НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

НД ТЗІ 2.7 -009-09

Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

Київ 2009

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної
служби спеціального зв'язку та
захисту інформації України
24 липня 2009 року № 172
із змінами згідно наказу Адміністрації
Держспецзв'язку від 28.12.2012 № 806

Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

НД ТЗІ 2.7-009-09

Адміністрація Держспецзв'язку

Київ

ПЕРЕДМОВА

РОЗРОБЛЕНО Товариством з обмеженою відповідальністю "Інститут комп'ютерних технологій".

ВНЕСЕНО Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Державної служби спеціального зв’язку та захисту інформації України.

ВВЕДЕНО ВПЕРШЕ.

ЗМІСТ

НД ТЗІ 2.7-009-09

Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

Чинний від 2009-07-24

1 Галузь застосування

Цей нормативний документ (НД) містить методичні вказівки та рекомендації щодо здійснення експертного оцінювання відповідності засобів захисту інформації в комп'ютерних системах від несанкціонованого доступу (НСД) та комплексів засобів захисту (КЗЗ) комплексних систем захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах (ІТС) вимогам до технічного захисту інформації (ТЗІ) в частині оцінювання функціональних послуг безпеки. У частині, що стосується методології проведення оцінювання, наведені рекомендації можуть також використовуватися при проведенні експертизи засобів захисту інформації, в яких сукупність реалізованих функцій захисту не в повному обсязі відповідає встановленим НД ТЗІ вимогам щодо реалізації функціональних послуг безпеки.

НД призначений для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, а також підприємств, установ і організацій всіх форм власності, які виконують роботи зі створення та проведення експертизи засобів захисту інформації в комп'ютерних системах від НСД на відповідність вимогам НД системи ТЗІ в Україні.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

ГОСТ 19.201-78 Единая система программной документации. Техническое задание. Требования к содержанию и оформлению.

ГОСТ 19.301-79 Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению.

ГОСТ 19.404-79 Единая система программной документации. Пояснительная записка. Требования к содержанию и оформлению.

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

ДСТУ 2851-94 Програмні засоби ЕОМ. Документування результатів випробувань.

ДСТУ 2853-94 Програмні засоби ЕОМ. Підготовлення і проведення випробувань.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни і визначення.

Положення про державну експертизу у сфері технічного захисту інформації. Затверджено наказом Адміністрації Державної служби

спеціального зв’язку та захисту інформації України № 93 від 16.05.2007. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

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

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

3 Визначення

У цьому НД ТЗІ застосовуються терміни та визначення, встановлені ДСТУ 3396.2-97 та НД ТЗІ 1.1-003-99.

Крім цього, використано такі терміни та визначення.

Випробування – експериментальне визначення кількісних та/або якісних характеристик властивостей об'єкта експертизи за результатом впливу на нього під час його функціонування.

Ефективність – властивість об'єкта експертизи, що характеризується мірою досягнення цілей, поставлених під час його створення.

Засіб випробувань – програмний, програмно-апаратний або апаратний засіб, що використовується з метою здійснення перевірок у процесі проведення випробувань.

Засіб технічного захисту інформації від НСД – програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну проектну та/або експлуатаційну документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз НСД для інформації, оброблюваної в ІТС.

Захищений від НСД компонент обчислювальної системи – програмний, апаратний або програмно-апаратний засіб, у якому додатково до основного призначення передбачено функції захисту інформації від загроз НСД.

Інформаційно-телекомунікаційна система – організаційно-технічна система, в якій реалізується технологія оброблення (створення, зберігання, передачі) інформації за допомогою технічних і програмних засобів. У контексті цього документа поняття інформаційно-телекомунікаційної системи розглядається як синонім поняття автоматизованої системи згідно з НД ТЗІ 1.1-003-99.

Метод випробувань – встановлений та документально зафіксований порядок проведення випробувань.

Методика випробувань – визначені (встановлені) способи проведення випробувань.

Об'єкт експертизи – засіб технічного захисту інформації від НСД, захищений від НСД компонент обчислювальної системи або КЗЗ КСЗІ, стосовно яких здійснюється експертиза з метою оцінювання функціональних послуг безпеки. У контексті цього документа поняття об'єкта експертизи розглядається як синонім поняття комп'ютерної системи згідно з НД ТЗІ 1.1-003-99.

Оцінювання – визначення ступеня відповідності об'єкта експертизи

заданим критеріям.

Перевірка – одинична контрольна дія в процесі проведення випробувань.

Працездатність – стан об'єкта експертизи, що характеризує його здатність виконувати певні функції із заданою ефективністю та протягом потрібного часу.

Програма випробувань – документована сукупність вимог, що підлягає перевірці в процесі проведення випробувань.

Тестова процедура – документально зафіксована послідовність здійснення перевірок у процесі проведення випробувань.

Тестове покриття – міра, що характеризує здатність тестових даних випробовувати вимоги до об'єкта експертизи.

Тестові дані – дані, що використовуються як вхідні в процесі проведення випробувань об'єкта експертизи.

Функціональна специфікація об'єкта експертизи – впорядкований перелік рівнів функціональних послуг безпеки, що реалізуються об'єктом експертизи, разом з описом їх політик.

4 Позначення та скорочення

У цьому НД ТЗІ використано такі позначення та скорочення:

Держспецзв'язку – Державна служба спеціального зв'язку та захисту інформації України;

ЕОМ – електронно-обчислювальна машина;

ЗТЗІ – засіб технічного захисту інформації;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОЕ – об'єкт експертизи;

ПЗП – постійний запам'ятовуючий пристрій;

СКБД – система керування базою даних;

ТЗІ – технічний захист інформації.

5 Загальний опис методології проведення оцінювання функціональних послуг безпеки

5.1 Загальні положення

5.1.1 Як зазначається в НД ТЗІ 1.1-002-99, з погляду методології в проблемі захисту інформації, оброблюваної в ІТС, від НСД можна виділити два напрями:

- забезпечення захищеності інформації в функціонуючих та/або створюваних ІТС;
- створення засобів технічного захисту інформації (ЗТЗІ) від НСД або захищених від НСД компонентів обчислювальної системи поза конкретним середовищем експлуатації.

5.1.2 Як в першому, так і в другому випадку доцільним, а якщо в ІТС планується оброблення інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (інформації, що

належить до державних інформаційних ресурсів або становить державну таємницю), обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам. Результатом проведеного оцінювання має бути відповідний висновок, на підставі якого власники ІТС та оброблюваних у них інформаційних ресурсів можуть приймати рішення щодо прийнятності та достатності вжитих заходів та реалізованих засобів.

У процесі проведення оцінювання, окрім сукупності показників, що характеризують конкретну ІТС або засіб захисту, необхідними також є:

- критерії оцінки, під якими слід розуміти сукупність вимог (шкала оцінки), яка використовується для оцінювання ефективності функцій захисту інформації та коректності їх реалізації;
- система оцінювання, під якою слід розуміти адміністративно-правову структуру, в рамках якої у певному співтоваристві органи, що здійснюють оцінювання, застосовують критерії оцінки;
- методологія оцінювання, яка визначає послідовність (алгоритм) дій, що виконуються експертами при оцінюванні ефективності функцій захисту інформації та коректності їх реалізації, а також форму подання результатів.

5.1.3 В Україні як критерії оцінки використовуються критерії, встановлені НД ТЗІ 2.5-004-99, а також вимоги діючих НД ТЗІ щодо забезпечення захисту інформації в ІТС різного призначення. Вони надають:

- порівняльну шкалу для оцінювання ефективності функцій і механізмів захисту інформації від НСД, реалізованих в ІТС, а також коректності їх реалізації;
- базу (орієнтири) для розроблення засобів захисту інформації, оброблюваної в ІТС, від НСД.

Згідно з вимогами НД ТЗІ 2.5-004-99, окремо оцінюються реалізовані функції захисту (функціональні послуги безпеки) та рівень гарантій коректності їх реалізації (рівень гарантій).

5.1.4 Система оцінювання в Україні функціонує на основі Положення про державну експертизу у сфері технічного захисту інформації. Згідно з вимогами цього документа, оцінювання відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам здійснюється шляхом проведення експертизи. Суб'єктами експертизи є: юридичні та фізичні особи, які є замовниками експертизи; Державна служби спеціального зв’язку та захисту інформації України, а також підприємства, установи та організації, які проводять експертизу за її дорученням (організатори експертизи); фізичні особи – виконавці експертних робіт з ТЗІ (експерти). Об'єктами експертизи (ОЕ) в частині, що стосується оцінювання функціональних послуг безпеки, можуть бути КЗЗ КСЗІ, ЗТЗІ від НСД, а також захищені від НСД компоненти обчислювальної системи.

5.1.5 Методологія оцінювання функцій захисту (функціональних послуг безпеки) передбачає виконання таких етапів робіт:

- попередній аналіз оцінюваного ОЕ;

- розроблення програми випробувань функціональних послуг безпеки;
- розроблення методики випробувань функціональних послуг безпеки;
- проведення випробувань;
- аналіз, документування та затвердження результатів випробувань.

5.2 Попередній аналіз об'єкта експертизи

5.2.1 Головною метою етапу попереднього аналізу є прийняття рішення щодо можливості проведення робіт з експертизи ОЕ, визначення обсягів та плану робіт. Послідовність та обсяг робіт експерта на цьому етапі залежать від варіанта подання ОЕ на експертизу, тобто:

- ОЕ у вигляді КЗЗ КСЗІ, ЗТЗІ від НСД або захищеного компонента обчислювальної системи подано на експертизу розробником разом з проектною та експлуатаційною документацією, при цьому в проектній документації розробником визначено функціональні специфікації ОЕ (перелік реалізованих в ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опис їх політики);
- ОЕ у вигляді ЗТЗІ від НСД або захищеного компонента обчислювальної системи подано на експертизу розробником, який володіє інформацією щодо особливостей реалізації в ОЕ функцій захисту, разом з експлуатаційною документацією, при цьому розробником не визначено функціональні специфікації ОЕ;
- ОЕ у вигляді ЗТЗІ від НСД або захищеного компонента обчислювальної системи подано на експертизу представником розробника (заявником), який не володіє інформацією щодо особливостей реалізації в ОЕ функцій захисту, разом з експлуатаційною документацією, при цьому розробником не визначено функціональні специфікації ОЕ.

5.2.2 Для досягнення поставленої мети етап проведення попереднього аналізу оцінюваного ОЕ передбачає виконання таких дій:

- дослідження оцінюваного ОЕ з метою перевірки його готовності до виконання робіт з експертизи;
- визначення (ідентифікація) або уточнення множини випробовуваних функціональних послуг безпеки, їх рівнів та політики;
- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів робіт.

5.2.2.1 У процесі дослідження оцінюваного ОЕ експертом має бути сформовано чітке уявлення про:

- інформаційну модель процесів оброблення інформації в оцінюваному ОЕ;
- оброблювані інформаційні ресурси і можливі загрози цим ресурсам;
- функціональні вимоги до оцінюваного ОЕ, в тому числі ті, що стосуються забезпечення захисту інформації від можливих загроз;
- засоби керування оцінюваним ОЕ.

При цьому необхідна інформація може отримуватися такими шляхами:

- ознайомлення з наданою документацією;
- анкетування розробників оцінюваного ОЕ;
- дослідження експертами оцінюваного ОЕ.

5.2.2.2 На основі результатів дослідження оцінюваного ОЕ, у випадку, якщо отримані результати підтверджують його готовність до проведення подальших робіт (слід розуміти, як мінімум, підтвердження працездатності ОЕ у заявлених умовах та функціонування згідно з характеристиками, наведеними в експлуатаційній документації), має бути здійснено визначення (ідентифікацію) або уточнення множини випробовуваних функціональних послуг безпеки, їх рівнів та політики. При цьому, за наявності у проектній або експлуатаційній документації чітко визначених функціональних специфікацій ОЕ, таку ідентифікацію (уточнення) можна здійснювати шляхом аналізу відповідності формальних вимог до функціональних послуг безпеки (функцій захисту) та опису порядку реалізації відповідних функцій в оцінюваному ОЕ, наведеного в проектній документації, а також результатів анкетування розробників з використанням переліку спеціальних запитань. За відсутності у проектній документації чітко визначених функціональних специфікацій ОЕ таку ідентифікацію можна здійснювати шляхом проведення експертами досліджень оцінюваного ОЕ, метою яких є ідентифікація (виявлення наявності) механізмів захисту та реалізованих ними функціональних послуг безпеки, оцінювання можливості запобігання ними певним загрозам інформації з подальшим уточненням політики функціональних послуг безпеки з використанням переліку спеціальних запитань. Методичні рекомендації щодо здійснення ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики викладено в розділі 6.

5.2.3 Результатом етапу попереднього аналізу має бути звіт, у якому експерти, що здійснювали аналіз, повинні викласти свою думку з приводу повноти і вмісту наданих матеріалів, обґрунтувати рішення щодо можливості та доцільності проведення подальших робіт з експертизи, а у випадку позитивного рішення – навести пропозиції щодо плану та послідовності проведення подальших робіт. Крім цього, у випадку позитивного рішення щодо проведення подальших робіт, результатом цього етапу має також бути узгоджений з розробником або заявником документ, що містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка ОЕ, наприклад, у вигляді технічних вимог до оцінюваного ОЕ в частині реалізації функціональних послуг безпеки та опису порядку реалізації цих вимог. Цей документ, у випадку успішного завершення експертизи, має бути поданий як невід'ємний додаток до експертного висновку щодо відповідності оцінюваного ОЕ вимогам НД ТЗІ.

5.2.4 У випадку подання розробником на експертизу ОЕ з визначеними у проектній документації функціональними специфікаціями експерт на етапі попереднього аналізу повинен використовувати:

- оцінюваний ОЕ у працездатному стані;

- проектну документацію на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації ОЕ у вигляді переліку реалізованих у ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики;

- експлуатаційну документацію на оцінюваний ОЕ (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо).

