже важливий етап для власника (розпорядника) системи тому, що саме по результатах його проведення він гарантуватиме йому впевненість в реалізації всіх налаштованих (уточнених) заходів захисту, які прописуються в ЦПБ на систему. Згідно з наказом Адміністрації Держспецзв'язку від 10.07.2024 № 354 [16] оцінка достатності заходів захисту інформації комплексних систем захисту інформації включає оцінку:

- визначення цільового профілю безпеки;
- реалізації базового профілю безпеки;
- реалізації цільового профілю безпеки.

Основним результатом на третьому етапі є отримання звіту оцінювання для декларування щодо відповідності реального стану КСЗІ вимогам з безпеки, які визначаються його ЦПБ. Організовує та проводить оцінку достатності власник (розпорядник) системи за допомогою власних фахівців, які мають дозвіл на проведення робіт з ТЗІ або із залученням сертифікованих компаній, які мають ліцензію на право проведення експертизи КСЗІ з оцінкою та аудитом захищеної ІС, ІКС. Знов слід зазначити, що Адміністрація Держспецзв'язку при оцінюванні достатності безпосередньої участі не приймає, лише, за потреби, може надавати консультаційні поради й ніякого впливу на власника (розпорядника) системи не здійснює.

Четвертий (останній) етап – декларування. Це заповнення власником декларації, яка й стане гарантом реалізації БПБ. Згідно з [4], декларація про відповідність КСЗІ, створеної з використанням БПБ та ЦПБ, подається до Адміністрації Держспецзв'язку власником (розпорядником) системи в електронній формі з використанням системи електронної взаємодії органів виконавчої влади з накладенням електронного підпису, що базується на кваліфікованому сертифікаті електронного підпису відповідно до вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг, а у разі наявності в них інформації з обмеженим доступом подання таких документів здійснюється з дотриманням встановлених правил роботи з документами, які містять інформацію з обмеженим доступом.

Періодичність подання декларацій становить три роки з дати подання декларації до Адміністрації Держспецзв'язку. На Адміністрацію Держспецзв'язку покладається функція ведення обліку задекларованих КСЗІ та публікації інформації про декларанта на своєму веб-сайті, крім матеріалів, що містять інформацію з обмеженим доступом.

Отже, в даному процесі Адміністрація Держспецзв'язку зосереджена лише на етапах розробки профілів безпеки та розробки рекомендацій щодо їх оцінки та надання консультацій (рис. 4).

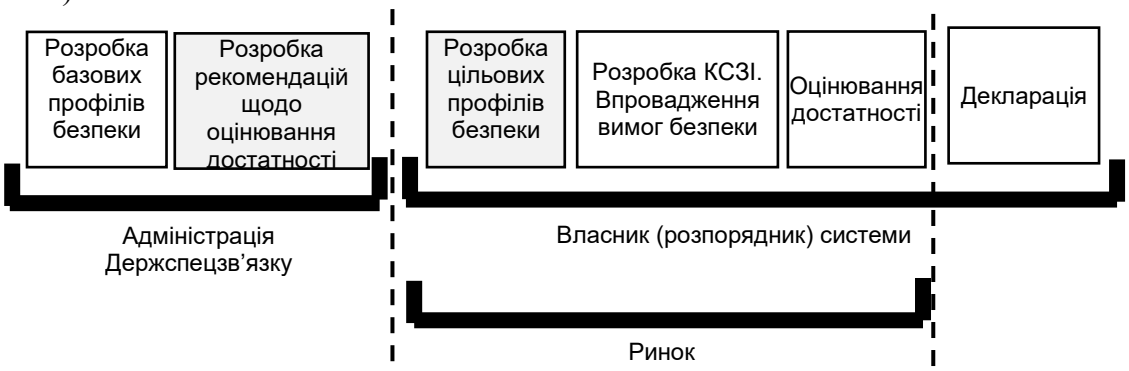

Рис. 4. Етапи, в яких беруть участь учасники експериментального проєкту

Таким чином, після обирання БПБ для відкритої та службової інформації, власник (розпорядник) системи проводить його налаштування. Після затвердження ЦПБ, де він самостійно обирає стандарти, які використовуються під час реалізації заходів захисту, методи та порядок впровадження заходів захисту, починається експлуатація як самої системи, так й КСЗІ, побудованої для неї. Головне правило – набір заходів захисту ЦПБ не може бути менше, ніж встановлено БПБ.