При цьому послідовність (алгоритм) дій експерта на етапі попереднього аналізу має бути такою (рисунок 1):

- перевірка факту надання експлуатаційної документації на ОЕ (опису засобу або системи; опису процедур інсталяції, генерації та запуску; настанови адміністратора; настанови користувача тощо) та наявності в ній відомостей, необхідних для виконання подальших робіт з оцінювання працездатності ОЕ. У випадку відсутності документації, подальші роботи мають припинятися;

- оцінювання працездатності поданого ОЕ (з використанням отриманої експлуатаційної документації) і визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності ОЕ, подальші роботи мають припинятися;

- перевірка наявності проектної документації на ОЕ (матеріалів передпроектних досліджень, технічного завдання, технічних вимог, матеріалів ескізного, технічного та робочого проектів тощо) і наявності в ній функціональних специфікацій ОЕ у вигляді переліку реалізованих в ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики. У випадку відсутності документації або відсутності у ній функціональних специфікацій ОЕ має розглядатися як такий, що наданий розробником без визначеної функціональної специфікації ОЕ;

- перевірка наявності у наведеній функціональній специфікації ОЕ послуги безпеки "Цілісність КЗЗ" рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня у функціональній специфікації ОЕ, подальші роботи мають припинятися;

- перевірка наявності у наведеній функціональній специфікації ОЕ функціональних послуг безпеки певного рівня, наявність яких, згідно з вимогами НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг, з вилученням із заявленого переліку функціональних послуг тих, необхідні умови реалізації яких відсутні;

- прийняття (після консультацій з розробником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки та продовження робіт;

- уточнення (з урахуванням наведених у розділі 6 методичних рекомендацій), із залученням розробника, фактів реалізації та політики всіх

функціональних послуг безпеки, що містяться в їх уточненому переліку;

- перевірка наявності в уточненому переліку реалізованих в ОЕ функціональних послуг безпеки послуги "Цілісність КЗЗ" рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня в уточненому переліку, подальші роботи мають припинятися;

- перевірка наявності в уточненому переліку реалізованих в ОЕ функціональних послуг безпеки послуг певного рівня, наявність яких, згідно з вимогами НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг, з вилученням з уточненого переліку функціональних послуг тих, необхідні умови реалізації яких відсутні;

- прийняття (після консультацій з розробником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки, наявність яких має бути підтверджено в процесі експертизи, та про продовження робіт;

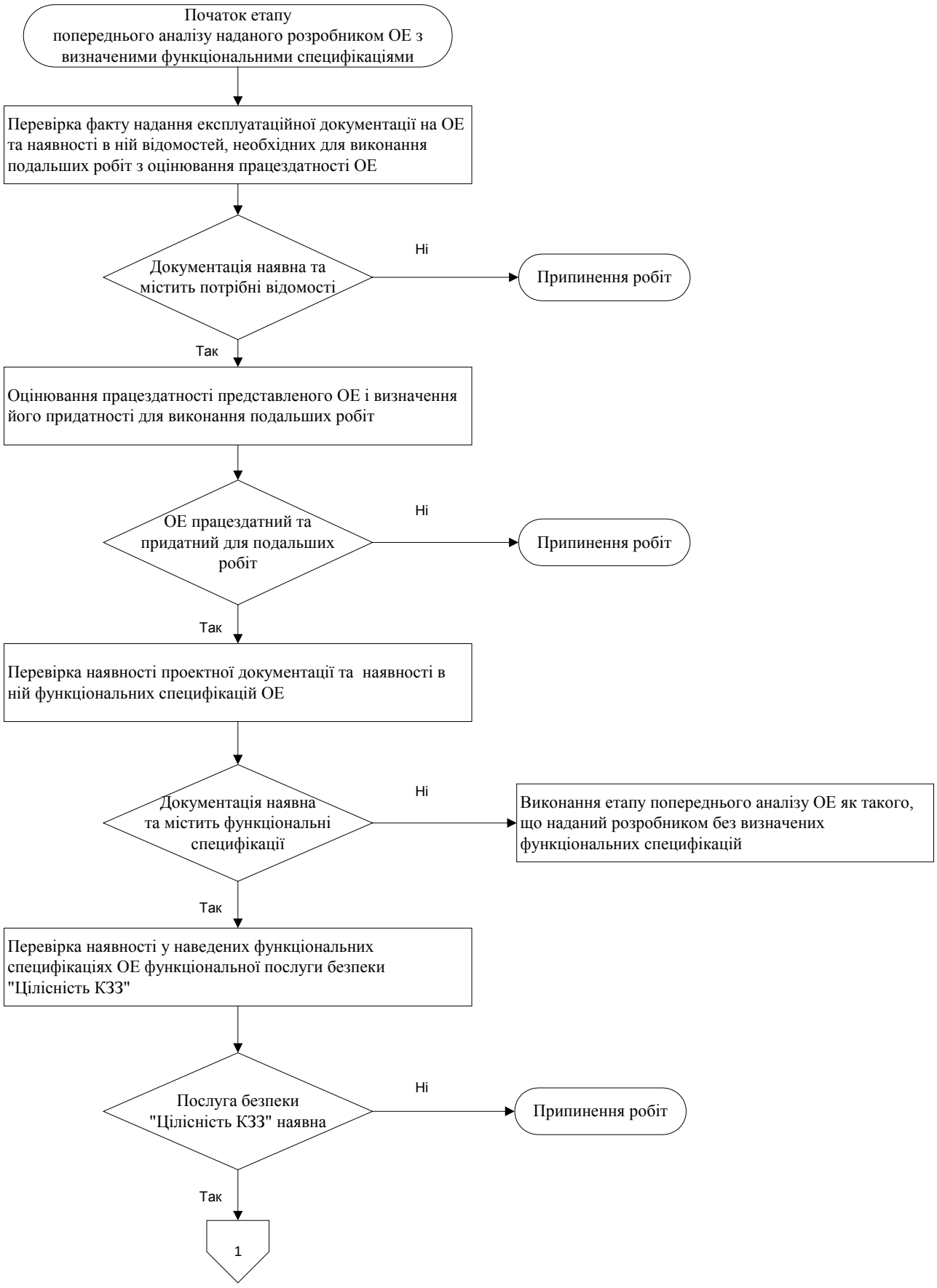

Рисунок 1 (частина 1)

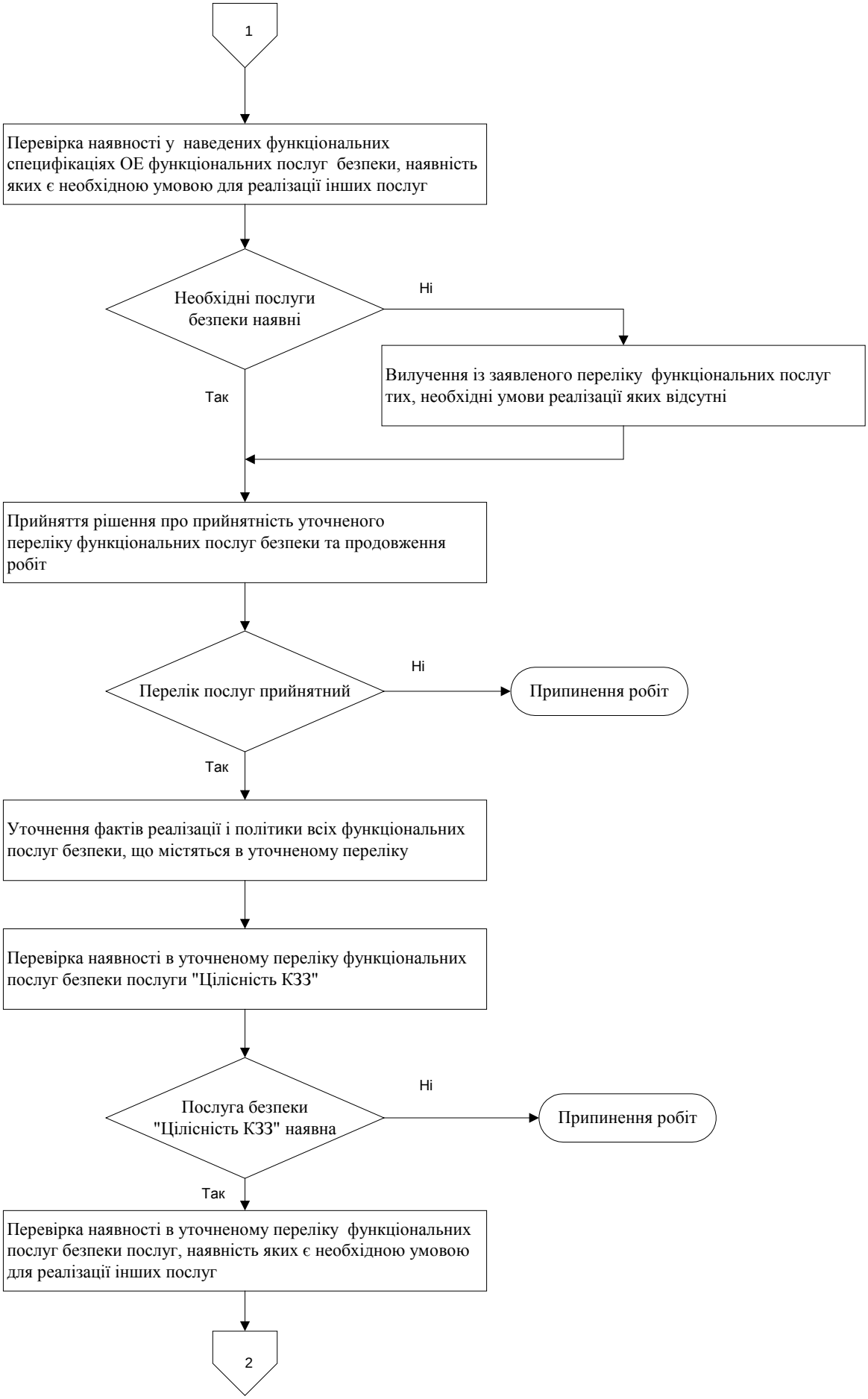

Рисунок 1 (частина 2)

EMBED Visio.Drawing.6

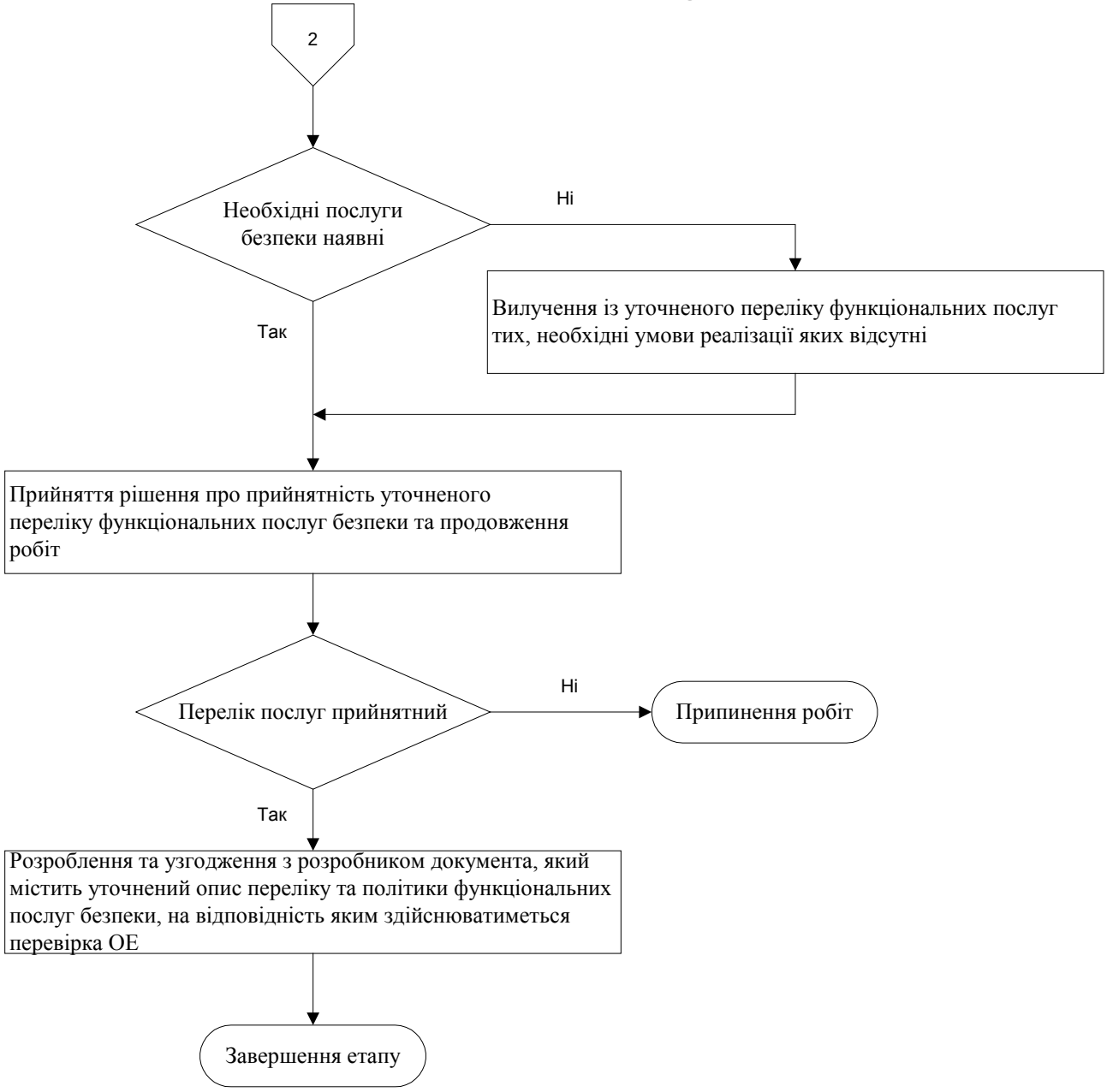

Рисунок 1 (частина 3)

- розроблення (із залученням розробника) та узгодження з розробником документа, який містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка ОЕ, наприклад, у вигляді технічних вимог до оцінюваного ОЕ в частині реалізації функціональних послуг безпеки та опису порядку реалізації цих вимог.

5.2.5 У випадку подання розробником на експертизу ОЕ без визначених функціональних специфікацій експерт на етапі попереднього аналізу повинен використовувати:

- оцінюваний ОЕ у працездатному стані;

- експлуатаційну документацію на оцінюваний ОЕ (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову

адміністратора; настанову користувача тощо).

При цьому послідовність (алгоритм) дій експерта на етапі попереднього аналізу має бути такою (рисунок 2):

Рисунок 2 (частина 1)

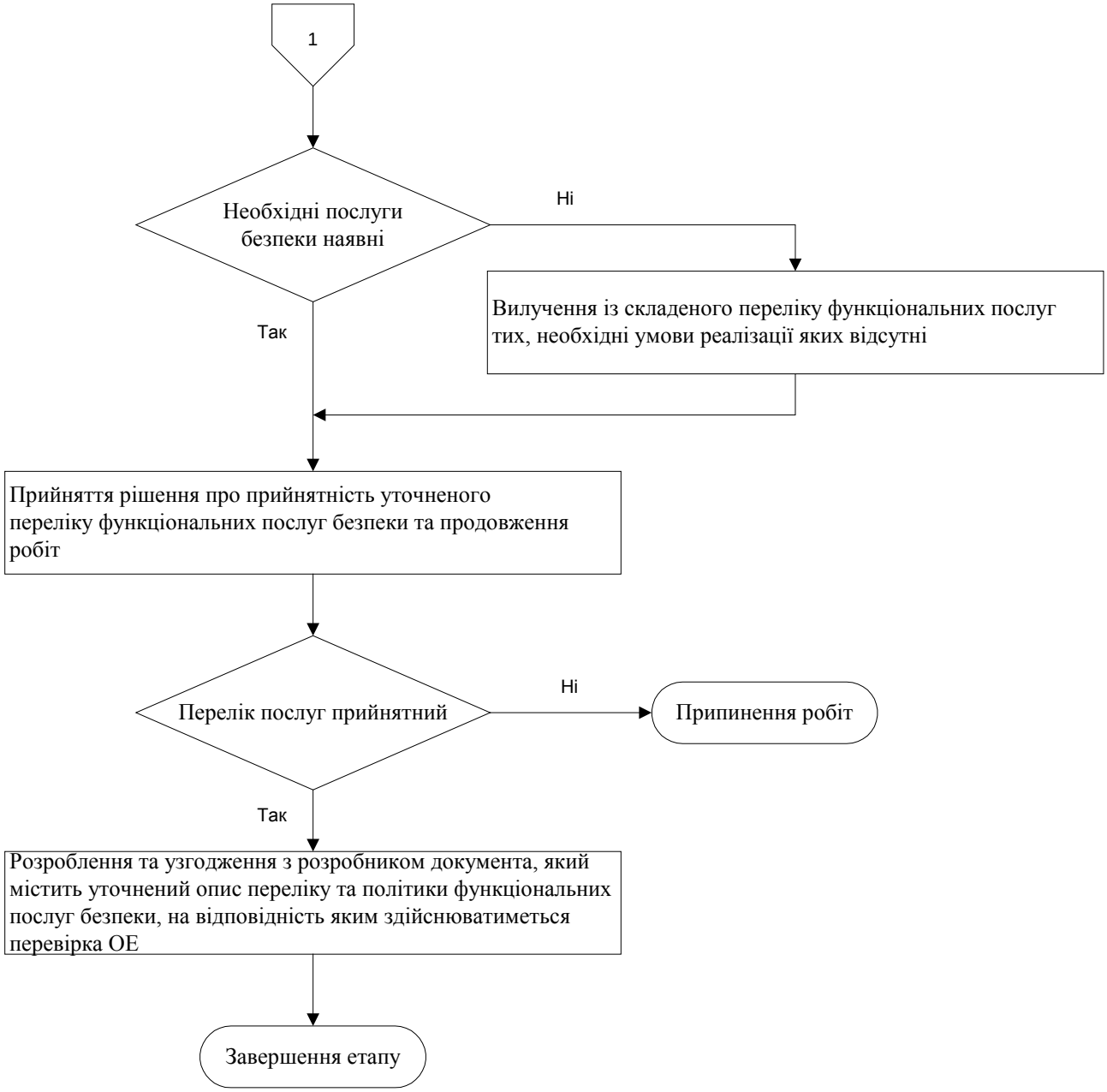

Рисунок 2 (частина 2)

- перевірка факту надання експлуатаційної документації на ОЕ (опису засобу або системи; опису процедур інсталяції, генерації та запуску; настанови адміністратора; настанови користувача тощо) та наявності в ній відомостей, необхідних для виконання подальших робіт з оцінювання працездатності ОЕ. У випадку відсутності документації, подальші роботи мають припинятися;

- оцінювання працездатності поданого ОЕ (з використанням отриманої експлуатаційної документації) і визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності ОЕ, подальші роботи мають припинятися;

- проведення (з урахуванням наведених у розділі 6 методичних рекомендацій), із залученням розробника, ідентифікації фактів реалізації та уточнення політики функціональних послуг безпеки;

- перевірка наявності у складеному переліку реалізованих в ОЕ функціональних послуг безпеки послуги "Цілісність КЗЗ" рівня НЦ-1 або вище. У випадку, якщо така функціональна послуга безпеки відсутня у складеному переліку, подальші роботи мають припинятися;

- перевірка наявності у складеному переліку реалізованих в ОЕ функціональних послуг безпеки послуг певного рівня, наявність яких, згідно з вимогами НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг, з вилученням з переліку функціональних послуг тих, необхідні умови реалізації яких відсутні;

- прийняття (після консультацій з розробником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки, наявність яких має бути підтверджено в процесі експертизи, та про продовження робіт;

- розроблення (із залученням розробника) та узгодження з розробником документа, який містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка ОЕ, наприклад, у вигляді уточнених технічних вимог до оцінюваного ОЕ в частині реалізації функціональних послуг безпеки та опису порядку реалізації цих вимог.

5.2.6 У випадку подання на експертизу представником розробника (заявником) ОЕ без визначених функціональних специфікацій, експерт на етапі попереднього аналізу має використовувати:

- ОЕ у працездатному стані, наданий для аналізу;

- експлуатаційну документацію на оцінюваний ОЕ (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо).

При цьому послідовність (алгоритм) дій експерта на етапі попереднього аналізу має бути такою (рисунок 3):

- перевірка факту надання експлуатаційної документації на ОЕ (опису засобу або системи; опису процедур інсталяції, генерації та запуску; настанови адміністратора; настанови користувача тощо) та наявності в ній відомостей, необхідних для виконання подальших робіт з оцінювання працездатності ОЕ. У випадку відсутності документації, подальші роботи мають припинятися;

- оцінювання працездатності наданого ОЕ (з використанням отриманої експлуатаційної документації) і визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності ОЕ, подальші роботи мають припинятися;

- виконання (з урахуванням наведених у розділі 6 методичних рекомендацій) власними силами дослідження ОЕ з метою ідентифікації фактів реалізації та уточнення політики функціональних послуг безпеки;

- перевірка наявності у складеному переліку реалізованих в ОЕ функціональних послуг безпеки послуги "Цілісність КЗЗ" рівня НЦ-1 або вище.

У випадку, якщо така функціональна послуга безпеки відсутня у складеному переліку, подальші роботи мають припинятися;

- перевірка наявності у складеному переліку реалізованих в ОЕ функціональних послуг безпеки послуг певного рівня, наявність яких, згідно з вимогами НД ТЗІ 2.5-004-99, є необхідною умовою для реалізації інших послуг, з вилученням з переліку функціональних послуг тих, необхідні умови реалізації яких відсутні;

- прийняття (після консультацій із заявником) рішення про прийнятність уточненого переліку реалізованих функціональних послуг безпеки, наявність яких має бути підтверджено в процесі експертизи, та про продовження робіт;

- розроблення та узгодження із заявником документа, який містить уточнений опис переліку та політики функціональних послуг безпеки, на відповідність яким здійснюватиметься перевірка ОЕ, наприклад, у вигляді технічних вимог до оцінюваного ОЕ в частині реалізації функціональних послуг безпеки та опису порядку реалізації цих вимог.

Рисунок 3 (частина 1)

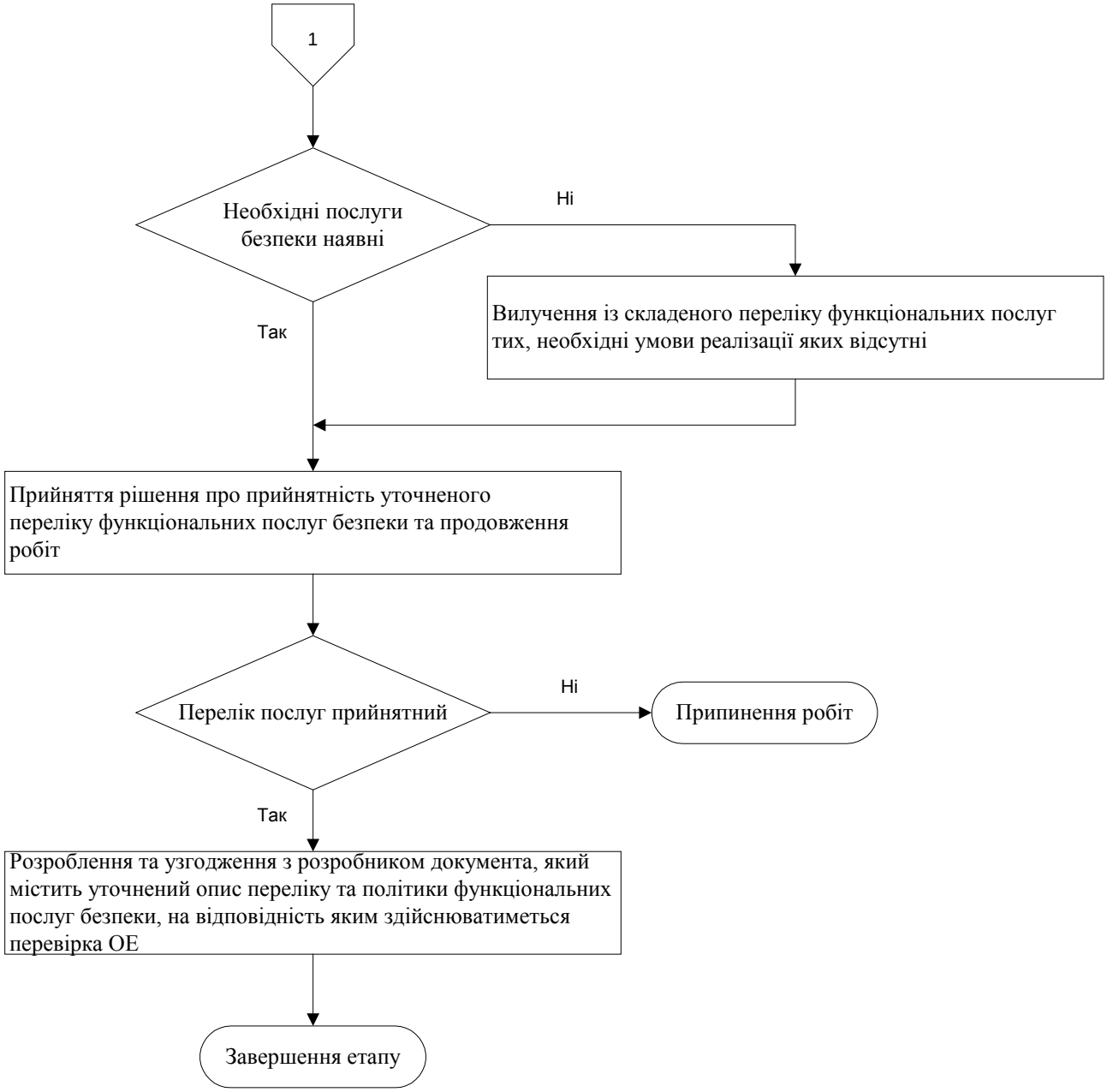

Рисунок 3 (частина 2)

5.3 Розроблення програми випробувань функціональних послуг безпеки

5.3.1 Головною метою цього етапу є розроблення та погодження у встановленому порядку програми проведення випробувань функціональних послуг безпеки. При цьому експертом, залежно від варіанта подання ОЕ на експертизу, на цьому етапі мають використовуватися:

- проектна документація (за наявності) на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації ОЕ у вигляді переліку реалізованих у ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики;

- документація (за наявності), що містить результати проведених розробником випробувань ОЕ (програма випробувань, методика випробувань,

протоколи випробувань тощо);

- підготовлений на етапі попереднього аналізу документ, який містить уточнений опис переліку та політики функціональних послуг безпеки, наприклад, у вигляді уточнених технічних вимог до оцінюваного ОЕ, на відповідність яким має здійснюватися перевірка ОЕ.

5.3.2 Основний зміст програми випробувань, яка розробляється на цьому етапі, становить опис того, що саме, тобто, які властивості оцінюваного ОЕ мають бути перевірені під час проведення випробувань з метою підтвердження або спростування реалізації в оцінюваному ОЕ уточненого на етапі попереднього аналізу переліку функціональних послуг безпеки. При визначенні цих властивостей в першу чергу слід керуватися наведеними в НД ТЗІ 2.5-004-99 вимогами щодо політики окремих функціональних послуг безпеки різних рівнів, а також результатами етапу попереднього аналізу. Крім цього, можуть бути враховані такі чинники:

- результати випробувань, надані розробником ОЕ. Мають бути враховані: аргументи розробника про достатність тестового покриття для тестування певних функціональних послуг безпеки; можливість розширення прийнятого розробником підходу; повнота і коректність проведених розробником випробувань функціональних послуг безпеки;

- відомі вразливості, характерні для того типу систем, до яких відноситься оцінюваний ОЕ, в тому числі наведені у матеріалах передпроектних досліджень;

- важливість різних функціональних послуг безпеки, реалізованих в оцінюваному ОЕ, з погляду запобігання можливим загрозам інформації;

- складність (комплексність) засобів реалізації функціональних послуг безпеки в оцінюваному ОЕ;

- можливість неявної перевірки окремих функціональних послуг безпеки;

- наявність в оцінюваному ОЕ нових або нерегламентованих НД ТЗІ функцій захисту.

5.3.3 Методичні вказівки з розроблення та документування програми випробувань функціональних послуг безпеки викладено в розділі 7.

Результатом етапу має бути розроблена та, згідно з вимогами Положення про державну експертизу у сфері технічного захисту інформації, погоджена із замовником експертизи і Державною службою спеціального зв’язку та захисту інформації України програма випробувань функціональних послуг безпеки.

5.4 Розроблення методики випробувань функціональних послуг безпеки

5.4.1 Головною метою цього етапу є розроблення та погодження у встановленому порядку методики проведення випробувань функціональних послуг безпеки. У процесі підготовки методики випробувань мають також бути виконані дії з вибору тестових процедур, методів випробувань і відповідних перевірок, розроблення (вибору) необхідних для випробувань програмних та/або апаратних засобів (засобів випробувань). При цьому експерт, залежно

від варіанта подання ОЕ на експертизу, на цьому етапі має використовувати:

- ОЕ у працездатному стані, підготовлений для проведення випробувань;

- проектну документацію (за наявності) на оцінюваний ОЕ (наприклад, матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації ОЕ у вигляді переліку реалізованих у ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики;

- експлуатаційну документацію на оцінюваний ОЕ (наприклад, опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);

- документацію (за наявності), що містить результати проведених розробником випробувань ОЕ (програму випробувань, методику випробувань, протоколи випробувань тощо);

- підготовлений на етапі попереднього аналізу документ, який містить уточнений
опис переліку та політики функціональних послуг безпеки, наприклад, у вигляді уточнених технічних вимог до оцінюваного ОЕ, на відповідність яким має здійснюватися перевірка ОЕ;

- підготовлену на попередньому етапі програму випробувань функціональних послуг безпеки.

5.4.2 У процесі розроблення методики випробувань, яка описує порядок та засоби проведення випробувань кожної функціональної послуги безпеки, зазначеної у програмі випробувань, експерт має, з урахуванням уточнених вимог до функціональних послуг безпеки, визначених на попередніх етапах, обрати найбільш прийнятний спосіб перевірки кожної послуги.

5.4.3 Під час розроблення методики випробувань мають враховуватися такі основні вимоги щодо загального підходу (стратегії) проведення випробувань:

- забезпечення достатності тестового покриття для перевірки кожної заявленої функціональної послуги безпеки з урахуванням її політики та особливостей реалізації;

- зниження кількості взаємозалежних методів випробувань (перевірок) різних функціональних послуг безпеки;

- забезпечення максимальної незалежності від стану оцінюваного ОЕ, тобто наявності засобів генерації всієї необхідної тестової та службової інформації для кожної перевірки;

- забезпечення максимального використання засобів автоматизації при проведенні випробувань, у тому числі для генерації тестової інформації, виконання підготовчих дій і безпосереднього виконання перевірок;

- забезпечення повторюваності процесу і результатів випробувань.

5.4.4 При виборі тестових процедур, методів випробувань і відповідних перевірок, залежно від виду оцінюваного ОЕ, можуть бути обрані такі підходи:

- підхід з використанням монолітного тестування (метод "чорної скриньки"), який передбачає використання в процесі проведення випробувань лише зовнішніх документованих інтерфейсів оцінюваного ОЕ, завдяки чому випробування можуть бути здійснені без використання додаткових спеціально розроблюваних засобів;

- підхід з використанням функціонально-синтетичного тестування (метод "білої скриньки"), який передбачає використання в процесі проведення випробувань як зовнішніх документованих інтерфейсів ОЕ, так і внутрішньосистемних інтерфейсів, але потребує спеціально розроблених засобів випробувань, що реалізують внутрішньосистемні інтерфейси доступу до функціональних компонентів оцінюваного продукту (системи);

- змішаний підхід (метод "сірої скриньки"), при використанні якого намагаються максимальну кількість перевірок здійснювати з використанням зовнішніх документованих інтерфейсів, а внутрішньосистемні інтерфейси використовувати лише для тих перевірок, які не можна виконати в інший спосіб.

5.4.5 Оскільки, згідно з НД ТЗІ, наявність, повнота та ступінь детальності опису внутрішньосистемних інтерфейсів залежать від заявленого рівня гарантій коректності реалізації функціональних послуг безпеки, вибір підходу щодо проведення випробувань має здійснюватися з урахуванням цього рівня гарантій.

5.4.6 Методичні вказівки з розроблення та документування методики випробувань функціональних послуг безпеки викладено в розділі 8.

Результатом етапу має бути розроблена та, згідно з вимогами Положення про державну експертизу у сфері технічного захисту інформації, погоджена з Державною службою спеціального зв’язку та захисту інформації України методика випробувань функціональних послуг безпеки.

5.5 Проведення випробувань

Головною метою цього етапу є здійснення, згідно із затвердженою методикою, перевірки та фіксації (у відповідному журналі проведення випробувань) фактів реалізації в оцінюваному ОЕ заявленого та уточненого експертом переліку функціональних послуг безпеки, а також підтвердження їх політики, уточненої експертом на етапі попереднього аналізу. При цьому, якщо в процесі проведення випробувань здійснювалася перевірка будь-яких додаткових властивостей ОЕ (наприклад, продуктивності або стійкості до проникнення), відповідні результати також мають бути зафіксовані.

5.6 Аналіз, документування та затвердження результатів випробувань

На цьому етапі має бути проведено аналіз отриманих у процесі проведення випробувань та зафіксованих відповідним чином результатів. На підставі результатів проведеного аналізу має бути складено протокол випробувань, в якому повинно бути наведено результати, отримані під час проведення випробувань за кожним пунктом методики випробувань, та зроблено висновок щодо відповідності або невідповідності наданого для випробувань ОЕ висунутим вимогам.

Методичні вказівки з виконання аналізу та документування результатів випробувань викладено в розділі 9.

Затверджений організатором експертизи протокол є підставою для підготовки та надання до Державної служби спеціального зв'язку та захисту інформації України для затвердження експертного висновку щодо відповідності або невідповідності оцінюваного ОЕ вимогам НД ТЗІ в Україні.