4. Особливі механізми налаштування цільового профілю безпеки

Для налаштування ЦПБ крок за кроком обираються відповідні, для певного виду інформації (відкрита, службова тощо), вимоги з БПБ, які в [15] для відкритої інформації відносяться до 15 класів заходів захисту, а для службової інформації – до 17 класів заходів захисту (табл. 1).

Таблиця 1

Перелік класів заходів захисту, використаних в БПБ для відкритої та службової інформації

№ з/п	ID класу	Назва класу	Кількість вимог в БПБ	
			для відкритої інформації	для службової інформації
1	AC	Управління доступом	16	16
2	AT	Обізнаність і навчання	2	2
3	AU	Аудит і підзвітність	8	8
4	CA	Оцінювання, акредитація та моніторинг безпеки	4	4
5	CM	Управління конфігурацією	6	10
6	IA	Ідентифікація та автентифікація	8	8
7	IR	Реагування на інциденти	4	4
8	MA	Технічне обслуговування	3	3
9	MP	Захист носіїв інформації	6	7
10	PE	Фізичний захист і захист робочого середовища	5	5
11	PL	Планування безпеки	2	3
12	PS	Кадрова безпека	2	2
13	RA	Оцінка ризику	2	2
14	SA	Придбання системи та послуг	-	3
15	SC	Системний і комунікаційний захист	10	10
16	SI	Цілісність системи та інформації	4	5
17	SR	Управління ризиками ланцюга поставок	-	3
		Всього:	82	95

Якщо в якості прикладу розглянути вимогу "1.12 Віддалений доступ" (рис. 5) [9], то для її реалізації власник (розпорядник) системи повинен впровадити заходи захисту, які виділені напівжирним прямокутником (позначені під номером 1). Це заходи захисту АС-17, АС-17(03), АС-17(04) з каталогу НД ТЗІ 3.6-006-24 [9].