6 Методичні рекомендації з ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики

6.1 Основні зусилля в процесі виконання цього етапу робіт повинні бути спрямовані, у першу чергу, на максимально коректну і ретельну ідентифікацію (виявлення наявності) засобів, що реалізують різні функціональні послуги безпеки. Таку ідентифікацію доцільно виконувати шляхом виявлення в оцінюваному ОЕ тих чи інших механізмів, що реалізують різні функції захисту, з подальшим аналізом того, наскільки ця функціональність відповідає вимогам НД ТЗІ 2.5-004-99 до різних функціональних послуг безпеки. Лише після прийняття рішення про факт наявності в ОЕ засобів реалізації тієї чи іншої послуги має виконуватися уточнення її політики, тобто множини об'єктів, стосовно яких реалізована послуга, а також порядку і правил функціонування механізмів, що реалізують послугу.

6.2 У процесі проведення ідентифікації засобів, що реалізують різні функції захисту, та співставлення цих функцій з вимогами НД ТЗІ 2.5-004-99 для подання на експертизу розробником ОЕ з визначеними функціональними специфікаціями у вигляді переліку реалізованих у ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики експерт має використовувати:

- проектну документацію на оцінюваний ОЕ (матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації ОЕ;
- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);
- результати дослідження експертами оцінюваного ОЕ;
- результати анкетування розробників оцінюваного ОЕ.

При цьому послідовність (алгоритм) дій експерта має бути такою (рисунок 4):

- уточнення складу та архітектури КЗЗ оцінюваного ОЕ шляхом анкетування розробника (з використанням запитань, наведених у розділі А.1 Додатка А) та подальшого контролю експертом достовірності та повноти наданих відповідей на основі результатів власних досліджень;

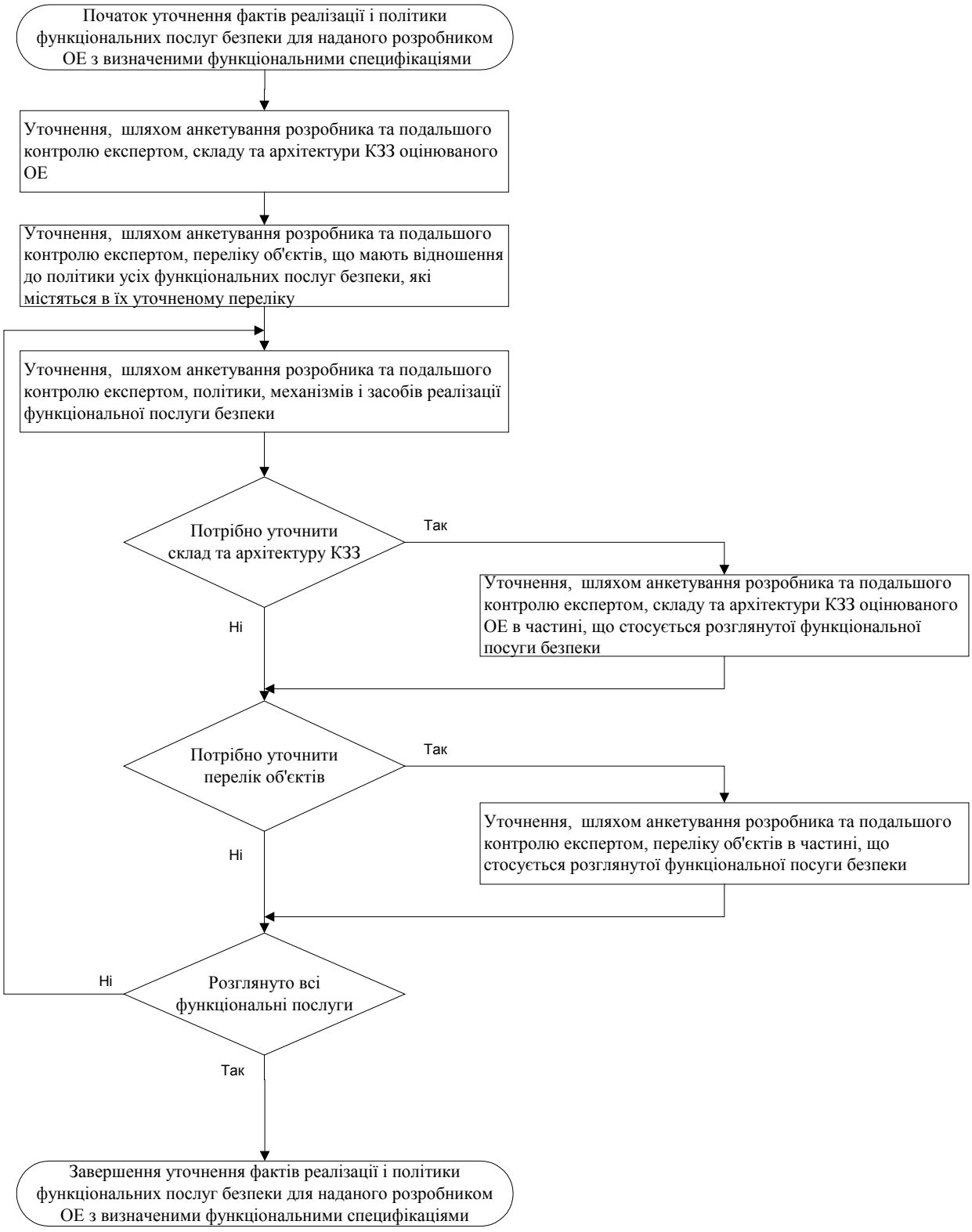

Рисунок 4

- уточнення переліку об'єктів, які мають відношення до політики всіх функціональних послуг безпеки, що містяться в їх уточненому переліку, шляхом анкетування розробника (з використанням запитань, наведених у розділі А.2 Додатка А) та подальшого контролю експертом достовірності та повноти наданих відповідей на основі результатів власних досліджень;

- уточнення політики, механізмів і засобів реалізації всіх функціональних

послуг безпеки, що містяться в їх уточненому в процесі проведення попереднього аналізу переліку, шляхом анкетування розробника (з використанням запитань, наведених у розділах А.3 – А.22 Додатка А) та подальшого контролю експертом достовірності та повноти наданих відповідей на основі результатів власних досліджень. При цьому, за необхідності, можуть бути уточнені також склад та архітектура КЗЗ оцінюваного ОЕ, а також перелік об'єктів, що мають відношення до політики певної функціональної послуги безпеки.

6.3 У процесі проведення ідентифікації засобів, що реалізують різні функції захисту, і співставлення цих функцій з вимогами НД ТЗІ 2.5-004-99 для наданого на експертизу розробником ОЕ без визначених функціональних специфікацій експерт має використовувати:

- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);
- результати дослідження експертами оцінюваного ОЕ;
- результати анкетування розробників оцінюваного ОЕ.

При цьому послідовність (алгоритм) дій експерта має бути такою (рисунок 5):

- уточнення складу та архітектури КЗЗ оцінюваного ОЕ шляхом анкетування розробника (з використанням запитань, наведених у розділі А.1 Додатка А) та подальшого контролю експертом достовірності та повноти наданих відповідей на основі результатів власних досліджень;
- уточнення переліку об'єктів, які, можливо, мають відношення до політики реалізованих функціональних послуг безпеки, шляхом анкетування розробника (з використанням запитань, наведених у розділі А.2 Додатка А) і подальшого контролю експертом достовірності та повноти наданих відповідей на основі результатів власних досліджень;
- ідентифікація та уточнення фактів реалізації, політики, механізмів і засобів реалізації різних функціональних послуг безпеки шляхом анкетування розробника (з використанням запитань, наведених у розділах А.3 – А.22 Додатка А) і подальшого контролю експертом достовірності та повноти наданих відповідей на основі результатів власних досліджень. При цьому, за необхідності, можуть бути уточнені також склад та архітектура КЗЗ оцінюваного ОЕ, а також перелік об'єктів, які мають відношення до політики певної функціональної послуги безпеки.

6.4 У процесі проведення ідентифікації засобів, що реалізують різні функції захисту, і співставлення цих функцій з вимогами НД ТЗІ 2.5-004-99 для наданого на експертизу представником розробника (заявником) ОЕ без визначених функціональних специфікацій експерт має використовувати:

- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);

- результати дослідження експертами оцінюваного ОЕ.

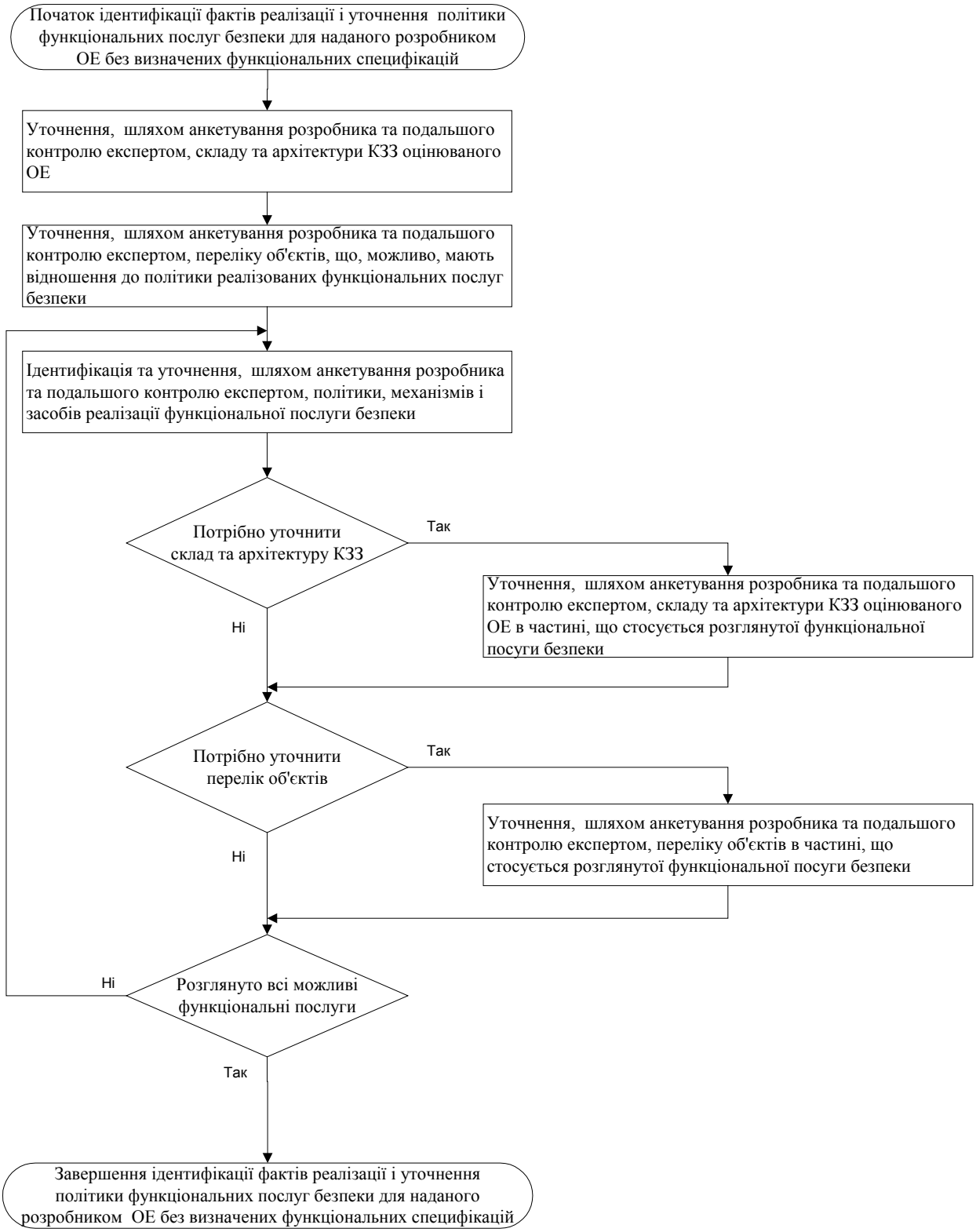

Рисунок 5

При цьому послідовність (алгоритм) дій експерта має бути такою (рисунок 6):

- уточнення складу та архітектури КЗЗ оцінюваного ОЕ шляхом дослідження ОЕ експертом та формулювання ним відповідей на запитання

розділу А.1 Додатка А;

- уточнення переліку об'єктів, які, можливо, мають відношення до політики реалізованих функціональних послуг безпеки, шляхом дослідження ОЕ експертом та формулювання ним відповідей на запитання розділу А.2 Додатка А;

- ідентифікація та уточнення фактів реалізації, політики, механізмів і засобів реалізації різних функціональних послуг безпеки та формулювання ним відповідей на запитання, що містяться в розділах А.3 – А.22 Додатка А. При цьому, за необхідності, можуть бути уточнені також склад та архітектура КЗЗ оцінюваного ОЕ, а також перелік об'єктів, які мають відношення до політики певної функціональної послуги безпеки.

6.5 Наведений у Додатку А перелік запитань, яким рекомендується скористатися в процесі проведення ідентифікації різних функціональних послуг безпеки, визначення їх рівнів і політики, складено з урахуванням вимог НД ТЗІ 2.5-004-99 до реалізації різних функціональних послуг, а також наведених у міжнародних стандартах та інших нормативних документах правил і особливостей функціонування механізмів захисту, що можуть використовуватися для реалізації відповідних послуг. У переліку запитань наведено також коментарі, які повинні дати експерту, з урахуванням відповідей на запитання, такі можливості: по-перше, прийняти рішення про факт наявності чи відсутності в оцінюваному ОЕ засобів, що реалізують ту чи іншу функціональну послугу безпеки; по-друге, уточнити її рівень і політику; по-третє, усвідомити механізми і засоби реалізації послуги, правила і порядок їх функціонування.

Відповіді на наведені в переліку запитання повинні формулюватися максимально докладно. При формулюванні відповідей на запитання, які вимагають наведення різних структур даних, використовуваних у процесі функціонування засобів реалізації функціональних послуг безпеки (наборів атрибутів доступу об'єктів, маркерів причетності тощо), або правил функціонування різних механізмів (протоколів автентифікації, правил оброблення запитів на надання доступу тощо), необхідно враховувати передбачуваний підхід до проведення випробувань засобів реалізації функціональних послуг. У випадку, якщо передбачається використовувати підхід монолітного тестування (рекомендується для ОЕ із заявленим рівнем гарантій коректності реалізації функціональних послуг безпеки Г-2 і нижче згідно з НД ТЗІ 2.5-004-99), описи відповідних структур даних і правил функціонування мають бути наведені у вигляді, що може бути заданий, змінений або перевірений з використанням лише зовнішніх інтерфейсів ОЕ. У випадку, якщо для випробувань засобів реалізації функціональних послуг безпеки передбачається використовувати підхід функціонально-синтетичного тестування (рекомендується для ОЕ із заявленим рівнем гарантій коректності реалізації функціональних послуг безпеки Г-3 і вище згідно з НД ТЗІ 2.5-004-99), описи відповідних структур даних і правил функціонування мають бути наведені у вигляді, що може бути заданий, змінений або перевірений з

використанням як зовнішніх, так і внутрішньосистемних інтерфейсів ОЕ.

6.6 Результати здійсненої ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики мають бути викладені у відповідному документі у вигляді технічних вимог до реалізованих функціональних послуг безпеки та опису порядку реалізації цих вимог. Вимоги до функціональних послуг безпеки та опис порядку їх реалізації повинні викладатися з урахуванням вимог НД ТЗІ 2.5-004-99 і результатів відповіді на запитання Додатка А. Розроблений документ має бути узгоджений з розробником ОЕ або заявником, який є представником розробника ОЕ. У процесі підготовки документа необхідно керуватися вимогами ГОСТ 34.602-89, ГОСТ 19.201-78, ГОСТ 19.404-79, інших стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, що стосуються документування результатів різних етапів проектування.

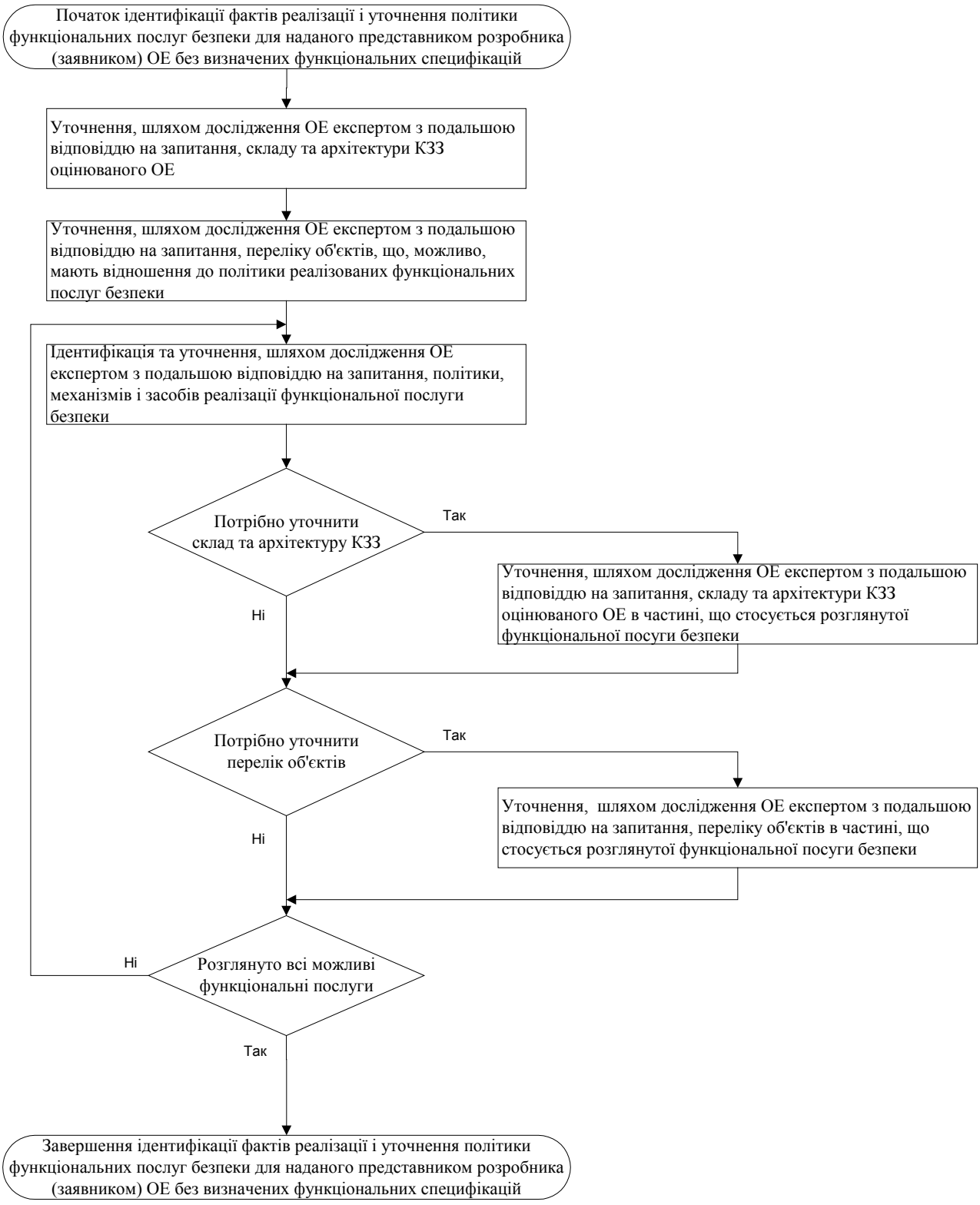

Рисунок 6

7 Методичні вказівки з розроблення та документування програми випробувань функціональних послуг безпеки

7.1 Оскільки основний зміст програми випробувань функціональних послуг безпеки має складати опис того, що саме, тобто, які властивості оцінюваного ОЕ мають бути перевірені під час проведення випробувань з метою підтвердження або спростування реалізації в оцінюваному ОЕ уточненого на етапі попереднього аналізу переліку функціональних послуг

безпеки, основні зусилля повинні бути спрямовані на те, щоб максимально повно відобразити в ній перелік тих перевірок (без наведення конкретних методів їх виконання), успішне виконання яких дозволить дійти обґрунтованого висновку про факт реалізації в оцінюваному ОЕ функціональної послуги безпеки певного рівня згідно із задекларованою політикою. Для цього програма випробувань має передбачати:

- виконання перевірок усіх вимог НД ТЗІ 2.5-004-99 до політики і порядку функціонування засобів, що реалізують усі визначені на етапі попереднього аналізу функціональні послуги безпеки, з урахуванням уточненої політики цих послуг і охопленням усіх об'єктів і засобів, на які поширюється ця політика;

- виконання перевірок усіх вимог НД ТЗІ 2.5-004-99, що стосуються реалізації необхідних умов (у вигляді функціональних послуг безпеки або рівня гарантій коректності їх реалізації) для всіх визначених на етапі попереднього аналізу функціональних послуг безпеки.

7.2 При розробленні програми випробувань функціональних послуг безпеки, залежно від варіанта подання ОЕ на експертизу, експерт має використовувати:

- проектну документацію на оцінюваний ОЕ (матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації у вигляді переліку реалізованих у ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики;

- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);

- документацію, що містить результати проведених розробником випробувань ОЕ (програму випробувань, методику випробувань, протоколи випробувань тощо);

- підготовлений на етапі попереднього аналізу документ, який містить уточнений опис переліку, політики функціональних послуг безпеки та порядку їх реалізації.

Крім цього, при формулюванні вимог програми випробувань функціональних послуг безпеки необхідно користуватися Додатком Б, у якому викладено вимоги до змісту програми випробувань різних функціональних послуг безпеки різних рівнів. Викладені вимоги сформульовані з урахуванням вимог НД ТЗІ 2.5-004-99, а також результатів виконаної з використанням переліку спеціальних запитань, наведеного в Додатку А, ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики.

7.3 При документуванні програми випробувань функціональних послуг безпеки, розробленої з урахуванням наведених вище та викладених у Додатку Б вимог, необхідно керуватися також вимогами Положення про державну експертизу у сфері технічного захисту інформації, ГОСТ 19.301-79, ДСТУ

2853-94, інших стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, що стосуються підготовлення та проведення випробувань.

8 Методичні вказівки з розроблення та документування методики випробувань функціональних послуг безпеки

8.1 Основний зміст методики випробувань функціональних послуг безпеки має складати виконаний з урахуванням вимог програми випробувань опис переліку, послідовності, порядку і методів виконання перевірок, метою яких є підтвердження фактів реалізації в оцінюваному ОЕ функціональних послуг безпеки певних рівнів згідно із задекларованою політикою. При цьому з метою забезпечення максимально достовірних результатів випробувань необхідно звернути особливу увагу на вибір підходу до тестування засобів реалізації функціональних послуг безпеки, а також вибір тестових даних.

8.2 Підхід монолітного тестування, який передбачає використання в процесі проведення випробувань лише зовнішніх документованих інтерфейсів оцінюваного ОЕ, має такі переваги:

- може використовуватися як розробниками, так і експертами;
- не вимагає знань особливостей внутрішньої реалізації різних функціональних послуг безпеки;
- відсутня необхідність порушення штатного режиму функціонування ОЕ та реалізованих у ньому засобів захисту;
- не потребує використання додаткових спеціальних засобів випробувань.

Але йому притаманні і недоліки:

- складність вибору достатнього тестового покриття без аналізу вхідного коду та особливостей внутрішньої реалізації ОЕ;
- складність усунення з тестового покриття надлишкових перевірок для різних функцій захисту, що реально реалізуються одними і тими ж функціональними компонентами;
- складність усунення взаємних залежностей між різними перевірками.

Цей підхід рекомендується використовувати при оцінюванні ОЕ із заявленим рівнем гарантій коректності реалізації функціональних послуг безпеки Г-2 і нижче згідно з НД ТЗІ 2.5-004-99.

8.3 Підхід функціонально-синтетичного тестування, який передбачає використання у процесі тестування як зовнішніх документованих інтерфейсів ОЕ, так і внутрішньосистемних інтерфейсів, порівняно з підходом монолітного тестування, має такі переваги:

- тестове покриття є більш повним і точним, тому що охоплює всі аспекти реалізації функціональних послуг безпеки;
- існують досить нескладні можливості усунення взаємних залежностей між різними перевірками.

Але йому притаманні і недоліки:

- можливість використання лише за наявності детальної інформації про

внутрішню структуру ОЕ та порядок організації взаємодії між його різними функціональними компонентами;

- можливість усунення з тестового покриття лише невеликої кількості надлишкових перевірок для різних функціональних послуг безпеки, реалізованих різними групами функціональних компонентів;

- необхідність використання спеціально розроблених засобів випробувань, у тому числі апаратних, які реалізують внутрішньосистемні інтерфейси доступу до функціональних компонентів оцінюваного ОЕ.

У зв'язку з необхідністю наявності детальної інформації про внутрішню структуру ОЕ та порядок організації взаємодії між його різними функціональними компонентами цей підхід може бути використаний лише при оцінюванні ОЕ із заявленим рівнем гарантій коректності реалізації функціональних послуг безпеки Г-3 і вище згідно з НД ТЗІ 2.5-004-99.

8.4 Найбільш прийнятним при оцінюванні ОЕ із заявленим рівнем гарантій коректності реалізації функціональних послуг безпеки Г-3 і вище згідно з НД ТЗІ 2.5-004-99 є змішаний підхід, при якому частина функціональних послуг випробовується з використанням підходу монолітного тестування, а частина – з використанням підходу функціонально-синтетичного тестування. При цьому для послуг, необхідною умовою реалізації яких у НД ТЗІ 2.5-004-99 зазначено вимогу забезпечення рівня гарантій коректності реалізації функціональних послуг безпеки Г-3 і вище, рекомендується використовувати лише підхід функціонально-синтетичного тестування.

8.5 Що стосується процесу вибору тестових даних, то його результати мають забезпечувати незалежність різних груп виконуваних перевірок (для виключення можливого взаємного впливу результатів перевірки одних функцій на результати перевірки інших), при цьому має також забезпечуватися достатність тестового покриття.

8.6 При розробленні методики випробувань функціональних послуг безпеки, залежно від варіанта подання ОЕ на експертизу, експерт має використовувати:

- ОЕ у працездатному стані, підготовлений для проведення випробувань;

- проектну документацію на оцінюваний ОЕ (матеріали передпроектних досліджень, технічне завдання, технічні вимоги, матеріали ескізного, технічного та робочого проектів тощо), яка, зокрема, містить функціональні специфікації ОЕ у вигляді переліку реалізованих у ОЕ функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 та опису їх політики;

- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратора; настанову користувача тощо);

- документацію, що містить результати проведених розробником випробувань ОЕ (програму випробувань, методику випробувань, протоколи випробувань тощо);

- підготовлений на етапі попереднього аналізу документ, який містить

уточнений опис переліку, політики функціональних послуг безпеки та порядку їх реалізації;

- підготовлену програму випробувань функціональних послуг безпеки.

Крім цього, при розробленні методик перевірки окремих функціональних послуг безпеки необхідно користуватися Додатком В, у якому викладено вимоги до змісту методики випробувань різних функціональних послуг безпеки різних рівнів, а також певні рекомендації щодо вибору методів випробувань. При цьому, окрім рекомендованих (або замість них), експертом можуть також бути обрані будь-які інші методи випробувань. Викладені вимоги сформульовано з урахуванням вимог НД ТЗІ 2.5-004-99, результатів проведення (з використанням наведеного в Додатку А переліку спеціальних запитань) ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики, а також вимог до програми випробувань функціональних послуг безпеки різних типів і рівнів, викладених у Додатку Б. Вимоги викладено з урахуванням необхідності забезпечення максимальної незалежності процедур випробувань різних функціональних послуг безпеки, повторюваності результатів випробувань і можливості їх однозначної інтерпретації. При розробленні, з урахуванням зазначених вимог, методики перевірки різних функціональних послуг безпеки експерт повинен звернути особливу увагу на вибір засобів випробувань, які, з урахуванням обраного підходу до тестування, повинні забезпечувати можливість виконання необхідних перевірок з використанням зовнішніх або внутрішньосистемних інтерфейсів ОЕ. Опис порядку виконання окремих перевірок обов'язково має містити: опис порядку ініціалізації ОЕ та засобів випробувань перед виконанням перевірки; опис послідовності дій, виконуваних у процесі перевірки; опис очікуваних результатів і правил їх інтерпретації. Повинна передбачатися можливість перевірки засобів реалізації функціональної послуги безпеки як у штатному, так і у позаштатному режимах функціонування, наприклад, у процесі виконання спроб НСД. При цьому слід зазначити, що остаточний аналіз та визначення стійкості реалізованих у ОЕ механізмів захисту мають здійснюватися в процесі оцінювання рівня гарантій коректності реалізованих у ОЕ функціональних послуг безпеки та не є предметом розгляду цього документа.

8.7 При документуванні методики випробувань функціональних послуг безпеки, розробленої з урахуванням наведених вище та викладених у Додатку В вимог, необхідно керуватися також вимогами Положення про державну експертизу у сфері технічного захисту інформації, ГОСТ 19.301-79, ДСТУ 2853-94, інших стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, що стосуються підготовлення та проведення випробувань.

9 Методичні вказівки з виконання аналізу та документування результатів випробувань

9.1 Оскільки головною метою цього етапу є підготовка обґрунтування для прийняття рішення щодо відповідності або невідповідності оцінюваного ОЕ висунутим вимогам, у першу чергу в процесі виконання аналізу отриманих і

зафіксованих результатів випробувань необхідно врахувати такі вимоги:

- у випадку, якщо результати проведених випробувань не дають підстав дійти висновку про реалізацію в оцінюваному ОЕ заявленої функціональної послуги безпеки певного рівня або реально реалізована в ОЕ політика послуги відрізняється від визначеної на етапі попереднього аналізу, то відповідна послуга має бути вилучена з функціонального профілю захищеності, який призначається ОЕ за результатами експертизи, або стосовно засобів її реалізації повинні бути повторно виконані дії щодо уточнення рівня послуги, її політики, доопрацювання програми і методики випробувань та проведення повторних випробувань;

- у випадку, якщо результати проведених випробувань не дають підстав дійти висновку про реалізацію в оцінюваному ОЕ певної функціональної послуги безпеки певного рівня, яка є необхідною умовою для реалізації інших функціональних послуг безпеки, то відповідні послуги мають бути вилучені з функціонального профілю захищеності, який призначається ОЕ за результатами експертизи, або стосовно засобів реалізації цих послуг повинні бути повторно виконані дії щодо уточнення рівнів послуг, їх політик, доопрацювання програми і методики випробувань та проведення повторних випробувань;

- у випадку, якщо результати проведених випробувань не дають підстав дійти висновку про реалізацію в оцінюваному ОЕ стосовно будь-якого функціонального модуля ОЕ, введеного до складу КЗЗ, послуги "Цілісність комплексу засобів захисту" рівня НЦ-1 або вище, то ОЕ не має призначатися функціональний профіль захищеності або відповідні функціональні модулі ОЕ мають розглядатися як такі, що не входять до складу КЗЗ, та, з урахуванням зміни складу КЗЗ, повинні бути повторно виконані дії щодо уточнення рівнів усіх послуг, їх політик, доопрацювання програми і методики випробувань та проведення повторних випробувань.

9.2 При документуванні результатів випробувань у відповідних протоколах мають бути викладені, з посиланням на відповідні пункти затверджених технічних вимог та методики випробувань, підстави, які дають або не дають змоги дійти висновку щодо успішності або неуспішності здійснення певних перевірок, та, з урахуванням цих висновків, підтвердження або не підтвердження фактів реалізації в оцінюваному ОЕ певних функціональних послуг безпеки. При складанні відповідних протоколів слід керуватися вимогами Положення про державну експертизу у сфері технічного захисту інформації, ДСТУ 2851-94, інших стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, що стосуються документування результатів випробувань.

Додаток А
Перелік спеціальних запитань для дослідження об'єкта експертизи з метою ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики
(рекомендований)

А.1 Склад і архітектура ОЕ та КЗЗ

Об'єктом експертизи на відповідність НД ТЗІ в Україні в частині, що стосується оцінювання функціональних послуг безпеки, можуть бути КЗЗ КСЗІ, ЗТЗІ від НСД, а також захищені від НСД компоненти обчислювальної системи. У всіх трьох випадках ОЕ складається, як правило, з множини компонентів, деякі з яких спеціально призначені для реалізації функцій захисту (функціональних послуг безпеки), інші можуть впливати на забезпечення захисту опосередковано, наприклад, забезпечувати функціонування компонентів першого типу, а треті можуть узагалі не бути задіяними при вирішенні задач захисту оброблюваної інформації. Множина всіх компонентів перших двох типів складає КЗЗ ОЕ. Відповіді на наведені в розділі А.1 Додатка А запитання повинні допомогти експерту усвідомити склад і архітектуру ОЕ, а також склад, архітектуру та основні особливості реалізації його КЗЗ. Відповіді повинні бути сформульовані на початковому етапі попереднього аналізу ОЕ та, за необхідності, можуть бути уточнені в процесі поглибленого аналізу особливостей реалізації різних функціональних послуг безпеки.