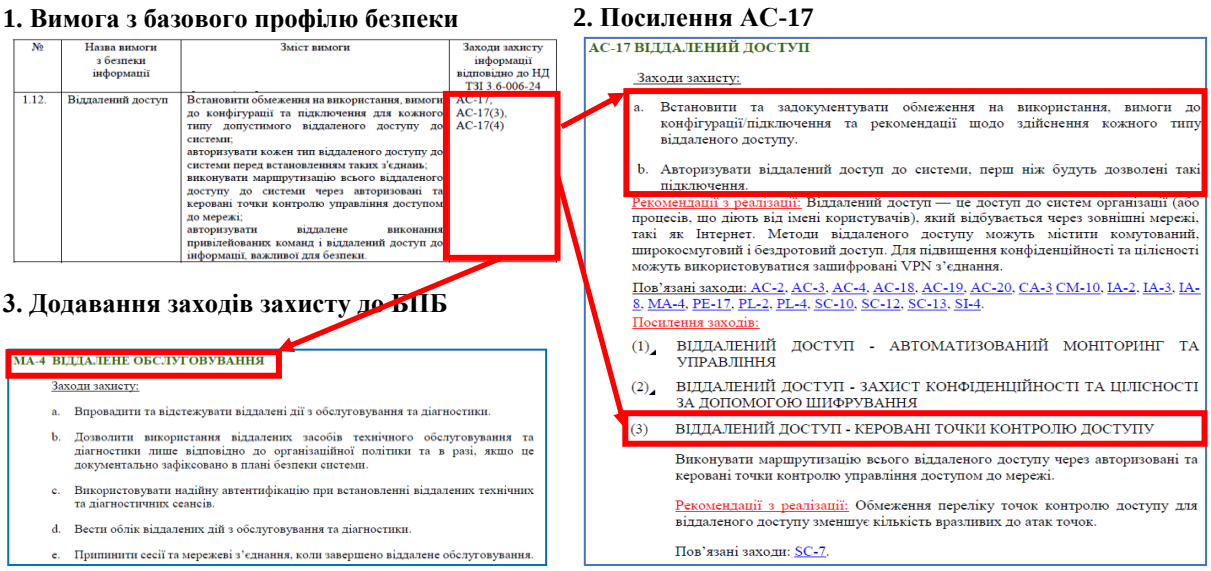

Рис. 5. Формування ЦПБ з посиленням МА-4

Відповідно до нормативно-правових актів організацій і проведення оцінки ризиків умов функціонування системи формується ЦПБ, в якому БПБ буде посилюватися або доповнюватися додатковими заходами захисту. Під номером 2 (рис. 5) зображено захід захисту АС-17 НД ТЗІ 3.6-006-24 [9], який потрібно реалізувати згідно з вимогами БПБ. Напівжирним прямокутником під номером 2 також виділено посилення АС-17(3) заходів захисту, які потрібно виконати та врахувати при налаштуванні ЦПБ. Однак під номером 3 наведений захід захисту МА-4, який не входить до складу БПБ, але може бути використаний при налаштуванні ЦПБ.

Таким чином, аналізуючи всі вимоги (табл. 1) проводиться їх співставлення із заходами захисту, які надаються каталогом НД ТЗІ 3.6-006-24 [9]. Слід також зазначити, що цей каталог є національним гармонізованим стандартом, що відповідає NIST 800-53 rev.5 [3], який періодично змінюється, виходячи з реалій існуючого стану програмних та апаратних можливостей зловмисників.

5. Модель проведення оцінювання достатності

Загальний процес оцінювання достовірності ЦПБ проводиться з метою [16]:

- підтвердження відповідності вибору базового профілю безпеки для формування цільового профілю безпеки;
- підтвердження наявності у цільовому профілі безпеки всіх вимог та заходів захисту базового профілю безпеки;
- підтвердження відповідності цільового профілю безпеки (сукупності заходів із захисту інформації та їх налаштувань) вимогам законодавства та стандартів у сфері захисту інформації, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки тощо для визначеної системи.

У нотації системи умовних позначень для моделювання бізнес-процесів (Business Process Model and Notation, BPMN) [17] процес оцінювання наведено на рис. 6.

Процедура оцінки базового профілю безпеки складається з мети заходу з оцінки та набору потенційних методів і об'єктів оцінки, які можуть бути використані для проведення оцінки. Кожна потенційна мета заходу з оцінки передбачає твердження про визначення, пов'язане з вимогою безпеки, визначеною базовим профілем. Якщо у вимозі з безпеки є параметр, визначений організацією (Organization-Defined Parameter, ODP), то мета заходу

з оцінки починається з формулювання, пов’язаного з визначенням ODP. Визначальні твердження пов’язані із змістом вимог з безпеки, щоб допомогти забезпечити простежуваність результатів оцінки до вимог.

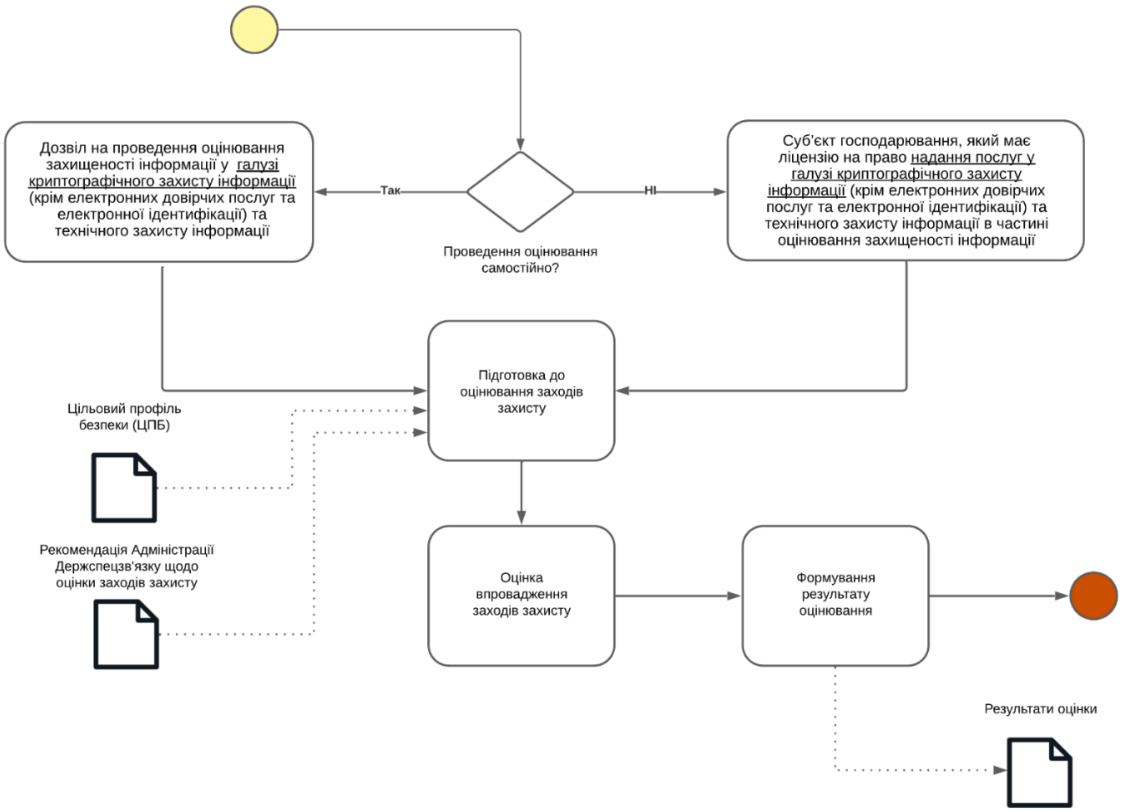

Рис. 6. Модель оцінювання достатності ЦПБ

Методи оцінки визначають характер і обсяг дій оцінювача і використовуються для полегшення розуміння, досягнення роз’яснень або отримання доказів. Потенційні методи оцінки передбачають дослідження, опитування та випробування [16]:

- метод дослідження – процес огляду, вивчення, інспектування, спостереження або аналізу об’єктів оцінки;
- метод опитування – процес проведення дискусій з окремими особами або групами щодо об’єктів оцінки;
- метод випробування – процес виконання об’єктами оцінки (тобто діями, механізмами) певних дій у визначених умовах з метою порівняння фактичної поведінки з очікуваною.

Методи оцінки містять атрибути глибини та охоплення, які визначають ретельність, обсяг і рівень зусиль для проведення оцінки, а також ступінь впевненості в тому, що вимоги з безпеки були виконані.

Розроблена рекомендація щодо оцінювання реалізації БПБ та ЦПБ надається з метою унеможливлення суб’єктивного оцінювання, щоб кожен експерт незалежно один від одного отримував однакові результати. Застосування процедури оцінювання до вимог безпеки дає результати оцінювання або висновки. Ці висновки узагальнюються і використовуються як докази того, що чи має вимога безпеки значення "позитивне" або "негативне".

"Позитивне" (П) вказує на те, що мета оцінювання була досягнута й отримано повністю прийнятний результат.

"Негативне" (Н) – означає, що експерт не зміг отримати достатньо інформації для прийняття рішення, яке вимагається у звіті про результати оцінювання.

У табл. 2 наведено приклад звіту з оцінки вимоги з безпеки 1.8 «Невдалі спроби входу в систему» базового профілю.