А.1.1 Склад і архітектура ОЕ

А.1.1.1 Наведіть перелік компонентів обчислювальної системи, на базі якої функціонує ОЕ, їх основні характеристики (тип, версія тощо) і стислий опис архітектури обчислювальної системи.

Примітка. Під компонентами обчислювальної системи слід розуміти як апаратні компоненти (сервери, робочі станції, активне мережеве обладнання, канали локальних обчислювальних мереж, канали мереж передачі даних тощо), так і програмні засоби (операційні системи, системи керування базами даних (СКБД), сервери застосувань тощо).

А.1.1.2 Наведіть перелік основних функціональних модулів (функціональних блоків) ОЕ, стислий опис кожного функціонального модуля з наведенням його призначення (з погляду функцій оброблення інформації, які реалізуються ОЕ), характеру і вигляду подання оброблюваної інформації, основних зв'язків (потоків команд і даних) з іншими функціональними модулями ОЕ та використовуваних при цьому інтерфейсів, характеру і вигляду подання інформації, що передається між функціональними модулями ОЕ в процесі його функціонування.

Примітка. Під функціональними модулями ОЕ слід розуміти компоненти, що реалізують чітко визначену функціональність. Наприклад, для операційної системи такими є:

- ядро;

- програми оброблення переривань;
- менеджер процесів;
- оброблювачі запитів введення-виведення інформації;
- менеджер введення-виведення інформації;
- інтерфейси користувач/процес;
- інтерфейси прикладного програмування;
- програми діагностики апаратури;
- програми тестування апаратури;
- командні мови/інтерфейси (використовувані для генерації системи операторами, адміністраторами, користувачами тощо).

А.1.1.3 Для кожного з функціональних модулів ОЕ (з наведених при відповіді на п. А.1.1.2) вкажіть, на базі або з використанням яких компонентів обчислювальної системи (з наведених при відповіді на п. А.1.1.1) він функціонує.

А.1.2 Склад і архітектура КЗЗ ОЕ

А.1.2.1 Наведіть перелік основних функціональних модулів ОЕ (з наведених при відповіді на п. А.1.1.2), що входять до складу КЗЗ, тобто спеціально призначені або для реалізації функцій захисту (функціональних послуг безпеки), або для реалізації функцій, які впливають на реалізацію функцій захисту опосередковано, наприклад, шляхом забезпечення функціонування компонентів першого типу.

А.1.2.2 Наведіть (з урахуванням відповідей на п. А.1.1.2, А.1.1.3, А.1.2.1) опис архітектури КЗЗ на рівні функціональних модулів КЗЗ, реалізованих у різних функціональних модулях ОЕ, виділивши в описі ядро КЗЗ та інші його компоненти. Наведіть стислий опис кожного функціонального модуля КЗЗ з наведенням його призначення, реалізованих функцій захисту (функціональних послуг безпеки), характеру і вигляду подання оброблюваної інформації, основних зв'язків (потоків команд і даних) з іншими функціональними модулями КЗЗ і використовуваних при цьому інтерфейсів, а також основних зв'язків (потоків команд і даних) з функціональними модулями ОЕ, що не входять до складу КЗЗ, і використовуваних при цьому інтерфейсів.

Примітка. Під ядром КЗЗ слід розуміти апаратні засоби, вбудоване програмне забезпечення (програми постійних запам'ятовуючих пристроїв (ПЗП)) і програмні засоби, що безпосередньо реалізують концепцію диспетчера доступу, тобто, є посередником при всіх спробах (запитах) доступу активних об'єктів (користувачів, процесів) до пасивних об'єктів.

А.2 Об'єкти ОЕ, що мають відношення до політики функціональних послуг безпеки

Відповідно до підходу, визначеного у діючих НД ТЗІ, КЗЗ розглядає ресурси

ОЕ як об'єкти та керує взаємодією цих об'єктів згідно з реалізованою політикою функціональних послуг безпеки. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (вміст, семантика, значення) і фізичне (форма, синтаксис). Об'єкт характеризується своїм станом, який, у свою чергу характеризується атрибутами і поведінкою, що визначає способи зміни стану. При розгляді взаємодії двох об'єктів ОЕ, які виступають як приймачі або джерела інформації, варто виділяти пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію. При визначенні політики функціональних послуг безпеки повинні виділятися і розглядатися такі типи об'єктів ОЕ: об'єкти-користувачі, об'єкти-процеси та пасивні об'єкти.

Об'єкти-користувачі та об'єкти-процеси є такими лише всередині конкретного домену — ізольованої логічної області, всередині якої об'єкти мають певні властивості, повноваження і зберігають певні відносини. В інших доменах об'єкти залишаються в пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим процесом або навіть об'єктом-користувачем, оскільки останній залишається "пасивним" з погляду керуючого об'єкта. Іншими словами, об'єкти можуть знаходитися в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт. Перехід між станами означає, що об'єкт просто розглядається в іншому контексті. Взаємодія двох об'єктів (звертання активного об'єкта до пасивного з метою одержання певного виду доступу) призводить до появи потоку інформації між об'єктами та/або зміни стану ОЕ. Як потік інформації розглядається будь-яка порція інформації, передана між об'єктами.

Відповіді на наведені в розділі А.2 Додатка А запитання повинні допомогти експерту усвідомити перелік об'єктів ОЕ та набір їх основних атрибутів, використовуваних функціональними модулями КЗЗ при реалізації різних функціональних послуг безпеки. Відповіді повинні бути сформульовані на початковому етапі попереднього аналізу ОЕ та, за необхідності, можуть бути уточнені в процесі поглибленого аналізу особливостей реалізації різних функціональних послуг безпеки.

А.2.1 Об'єкти-користувачі та їх атрибути доступу

А.2.1.1 Наведіть перелік різних ролей (типів) користувачів (що характеризуються чітко визначеною сукупністю доступних користувачам функцій з керування ОЕ, КЗЗ та оброблення інформації), які підтримуються в ОЕ.

Примітка. Під користувачем слід розуміти фізичну особу, яка може взаємодіяти з ОЕ за допомогою наданого їй інтерфейсу. Як приклади ролей користувачів, підтримуваних, наприклад, операційною системою, можуть розглядатися такі ролі:

- суперкористувач;
- системний оператор;
- адміністратор системи;

- оператор резервного копіювання;
- досвідчений користувач;
- користувач тощо.

А.2.1.2 Для кожної з ролей, наведених при відповіді на запитання п. А.2.1.1, наведіть опис порядку створення та знищення об'єктів-користувачів відповідного типу, а також вигляду їх представлення у всіх функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2).

Примітка. В описах, що наводяться, для кожного функціонального модуля ОЕ, що входить до складу КЗЗ, повинно бути зазначено, в який момент і яким чином створюються об'єкти-користувачі певного типу, що є представленням фізичних користувачів в ОЕ (наприклад, вони можуть створюватися при вході користувача в систему, при породженні процесу, встановленні з'єднання тощо), яким чином (у вигляді спеціальних структур даних або будь-яким іншим способом) представляються об'єкти-користувачі у функціональному модулі ОЕ, з яким об'єктом системи зв'язуються структури даних (маркери), що представляють користувачів у функціональному модулі ОЕ (наприклад, з породженим процесом, активним мережевим з'єднанням, підключеним до сервера віддаленим терміналом або робочою станцією тощо), яким чином (наприклад, при завершенні процесу, закритті мережевого з'єднання, відключенні від сервера віддаленого термінала або робочої станції) знищуються об'єкти-користувачі і структури даних (маркери), що представляють їх у функціональному модулі ОЕ .

А.2.1.3 Для кожного з типів об'єктів-користувачів і кожного вигляду їх представлення в різних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.2.1.2), наведіть опис складу структур даних (маркерів), що представляють користувачів у функціональних модулях ОЕ, у вигляді опису переліку і можливих значень атрибутів доступу об'єктів-користувачів, що входять або не входять до складу цих структур, але однозначно пов'язані з ними.

Примітка. Як можливі атрибути доступу об'єктів-користувачів, що входять до складу структур даних (маркерів), які представляють користувачів у функціональних модулях ОЕ, що входять до складу КЗЗ, або однозначно пов'язані з ними, можуть, наприклад, використовуватися:

- псевдонім користувача;
- ідентифікатор користувача;
- ідентифікатори груп, членом яких є користувач;
- ідентифікатор ролі користувача;
- рівень допуску користувача;
- ознаки наявності/ відсутності у користувача різних адміністративних повноважень (привілеїв);
- список повноважень користувача, що визначає права доступу до різних

пасивних об'єктів тощо.

А.2.2 Об'єкти-процеси та їх атрибути доступу

А.2.2.1 Наведіть (з урахуванням відповідей на п. А.1.1.2, А.1.1.3) перелік різних типів процесів (процесів, які породжуються з програм з різним виглядом подання виконуваного коду), що підтримуються в ОЕ.

Примітка. Як приклади різних типів процесів, залежно від призначення, архітектури і прикладної функціональності ОЕ, можуть розглядатися, наприклад, такі:

- прикладні та системні програми у вигляді виконуваних модулів;
- динамічні бібліотеки;
- системні драйвери;
- скриптові модулі;
- процедури та методи, що реалізують різні прикладні функції в межах ОЕ тощо.

А.2.2.2 Для кожного з типів процесів, наведених при відповіді на запитання п. А.2.2.1, наведіть опис порядку створення і знищення об'єктів-процесів відповідного типу, а також вигляду їх представлення у всіх функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2).

Примітка. В описах, що наводяться, для кожного функціонального модуля ОЕ, що входить до складу КЗЗ, повинно бути зазначено, яким чином при старті (запуску) програм створюються об'єкти-процеси певного типу, яким чином (у вигляді спеціальних структур даних або інакше) представляються об'єкти-процеси у функціональному модулі ОЕ, яким чином (наприклад, при завершенні процесу, завершенні батьківського процесу тощо) знищуються об'єкти-процеси і структури даних (маркери), що представляють їх у функціональному модулі ОЕ.

А.2.2.3 Для кожного з типів об'єктів-процесів і кожного вигляду їх представлення в різних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.2.2.1, А.2.2.2), наведіть опис складу структур даних (маркерів), які представляють процеси у функціональних модулях ОЕ, що входять до складу КЗЗ, у вигляді опису переліку і можливих значень атрибутів доступу об'єктів-процесів, що входять або не входять до складу цих структур, але однозначно пов'язані з ними.

Примітка. Як можливі атрибути доступу об'єктів-процесів, що входять до складу структур даних (маркерів), які представляють процеси у функціональних модулях ОЕ, що входять до складу КЗЗ, або однозначно пов'язані з ними, можуть, наприклад, використовуватися:

- найменування програми (процесу);
- ідентифікатор процесу;
- ідентифікатори груп, до яких входить процес;

- рівень допуску процесу;
- ознаки наявності/ відсутності у процесу різних адміністративних повноважень (привілеїв);
- список повноважень процесу, що визначає права доступу до різних пасивних об'єктів тощо.

А.2.2.4 Для кожного з типів об'єктів-процесів, кожного вигляду їх представлення в різних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.2.2.1, А.2.2.2) і різного складу структур даних (маркерів), що представляють процеси у функціональних модулях ОЕ (з урахуванням відповіді на п. А.2.2.3), наведіть опис порядку і правил ініціалізації та успадкування атрибутів доступу дочірніх процесів від об'єктів-користувачів або об'єктів-процесів, що їх породжують.

А.2.3 Пасивні об'єкти та їх атрибути доступу

А.2.3.1 Наведіть (з урахуванням відповідей на п. А.1.1.2, А.1.1.3) перелік різних типів пасивних об'єктів, у вигляді яких можуть бути представлені в процесі функціонування ОЕ інформаційні ресурси, що зберігаються, обробляються та передаються в процесі функціонування ОЕ та над якими виконуються певні дії.

Примітка. Як приклади різних типів пасивних об'єктів, залежно від призначення, архітектури і прикладної функціональності ОЕ, можуть розглядатися, наприклад, такі:

- каталоги;
- файли;
- сегменти оперативної пам'яті;
- процеси;
- зовнішні пристрої;
- таблиці СКБД;
- записи таблиць СКБД;
- джерела та/або приймачі даних для мережевих комунікацій тощо.

А.2.3.2 Для кожного з типів пасивних об'єктів, наведених при відповіді на запитання
п. А.2.3.1, наведіть опис порядку створення (ініціалізації) та знищення пасивних об'єктів і пов'язаних з ними наборів атрибутів доступу в процесі оброблення у всіх функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2).

Примітка. В описах, які наводяться, для кожного функціонального модуля ОЕ, що входить до складу КЗЗ, повинно бути зазначено, у якому вигляді створюються (ініціалізуються) нові пасивні об'єкти, яким чином (у вигляді спеціальних структур даних або в інший спосіб) надаються пов'язані з ними набори атрибутів доступу в цьому функціональному модулі ОЕ, яким чином виконується знищення пасивних об'єктів і пов'язаних з ними наборів атрибутів

доступу.

А.2.3.3 Для кожного з типів пасивних об'єктів, наведених при відповіді на запитання
п. А.2.3.1, і пов'язаних з ними наборів атрибутів доступу (з урахуванням відповідей на
п. А.2.3.1, А.2.3.2) наведіть опис складу наборів атрибутів доступу у вигляді опису переліку і можливих значень атрибутів доступу пасивних об'єктів, що входять до складу цих наборів.

Примітка. Як можливі атрибути доступу пасивних об'єктів, що входять до складу наборів атрибутів доступу, можуть, наприклад, використовуватися:

- найменування пасивного об'єкта;
- ідентифікатор пасивного об'єкта;
- ідентифікатор власника пасивного об'єкта;
- ідентифікатор групи власника пасивного об'єкта;
- рівень доступу;
- мітка доступу;
- список керування доступом, що визначає права доступу різних об'єктів-користувачів, об'єктів-процесів та/або їх груп до пасивного об'єкта тощо.

А.3 Послуги довірчої/адміністративної конфіденційності

Послуги довірчої/адміністративної конфіденційності забезпечують можливість керування потоками інформації від захищених пасивних об'єктів до об'єктів-користувачів з метою захисту пасивних об'єктів від несанкціонованого ознайомлення з їх умістом (компрометації). Відповіді на наведені в розділі А.3 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ послуг довірчої/ адміністративної конфіденційності, перелік об'єктів різного типу, стосовно яких визначено політику і реалізовані ці функціональні послуги безпеки, атрибутів доступу, використовуваних функціональними модулями КЗЗ при реалізації відповідних послуг. Сформульовані відповіді дозволять експерту визначити рівні, політику, засоби, механізми та особливості реалізації послуг довірчої/ адміністративної конфіденційності, а також одержати вхідні дані для розроблення програм і методик випробувань цих послуг.

А.3.1 Чи існує в ОЕ для будь-якого з типів пасивних об'єктів, наведених при відповіді на запитання п. А.2.3.1, можливість розмежування доступу з боку користувачів, що відносяться до будь-яких з ролей (наведених при відповіді на п. А.2.1.1), або процесів різного типу (наведених при відповіді на п. А.2.2.1) до пасивних об'єктів цього типу з метою одержання інформації, що міститься в пасивному об'єкті.

Примітка. Якщо такої можливості не існує, тобто, всі користувачі в межах певної ролі або всі процеси певного типу завжди мають однакові можливості доступу з метою одержання інформації (читання) до всієї множини пасивних об'єктів усіх типів, то це означає, що послуги довірчої та/або адміністративної

конфіденційності засобами КЗЗ ОЕ не реалізуються і відповідати на запитання п. А.3.2-А.3.13 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ реалізуються послуги довірчої та/або адміністративної конфіденційності, їх політики і рівні можуть бути уточнені при відповіді на запитання п. А.3.2-А.3.13.