Таблиця 2

Фрагмент оцінювання достовірності для вимоги безпеки 1.8 «Невдалі спроби входу в систему»

Номер вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
1.8	Невдалі спроби входу в систему			
	A.1.8.ODP[01]	визначена кількість послідовних невдалих спроб входу користувача в систему, дозволених протягом певного періоду часу;	П	*Дослідження:* 1. В політиці безпеки організації, яка затверджена наказом директора №111 від 26.06.2024 року, у розділі «Політика використання паролів» визначено кількість послідовних недійсних спроб входу до системи – 5 спроб; 2. В документі «Технічний проєкт. Пояснювальна записка» (реєстр. № 123 від 26.06.2024 року) у відповідності до пункту 4 розділу 3 політика використання паролів реалізується засобами ОС Windows 10 (параметр налаштування «Account lockout threshold»). 3. У налаштуваннях ОС Windows 10 системи параметр «Account lockout threshold» встановлено «5». *Опитування:* 1. Адміністратор безпеки – здійснив налаштування системи у відповідності до «Інструкції адміністратора безпеки» (реєстр. № 121 від 26.06.2024 року) та документу «Технічний проєкт. Пояснювальна записка» (реєстр. № 123 від 26.06.2024 року). *Випробування:* 1. Після 5 спроб введення неправильного паролю до ОС Windows 10 система блокується.
	A.1.8.ODP[02]	визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача;	Н	*Дослідження:* 1. У політиці безпеки організації, яка затверджена наказом директора №111 від 26.06.2024 року, у розділі «Політика використання паролів» визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача – 5 хвилин. 2. Механізми реалізації вимоги **не визначені.** 3. Спосіб налаштування механізмів **не визначено.** *Опитування:* 1. Адміністратор безпеки – відповідні налаштування системи **не проводив**. *Випробування:* 1. В продовж 7 хвилин здійснено 4 спроби введення неправильного паролю до ОС Windows 10 системи – система **не блокується.**
	A.1.8	визначено кількість послідовних невірних спроб входу користувача протягом <A.1.8.ODP[02]: період часу> обмежено до <A.1.8.ODP[01]: кількість>.	Н	*Коментарі:* 1. Вимога не може бути оцінена – A.1.8.ODP[02] **оцінена негативно**.
	Загальна оцінка реалізації вимоги 1.8		**Не реалізовано**	

У табл. 2 «Номер вимоги» відповідає номеру вимоги з безпеки базового профілю для систем, де обробляється відповідна інформації за видом доступу.

Позначення заходів з оцінки мають буквено-цифрові ідентифікатори. Кожний захід з оцінки починається з літери «А», яка вказує на те, що воно є частиною процедури оцінки. Наступна послідовність цифр та/або літер (наприклад, 1.8.ODP[01]) вказує на ідентифікатор вимоги безпеки з базового профілю для ІКС, де обробляється відповідна інформації за видом доступу (та конкретний елемент контролю, якщо це багатокомпонентна вимога), яка є метою заходу з оцінки. Параметри, визначені організацією, позначаються літерами «ODP». Якщо в заяві про визначення є декілька ODP, номер ODP вказується в квадратних дужках (наприклад, A.1.8.ODP[01]). Квадратні дужки також використовуються для позначення того, коли процедура оцінки далі розбиває вимогу на більш детальні заяви про визначення (наприклад, A.1.8.ODP[01], A.1.8.ODP[02]).

Порядок оцінки КСЗІ на основі ЦПБ визначається власником системи самостійно та здійснюється суб'єктами господарювання, які мають ліцензію на право надання послуг в галузі криптографічного захисту інформації (крім надання електронних довірчих послуг та електронної ідентифікації) та технічного захисту інформації в частині оцінювання захищеності інформації або учасниками експериментального проєкту, які мають дозвіл на проведення робіт з ТЗІ для власників в частині захищеності інформації.

6. Модель декларування відповідності

Результат оцінки КСЗІ на основі ЦПБ, що підготовлено в рамках цього експериментального проєкту, приймається як результат державної експертизи. За умов виконання всіх етапів та вимог, власник системи декларує, що набір заходів захисту, визначених ЦПБ, відповідає мінімальному набору заходів захисту, встановленому в БПБ для відповідного виду інформації. В нотації BPMN процес декларації показаний на рис. 7.

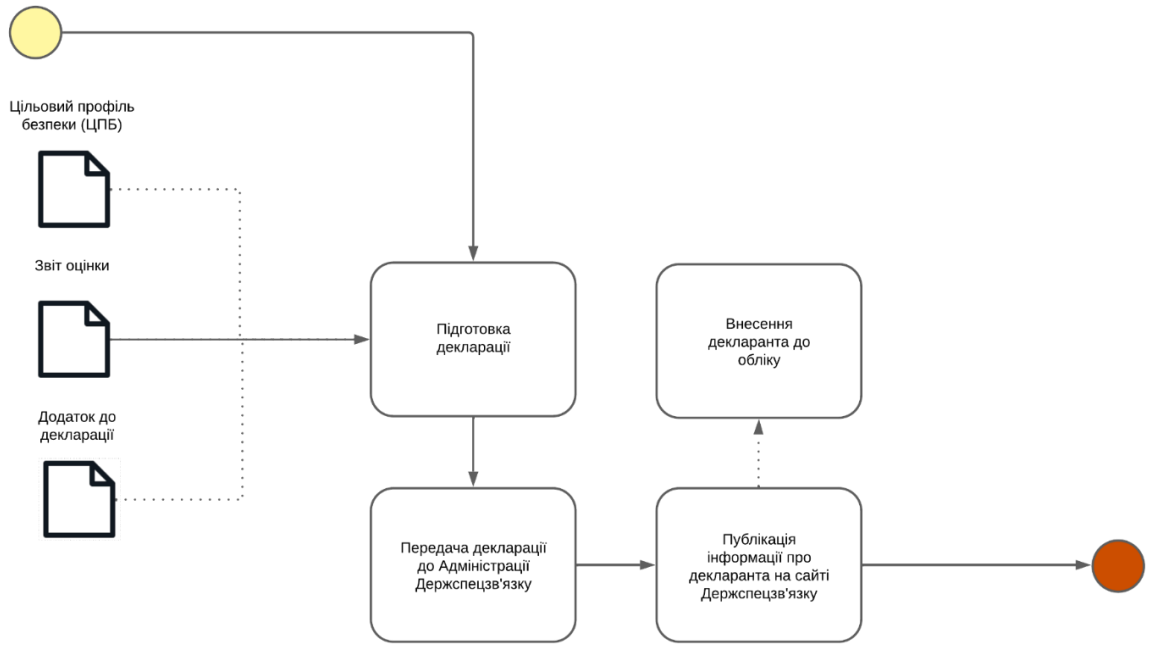

Рис. 7. Модель декларування відповідності

Декларація про відповідність КСЗІ подається до Адміністрації Держспецзв'язку власником системи в електронній формі з накладанням кваліфікованого електронного підпису, а для документів з обмеженим доступом – в установленому законодавством порядку. Облік систем, які мають КСЗІ, побудованих з використанням профілів безпеки, буде здійснюватися Адміністрацією Держспецзв'язку.

Дата на відсилання декларації про відповідність до Адміністрації Держспецзв'язку буде вважатися датою підтвердження відповідності цієї КСЗІ в системах, побудованих з використанням профілів безпеки та не потребує відповіді від Адміністрації Держспецзв'язку.

Адміністрація Держспецзв'язку буде публікувати інформацію про декларантів на сайті Держспецзв'язку. Щодо перевірки КСЗІ в системах, побудованих з використанням профілів безпеки, то вона буде здійснюватися в рамках державного контролю за станом технічного захисту інформації державних інформаційних ресурсів та інформації, вимоги до захисту яких встановлені законом.

Адміністрація Держспецзв'язку, з метою визначення ефективності реалізації експериментального проєкту, здійснює моніторинг системи захисту інформації в системах, побудованих з використанням даних профілів. Моніторинг проводиться з метою надання методичної консультативної підтримки. Строк дії декларації становить три роки з дня підтвердження її відповідності [4].

У разі закінчення терміну дії декларації про відповідність або зміну ЦПБ, декларація про відповідність КСЗІ вважатиметься недійсною. Додаткове декларування КСЗІ в системах, побудованих з використанням профілів безпеки, відбувається за наступних підстав: закінчення терміну дії декларації про відповідність, або в разі зміни ЦПБ, або після усунення недоліків, виявлених за результатами проведення державного контролю.