А.3.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми керування доступом з боку об'єктів-користувачів одного чи декількох типів, наведених при відповіді на п. А.2.1.2, або об'єктів-процесів одного чи декількох типів, наведених при відповіді на п. А.2.2.1, до пасивних об'єктів одного чи декількох типів, наведених при відповіді на п. А.2.3.1, шляхом аналізу запитів на доступ з боку користувачів або об'єктів-процесів з метою одержання інформації, що міститься в пасивному об'єкті, і прийняття рішення на підставі інформації, що міститься в наборах атрибутів доступу ініціатора запиту (користувача або об'єкта-процесу) і пасивного об'єкта (з урахуванням відповідей на п. А.2.1.3, А.2.2.3, А.2.3.3). Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2) засоби, які дозволяють користувачам, що відносяться до будь-яких з ролей (наведених при відповіді на п. А.2.1.1), змінювати відповідні набори атрибутів доступу об'єктів-користувачів та/або об'єктів-процесів і пасивних об'єктів.

Примітка. Механізмами, що забезпечують реалізацію послуг довірчої та адміністративної конфіденційності, є механізми керування доступом, тобто надання можливості доступу до ресурсу згідно зі спеціально визначеними правилами. Як основні схеми, на підставі яких може здійснюватися керування доступом, можуть використовуватися такі:

- на підставі списків керування доступом (під списком керування доступом слід розуміти пов'язаний із запитуваним ресурсом набір атрибутів доступу у вигляді сукупностей ідентифікаторів ініціаторів запиту та атрибутів, що визначають дозволені види доступу або операції над запитуваним ресурсом);

- на підставі списків повноважень (під списком повноважень слід розуміти пов'язаний з ініціатором запиту набір атрибутів доступу у вигляді сукупності операцій, дозволених над заданою множиною запитуваних ресурсів);

- на підставі міток безпеки (під мітками слід розуміти атрибути доступу, пов'язані як з ініціатором запиту, так і з запитуваним ресурсом, рішення про надання доступу приймається на підставі оброблення міток ініціатора і ресурсу за заданими правилами).

Для прийняття рішення про можливість надання доступу ці механізми можуть використовувати, наприклад:

- ідентифікатори відповідних об'єктів;

- ідентифікатори груп відповідних об'єктів;
- інформацію про права доступу до пасивних об'єктів у вигляді міток доступу, списків керування доступом або списків повноважень;
- інформацію про права володіння пасивним об'єктом;
- інформацію про час спроби доступу;
- інформацію про маршрут запиту доступу в розподілених системах;
- інформацію про тривалість сеансу доступу до ресурсу.

Засоби керування доступом, що приймають рішення про можливість задоволення або відхилення запиту, повинні бути реалізовані в тих компонентах КЗЗ, що входять до складу ядра КЗЗ і реалізують концепцію диспетчера доступу. Засоби, що дозволяють змінювати атрибути доступу, можуть бути реалізовані в довільних компонентах КЗЗ. Якщо зазначених засобів у складі КЗЗ немає, то це означає, що послуги довірчої та/або адміністративної конфіденційності засобами КЗЗ ОЕ не реалізовуються і відповідати на запитання п. А.3.3-А.3.13 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ реалізовуються послуги довірчої та/або адміністративної конфіденційності, їх політики і рівні можуть бути уточнені при відповіді на запитання п. А.3.3-А.3.13.

А.3.3 Чи дозволяють реалізовані у складі функціональних модулів ОЕ, що входять до складу КЗЗ, засоби (з урахуванням відповіді на п. А.3.2) змінювати атрибути доступу об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів, на підставі яких реалізується керування доступом:

А.3.3.1 будь-яким користувачам, що відносяться до кожної з ролей, наведених при відповіді на п. А.2.1.1, але лише для частини пасивних об'єктів певних типів, наведених при відповіді на п. А.2.3.1, що належать їх домену, тобто з урахуванням атрибутів, наведених при відповіді на п. А.2.3.3, що визначають їх права володіння цими пасивними об'єктами;

А.3.3.2 будь-яким користувачам, що відносяться лише до певних ролей, наведених при відповіді на п. А.2.1.1, для всіх пасивних об'єктів певних типів, наведених при відповіді на п. А.2.3.1, без урахування атрибутів, що визначають їх права володіння цими пасивними об'єктами.

У випадку позитивної відповіді на п. А.3.3.1 можна стверджувати, що засобами КЗЗ реалізуються послуги довірчої конфіденційності. У випадку позитивної відповіді на п. А.3.3.2 можна стверджувати, що засобами КЗЗ реалізуються послуги адміністративної конфіденційності. Політики і рівні відповідних послуг для пасивних об'єктів різного типу можуть бути уточнені при відповіді на запитання п. А.3.4-А.3.13.

А.3.4 Чи відноситься політика послуг довірчої або адміністративної конфіденційності, реалізована КЗЗ (чи забезпечується можливість керування доступом користувачів або об'єктів-процесів до пасивних об'єктів, з урахуванням відповідей на п. А.3.3.1, А.3.3.2):

А.3.4.1 до всіх типів об'єктів-користувачів, об'єктів-процесів і пасивних

об'єктів, наведених при відповіді на п. А.2.1.2, А.2.2.1, А.2.3.1;

А.3.4.2 лише до певних (укажіть, до яких) типів об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів, наведених при відповіді на п. А.2.1.2, А.2.2.1, А.2.3.1.

У випадку позитивної відповіді на п. А.3.4.1 можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої конфіденційності рівнів КД-3 чи КД-4 або адміністративної конфіденційності рівнів КА-3 чи КА-4. У цьому випадку політика і рівні відповідних послуг можуть бути уточнені при відповіді на запитання п. А.3.5.2, А.3.6-А.3.13. У випадку негативної відповіді на п. А.3.4.1 можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої конфіденційності рівнів КД-1 чи КД-2 або адміністративної конфіденційності рівнів КА-1 чи КА-2 стосовно об'єктів, наведених при відповіді на п. А.3.4.2. У цьому випадку політика і рівні відповідних послуг можуть бути уточнені при відповіді на запитання п. А.3.5.1, А.3.5.2, А.3.6-А.3.13.

А.3.5 На підставі яких атрибутів доступу:

А.3.5.1 об'єктів-процесів і пасивних об'єктів різних типів (з урахуванням відповідей на п. А.2.2.3, А.2.3.3) або

А.3.5.2 об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різних типів (з урахуванням відповідей на п. А.2.1.3, А.2.2.3 і А.2.3.3),

та згідно з якими правилами реалізується розмежування доступу для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4, до яких відноситься політика послуг довірчої або адміністративної конфіденційності.

А.3.6 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.3.2) з використанням механізмів керування доступом, здійснюється оброблення запитів на надання доступу (розмежування доступу) згідно із зазначеними при відповіді на п. А.3.5 правилами для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4.

А.3.7 На підставі яких атрибутів пасивних об'єктів (з урахуванням відповіді на п. А.2.3.3) та атрибутів доступу об'єктів-користувачів (з урахуванням відповіді на п. А.2.1.3), що визначають права володіння для послуги довірчої конфіденційності або адміністративні повноваження для послуги адміністративної конфіденційності, і згідно з якими правилами здійснюється оброблення запитів на зміну прав доступу до захищених об'єктів для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4.

А.3.8 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.3.2), здійснюється оброблення запитів на зміну прав доступу до захищених об'єктів згідно із зазначеними при відповіді на п. А.3.7 правилами для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4.

А.3.9 Чи існує у функціональних компонентах ОЕ, що входять до складу

КЗЗ та наведені при відповіді на п. А.3.8, з використанням атрибутів доступу, наведених при відповіді на п. А.3.5, А.3.7 для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4:

А.3.9.1 можливість визначення конкретних процесів та/або груп процесів, що мають право одержувати інформацію від об'єкта;

А.3.9.2 можливість визначення конкретних користувачів та/або груп користувачів, що мають право одержувати інформацію від об'єкта;

А.3.9.3 можливість визначення конкретних користувачів (і груп користувачів), що мають, а також тих, що не мають права одержувати інформацію від об'єкта;

А.3.9.4 можливість визначення конкретних користувачів і процесів (і груп користувачів та процесів), що мають, а також тих, що не мають права одержувати інформацію від об'єкта.

Примітка. У випадку позитивної відповіді на п. А.3.9.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої конфіденційності рівня КД-1 або адміністративної конфіденційності рівня КА-1. У випадку позитивної відповіді на п. А.3.9.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої конфіденційності рівня КД-2 або адміністративної конфіденційності рівня КА-2. У випадку позитивної відповіді на п. А.3.9.3 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої конфіденційності рівня КД-3 або адміністративної конфіденційності рівня КА-3. У випадку позитивної відповіді на п. А.3.9.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої конфіденційності рівня КД-4 або адміністративної конфіденційності рівня КА-4.

А.3.10 Чи існує у функціональних компонентах ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.3.8, з використанням атрибутів доступу, наведених при відповіді на п. А.3.5, А.3.7 для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4:

А.3.10.1 можливість визначення конкретних користувачів та/або груп користувачів, що мають право ініціювати процес;

А.3.10.2 можливість визначення конкретних користувачів (і груп користувачів), що мають, а також тих, що не мають права ініціювати процес.

Примітка. У випадку позитивної відповіді на п. А.3.10.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої конфіденційності рівня КД-2 або адміністративної конфіденційності рівня КА-2. У випадку позитивної відповіді на п. А.3.10.2 можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої конфіденційності рівнів КД-3 чи КД-4 або адміністративної конфіденційності рівнів КА-3 чи КА-4.

А.3.11 Які атрибути доступу, наведені при відповіді на п. А.3.5, А.3.7, що характеризують права доступу до захищених пасивних об'єктів різного типу, наведених при відповіді на п. А.3.4, установлюються:

А.3.11.1 у момент створення пасивного об'єкта;

А.3.11.2 у момент ініціалізації об'єкта.

Укажіть, яке значення призначається кожному атрибуту, обґрунтуйте його безпечність.

А.3.12 Чи зберігаються, якщо так, то які, атрибути доступу пасивних об'єктів, наведені при відповіді на п. А.3.5, А.3.7, що характеризують права користувачів на одержання інформації з цих об'єктів (укажіть для пасивних об'єктів кожного типу, наведених при відповіді на п. А.3.4) при експорті об'єкта за межу ОЕ. Яким чином здійснюється зв'язування переданих наборів атрибутів доступу з експортованими пасивними об'єктами різного типу.

А.3.13 Чи зберігаються, якщо так, то які, атрибути доступу пасивних об'єктів, наведені при відповіді на п. А.3.5, А.3.7, що характеризують права користувачів на одержання інформації з цих об'єктів (укажіть для пасивних об'єктів кожного типу, наведених при відповіді на п. А.3.4) при імпорті об'єкта із-за межі ОЕ. Яким чином здійснюється зв'язування прийнятих наборів атрибутів доступу з імпортованими пасивними об'єктами різного типу.

А.4 Повторне використання об'єктів

Послуга "Повторне використання об'єктів" дозволяє забезпечити коректність повторного використання поділюваних ресурсів, гарантуючи, що у випадку, якщо поділюваний ресурс виділяється новому користувачу або процесу, він не містить інформації, що залишилася від попереднього користувача або процесу. Відповіді на наведені в розділі А.4 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік пасивних об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.4.1 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми звільнення (очищення) вмісту поділюваних ресурсів, використовуваних для збереження пасивних об'єктів будь-яких типів, наведених при відповіді на п. А.2.3.1, а також їх атрибутів доступу, наведених при відповіді на п. А.2.3.3.

Примітка. Механізмами, що забезпечують реалізацію послуги "Повторне використання об'єктів", є механізми:

- ініціалізації (заповнення наперед заданими або випадковими даними) вмісту поділюваних ресурсів, використовуваних для збереження пасивних об'єктів;

- ініціалізації (видалення) атрибутів доступу пасивних об'єктів, що видаляються.

Ці механізми можуть бути реалізовані або в компонентах КЗЗ, що входять до складу ядра КЗЗ і в яких здійснюється оброблення запитів на видалення пасивних об'єктів і звільнення займаних об'єктами поділюваних ресурсів, або в компонентах КЗЗ, у яких здійснюється оброблення запитів на створення нових пасивних об'єктів і виділення необхідних для їх збереження поділюваних

ресурсів. Якщо зазначених засобів у складі КЗЗ немає, то це означає, що послуга "Повторне використання об'єктів" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.4.2-А.4.4 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Повторне використання об'єктів", остаточно факт її реалізації і політика можуть бути уточнені при відповіді на запитання п. А.4.2-А.4.4.

А.4.2 Чи забезпечується засобами КЗЗ, наведеними при відповіді на п. А.4.1, можливість звільнення (очищення) вмісту поділюваних ресурсів, використовуваних для збереження пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4, стосовно яких визначені політики послуг довірчої та адміністративної конфіденційності, а також їх атрибутів доступу.

У випадку позитивної відповіді на п. А.4.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Повторне використання об'єктів" рівня КО-1. У цьому випадку політика послуги може бути уточнена при відповіді на запитання п. А.4.3-А.4.4. У випадку негативної відповіді на п. А.4.2 можна стверджувати, що засобами КЗЗ послуга "Повторне використання об'єктів" рівня КО-1 не реалізується і відповідати на запитання п. А.4.3-А.4.4 не потрібно.

А.4.3 З використанням яких механізмів і в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.4.1), реалізується послуга "Повторне використання об'єктів" стосовно атрибутів доступу пасивних об'єктів кожного з типів, наведених при відповіді на п. А.4.2. Укажіть значення, що призначаються атрибутам видалених пасивних об'єктів.

А.4.4 З використанням яких механізмів і в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.4.1), реалізується послуга "Повторне використання об'єктів" стосовно ресурсів, використовуваних для збереження захищених пасивних об'єктів кожного з типів, наведених при відповіді на п. А.4.2.

А.5 Аналіз прихованих каналів

Реалізація послуги "Аналіз прихованих каналів" дозволяє виявити і виключити потоки інформації, що існують, але не контролюються іншими функціональними послугами безпеки. Відповіді на наведені в розділі А.5 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, її рівень, політику, засоби, механізми та особливості реалізації, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.5.1 Чи наведені в проектній або експлуатаційній документації на ОЕ результати аналізу прихованих каналів, проведеного з метою виявлення і виключення потоків інформації, що існують, але не контролюються іншими послугами безпеки. Яку множину прихованих каналів виявлено в процесі аналізу. Використання цих каналів може призвести до порушення конфіденційності інформації, що міститься в пасивних об'єктах певного типу, наведених при відповіді на п. А.2.3.1.

Примітка. У випадку позитивної відповіді на п. А.5.1 можна

стверджувати, що в ОЕ може бути реалізована послуга "Аналіз прихованих каналів" рівня КК-1, КК-2 чи КК-3. У цьому випадку політика послуги може бути уточнена при відповіді на запитання п. А.5.2-А.5.5. У випадку негативної відповіді на п. А.5.1 можна стверджувати, що послуга "Аналіз прихованих каналів" в ОЕ не реалізується і відповідати на запитання п. А.5.2-А.5.5 не потрібно.

А.5.2 Чи документовані (описані з погляду механізму реалізації) у наведених при відповіді на п. А.5.1 результатах усі виявлені в апаратному і програмному забезпеченні, а також у програмах ПЗП приховані канали. Які особливості і можливості яких функціональних компонентів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), при цьому використовуються. Наведіть перелік документованих прихованих каналів з їх характеристиками.

Примітка. У випадку позитивної відповіді на п. А.5.2 можна стверджувати, що в ОЕ може бути реалізована послуга "Аналіз прихованих каналів" рівня КК-1, КК-2 чи КК-3. У цьому випадку політика послуги може бути уточнена при відповіді на запитання п. А.5.3-А.5.5. У випадку негативної відповіді на п. А.5.2 можна стверджувати, що послуга "Аналіз прихованих каналів" в ОЕ не реалізується і відповідати на запитання п. А.5.3-А.5.5 не потрібно.