Висновки

1. Розглянутий підхід декларування дозволить поєднати сучасні нормативно-правові документи, які утворюють систему використання профілів безпеки інформації при розгортанні КСЗІ, та спрощення отримання підстав експлуатувати інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи з обробкою відкритої та службової інформації.

2. Розглянутий підхід дозволить підвищити рівень обізнаності проєктувальників та розробників КСЗІ, надавши підготовлений заздалегідь базовий профіль безпеки та вказавши шлях його застосування.

3. Побудовано логічну сукупність нормативно-правових актів, яка дозволить орієнтуватися в сучасних підходах, які ґрунтуються на стандартах NIST США.

4. Основна увага у роботі приділена процесу розробки профілів безпеки, впровадженню вимог безпеки, механізмам оцінювання достатності та подальшого декларування відповідності КСЗІ в системах, створених з використанням профілів безпеки.

Список літератури:

1. ISO/IEC 27000 family. Information security management. URL: https://www.iso.org/standard/iso-iec-27000-family
2. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53375
3. NIST SP 800-53 rev. 5 Security and Privacy Controls for Information Systems and Organizations, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
4. Постанова Кабінету Міністрів України від 30.05.2024 № 627 "Про реалізацію експериментального проєкту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації". URL: https://zakon.rada.gov.ua/laws/show/627-2024-п.
5. НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі, 2000. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf
6. NIST SP 800-53A rev. 5 Assessing Security and Privacy Controls in Information Systems and Organizations, 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf
7. NIST SP 800-171 rev. 3. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 2024. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf
8. NIST SP 800-171A rev. 3. Assessing Security Requirements for Controlled Unclassified Information, 2024. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171Ar3.pdf.

9. 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, 2024. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=64620
10. 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, 2021. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53377
11. IT Engineering. URL: https://it-engineering.com.ua
12. Державна IT-компанія "ІНФОТЕХ" URL: https://infotech.gov.ua.
13. АТ "ІІТ" URL: https://infotech.gov.ua
14. H-X Technologies URL: https://www.h-x.technology.
15. Наказ Адміністрації Держспецзв'язку від 26.06.2024 "Про визначення Базового профілю безпеки інформації". URL: https://www.cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-24-06-2024-317-pro-viznachennya-bazovogo-profilyu-bezpeki-informaciyi
16. Наказ Адміністрації Держспецзв'язку від 10.07.2024 "Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації". URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-10-07-2024-354-pro-zatverdzhennya-rekomendacii-z-ocinki-dostatnosti-zakhodiv-zakhistu-informaciyi-kompleksnikh-sistem-zakhistu-informaciyi-v-informaciinikh-elektronnikh-komunikaciinikh-ta-informaciino-komunikaciinikh-sistemakh-stvorenikh-z-vikoristannyam-profiliv-bezpeki-informaciyi
17. Система умовних позначень (нотація) для моделювання бізнес-процесів версії 2.0. URL: https://uk.wikipedia.org/wiki/BPMN

Надійшла до редколегії 10.06.2024

Відомості про авторів:

Потій Олександр Володимирович – д-р техн. наук, професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України; e-mail: Potav1971@gmail.com4 ORCID: https://orcid.org/0009-0004-9332-4414

Голубничий Дмитро Юрійович – канд. техн. наук, доцент, Харківський національний економічний університет імені Семена Кузнеця, доцент кафедри інформаційних систем, факультет інформаційних технологій, АТ "Інститут Інформаційних Технологій", начальник відділу наукових досліджень; Україна; e-mail: dmytro.holubnychyi@hneu.net, ORCID: https://orcid.org/0000-0002-6873-7004

Васильєв Юрій Костянтинович – Державна служба спеціального зв'язку та захисту інформації України, e-mail: y.vasyliev@cip.gov.ua

Єсіна Марина Віталіївна – канд. техн. наук, доцент, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ "Інститут Інформаційних Технологій", науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606