А.5.3 Чи усунуті всі виявлені на етапі аналізу та наведені при відповіді на п. А.5.2 приховані канали. Якщо так, то вкажіть, з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), здійснюється усунення (запобігання можливості використання) кожного виявленого на етапі аналізу прихованого каналу.

Примітка. У випадку позитивної відповіді на п. А.5.3 можна стверджувати, що в ОЕ може бути реалізована послуга "Аналіз прихованих каналів" рівня КК-3. У випадку негативної відповіді на п. А.5.3 можна стверджувати, що в ОЕ може бути реалізована послуга "Аналіз прихованих каналів" рівня КК-1 чи КК-2. У цьому випадку рівень і політика послуги можуть бути уточнені при відповіді на запитання п. А.5.4-А.5.5.

А.5.4 Чи документована (на підставі теоретичної оцінки або вимірів) максимальна пропускна здатність кожного з виявлених та наведених при відповіді на п. А.5.2 прихованих каналів. Чи документована сукупна пропускна здатність для груп прихованих каналів, що можуть використовуватися спільно (якщо такі існують). Наведіть відповідні дані для всіх виявлених груп прихованих каналів.

Примітка. У випадку позитивної відповіді на п. А.5.4 можна стверджувати, що в ОЕ може бути реалізована послуга "Аналіз прихованих каналів" рівня КК-1 чи КК-2. У цьому випадку політика послуги може бути уточнена при відповіді на запитання п. А.5.5. У випадку негативної відповіді на п. А.5.4 можна стверджувати, що послуга "Аналіз прихованих каналів" в ОЕ не реалізується і відповідати на запитання п. А.5.5 не потрібно.

А.5.5 Чи здійснюється в будь-яких функціональних компонентах ОЕ, що

входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), контроль використання будь-якої затвердженої підмножини множини виявлених, документованих та наведених при відповіді на п. А.5.2 прихованих каналів. Якщо так, то з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється контроль використання цієї підмножини множини документованих прихованих каналів. Наведіть опис для кожного з каналів, внесених до затвердженої підмножини.

Примітка. У випадку позитивної відповіді на п. А.5.2 можна стверджувати, що в ОЕ може бути реалізована послуга "Аналіз прихованих каналів" рівня КК-2.

А.6 Конфіденційність при обміні

Послуга "Конфіденційність при обміні" дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, при їх передачі (експорті/імпорті) через незахищене середовище. Відповіді на наведені в розділі А.6 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.6.1 Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними компонентами ОЕ через незахищене середовище пасивними об'єктами будь-якого з типів, наведених при відповіді на запитання п. А.2.3.1. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об'єктів.

Примітка. У випадку позитивної відповіді на п. А.6.1 можна стверджувати, що в ОЕ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-1, КВ-2, КВ-3 чи КВ-4. У цьому випадку факт реалізації послуги, її політика і рівень можуть бути уточнені при відповіді на запитання п. А.6.2-А.6.13. У випадку негативної відповіді на п. А.6.1 можна стверджувати, що послуга "Конфіденційність при обміні" в ОЕ не реалізується і відповідати на запитання п. А.6.2-А.6.13 не потрібно.

А.6.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми, що забезпечують захист пасивних об'єктів будь-яких типів, наведених при відповіді на п. А.6.1, від безпосереднього ознайомлення з інформацією, що міститься в цих об'єктах, при їх передачі між різними компонентами ОЕ через незахищене середовище.

Примітка. Функціонування механізмів, що забезпечують реалізацію послуги "Конфіденційність при обміні", може ґрунтуватися на одному з таких принципів:

- забезпечення конфіденційності шляхом керування маршрутом передачі пасивних об'єктів з метою унеможливлення несанкціонованого ознайомлення з

їх умістом;

- забезпечення конфіденційності шляхом приховування семантики (вмісту) переданих пасивних об'єктів з використанням шифрування;

- забезпечення конфіденційності шляхом заповнення трафіка методом доповнення хибних даних;

- забезпечення конфіденційності шляхом заповнення трафіка методом генерації хибних повідомлень;

- забезпечення конфіденційності шляхом використання змінного надання даних;

- забезпечення конфіденційності шляхом розподілу каналів для передачі різних частин повідомлення (розподілу спектра);

- забезпечення конфіденційності шляхом організації прихованого каналу передачі усередині іншого відкритого каналу (стеганографія).

Якщо засобів, що реалізують зазначені механізми, у складі КЗЗ немає, то це означає, що послуга "Конфіденційність при обміні" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.6.3-А.6.13 не потрібно. Якщо ж такі засоби існують, то це означає, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні", остаточно факт її реалізації і політика можуть бути уточнені при відповіді на запитання п. А.6.3-А.6.13.

А.6.3 Чи відноситься політика послуги "Конфіденційність при обміні", реалізована КЗЗ (чи забезпечується можливість захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах):

А.6.3.1 до пасивних об'єктів усіх типів, наведених при відповіді на п. А.6.1, а також до використовуваних для їх приймання/передачі функціональних модулів ОЕ, що входять до складу КЗЗ (інтерфейсних процесів);

А.6.3.2 лише до пасивних об'єктів певних (укажіть яких) типів, наведених при відповіді на п. А.6.1, а також до використовуваних для їх приймання/передачі функціональних модулів ОЕ, що входять до складу КЗЗ (інтерфейсних процесів).

Примітка. У випадку позитивної відповіді на п. А.6.3.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3 чи КВ-4. У випадку негативної відповіді на п. А.6.3.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-1 чи КВ-2 стосовно об'єктів, наведених при відповіді на п. А.6.3.2.

А.6.4 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.6.2), з використанням яких саме механізмів захисту реалізується захист від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, наведених при відповіді на п. А.6.3.1 чи А.6.3.2. Який рівень захищеності забезпечується використовуваними механізмами. Якими параметрами (якими атрибутами доступу пасивних об'єктів або властивостями використовуваних механізмів) визначається рівень

захищеності, що забезпечується для пасивних об'єктів різного типу, наведених при відповіді на п. А.6.3.1 чи А.6.3.2. Чи існує можливість у користувачів та/або процесів (укажіть яких, з урахуванням відповідей на п. А.2.1.1, А.2.1.2, А.2.2.1, А.2.2.2) з використанням відповідних функціональних модулів ОЕ, що входять до складу КЗЗ (укажіть яких, з урахуванням відповідей на п. А.1.2.1, А.1.2.2), керувати (шляхом зміни відповідних параметрів) рівнем захищеності, що забезпечується для пасивних об'єктів різного типу.

Примітка. У випадку позитивної відповіді на п. А.6.4 (в частині можливості керування рівнем захищеності) можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-2, КВ-3 чи КВ-4. У випадку негативної відповіді на п. А.6.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-1, відповідати на запитання п. А.6.5-А.6.13 не потрібно.

А.6.5 Чи існує можливість у наведених при відповіді на п. А.6.4 засобах керування рівнем захищеності, що забезпечується для пасивних об'єктів різного типу, оброблення запитів на присвоєння або зміну рівня захищеності лише у випадку, якщо вони надходять від користувачів, які відносяться лише до певних ролей, наведених при відповіді на п. А.2.1.1 (від адміністраторів або користувачів, яким надані відповідні повноваження). На підставі яких атрибутів об'єктів-користувачів (з урахуванням відповіді на п. А.2.1.3), що визначають їх повноваження, та за якими правилами виконується оброблення цих запитів.

Примітка. У випадку позитивної відповіді на п. А.6.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-2, КВ-3 чи КВ-4. У випадку негативної відповіді на п. А.6.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-1, відповідати на запитання п. А.6.6-А.6.13 не потрібно.

А.6.6 Чи обробляються у засобах, наведених при відповіді на п. А.6.4, запити на експорт (передачу) захищеного пасивного об'єкта передавальним компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

А.6.6.1 атрибутів доступу інтерфейсного процесу, що здійснює передачу, і КЗЗ (компонента КЗЗ), що є приймачем об'єкта (вкажіть яких, з урахуванням відповіді на п. А.2.2.3);

А.6.6.2 лише атрибутів доступу інтерфейсного процесу, що здійснює передачу (вкажіть яких, з урахуванням відповіді на п. А.2.2.3).

Примітка. У випадку позитивної відповіді на п. А.6.6.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3 чи КВ-4. У випадку негативної відповіді на п. А.6.6.1 і позитивної відповіді на п. А.6.6.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-2. У випадку негативних відповідей на п. А.6.6.1 і А.6.6.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні"

рівня КВ-1, відповідати на запитання п. А.6.7-А.6.13 не потрібно.

А.6.7 Чи обробляються запити на імпорт (приймання) захищеного пасивного об'єкта приймаючим компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

А.6.7.1 атрибутів доступу інтерфейсного процесу, що здійснює приймання, і КЗЗ (компонента КЗЗ), що є джерелом об'єкта (вкажіть яких, з урахуванням відповіді на п. А.2.2.3);

А.6.7.2 лише атрибутів доступу інтерфейсного процесу, що здійснює приймання (укажіть яких, з урахуванням відповіді на п. А.2.2.3).

Примітка. У випадку позитивної відповіді на п. А.6.7.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3 чи КВ-4. У випадку негативної відповіді на п. А.6.7.1 і позитивної відповіді на п. А.6.7.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-2, відповідати на запитання п. А.6.8-А.6.13 не потрібно. У випадку негативних відповідей на п. А.6.7.1 і А.6.7.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-1, відповідати на запитання п. А.6.8-А.6.13 не потрібно.

А.6.8 Чи є представлення захищеного переданого пасивного об'єкта функцією атрибутів доступу інтерфейсного процесу (з урахуванням відповідей на п. А.6.6.1, А.6.6.2), самого об'єкта (з урахуванням відповіді на п. А.2.3.3), а також його джерела і приймача (з урахуванням відповідей на п. А.6.6.1, А.6.6.2). Якщо так, то опишіть відповідну функціональну залежність.

Примітка. У випадку позитивної відповіді на п. А.6.8 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3 чи КВ-4. У випадку негативної відповіді на п. А.6.8 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-2, відповідати на запитання п. А.6.9-А.6.13 не потрібно.

А.6.9 Чи наведені в проектній або експлуатаційній документації на ОЕ результати аналізу прихованих каналів обміну. Яку множину прихованих каналів обміну, що дозволяють порушити конфіденційність інформації шляхом спільного аналізу ряду отриманих об'єктів, виявлено в процесі аналізу. До порушення конфіденційності інформації, що міститься в пасивних об'єктах будь-якого з типів, наведених при відповіді на п. А.6.3.1, може призвести використання цих каналів. Наведіть опис інформації, яку можна одержати шляхом спільного аналізу ряду отриманих об'єктів.

Примітка. У випадку позитивної відповіді на п. А.6.9 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-4. У випадку негативної відповіді на п. А.6.9 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3, відповідати на запитання п. А.6.10-А.6.13 не потрібно.

А.6.10 Чи документовані (описані з погляду механізму реалізації) у наведених при відповіді на п. А.6.9 результатах усі виявлені в процесі аналізу приховані канали обміну. Які особливості і можливості яких функціональних компонентів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), при цьому використовуються. Наведіть перелік документованих прихованих каналів обміну з їх характеристиками.

Примітка. У випадку позитивної відповіді на п. А.6.10 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-4. У випадку негативної відповіді на п. А.6.10 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3, відповідати на запитання п. А.6.11-А.6.13 не потрібно.

А.6.11 Чи документована (на підставі теоретичної оцінки або вимірів) максимальна пропускна здатність кожного виявленого прихованого каналу обміну (з урахуванням відповіді на п. А.6.10). Наведіть відповідні дані для кожного виявленого прихованого каналу обміну.

Примітка. У випадку позитивної відповіді на п. А.6.11 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-4. У випадку негативної відповіді на п. А.6.11 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3, відповідати на запитання п. А.6.12-А.6.13 не потрібно.

А.6.12 Чи здійснюється в будь-яких функціональних компонентах ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реєстрація використання будь-якої затвердженої підмножини множини виявлених і документованих (з урахуванням відповідей на п. А.6.9, А.6.10) прихованих каналів обміну. Якщо так, то з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється реєстрація використання цієї підмножини множини документованих прихованих каналів обміну. Наведіть опис для кожного з каналів, внесених до затвердженої підмножини.

Примітка. У випадку позитивної відповіді на п. А.6.12 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-4. У випадку негативної відповіді на п. А.6.12 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-3, відповідати на запитання п. А.6.13 не потрібно.

А.6.13 Чи забезпечується у функціональних компонентах ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), усунення всіх виявлених на етапі аналізу та наведених при відповіді на п. А.6.9 прихованих каналів обміну. Якщо так, то з використанням яких механізмів і в яких функціональних компонентах ОЕ, що входять до складу КЗЗ, здійснюється усунення (запобігання можливості використання) або часткове перекриття кожного виявленого на етапі аналізу і наведеного при відповіді на п. А.6.9 прихованого каналу обміну.

Примітка. У випадку позитивної відповіді на п. А.6.13 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні" рівня КВ-4.

А.7 Послуги довірчої/адміністративної цілісності

Послуги довірчої/адміністративної цілісності забезпечують можливість керування потоками інформації від об'єктів-користувачів до захищених пасивних об'єктів з метою захисту пасивних об'єктів від несанкціонованого створення, модифікації або видалення. Відповіді на наведені в розділі А.7 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ послуг довірчої/адміністративної цілісності, перелік об'єктів різного типу, стосовно яких визначена політика і реалізовані ці функціональні послуги безпеки, атрибутів доступу, використовуваних функціональними модулями КЗЗ при реалізації відповідних послуг. Сформульовані відповіді дозволять експерту визначити рівні, політику, засоби, механізми та особливості реалізації послуг довірчої/адміністративної цілісності, а також одержати вхідні дані для розроблення програм і методик випробувань цих послуг.

А.7.1 Чи існує в ОЕ для будь-якого з типів пасивних об'єктів, наведених при відповіді на запитання п. А.2.3.1, можливість розмежування доступу з боку користувачів, що відносяться до будь-якої з ролей (наведених при відповіді на п. А.2.1.1), або процесів різного типу (наведених при відповіді на п. А.2.2.1) до пасивних об'єктів цього типу з метою створення/ модифікації/ видалення об'єктів (створення потоків інформації від користувачів до об'єктів).

Примітка. Якщо такої можливості не існує, тобто, всі користувачі у межах певної ролі або всі процеси певного типу завжди мають однакові можливості доступу з метою створення/модифікації/видалення до всієї множини пасивних об'єктів усіх типів, то це означає, що послуги довірчої та/або адміністративної цілісності засобами КЗЗ ОЕ не реалізуються і відповідати на запитання п. А.7.2-А.7.13 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ реалізуються послуги довірчої та/або адміністративної цілісності, їх політики і рівні можуть бути уточнені при відповіді на запитання п. А.7.2-А.7.13.

А.7.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми керування доступом з боку об'єктів-користувачів одного чи декількох типів, наведених при відповіді на п. А.2.1.2, або об'єктів-процесів одного чи декількох типів, наведених при відповіді на п. А.2.2.1, до пасивних об'єктів одного чи декількох типів, наведених при відповіді на п. А.2.3.1, шляхом аналізу запитів на доступ з боку користувачів або об'єктів-процесів з метою створення/модифікації/видалення пасивного об'єкта (зміни об'єкта) і прийняття рішення на підставі інформації, що міститься в наборах атрибутів доступу ініціатора запиту (користувача або об'єкта-процесу) і пасивного об'єкта (з урахуванням відповідей на п. А.2.1.3, А.2.2.3, А.2.3.3). Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби, які дозволяють

користувачам, що відносяться до будь-якої з ролей (наведених при відповіді на п. А.2.1.1), змінювати відповідні набори атрибутів доступу об'єктів-користувачів та/або об'єктів-процесів і пасивних об'єктів.

Примітка. Механізмами, що забезпечують реалізацію послуг довірчої та адміністративної цілісності, є механізми керування доступом, тобто, надання можливості доступу до ресурсу згідно зі спеціально визначеними правилами. Як основні схеми, на підставі яких може здійснюватися керування доступом, можуть використовуватися схеми:

- на підставі списків керування доступом (під списком керування доступом слід розуміти пов'язаний із запитуваним ресурсом набір атрибутів доступу у вигляді сукупностей ідентифікаторів ініціаторів запиту та атрибутів, що визначають дозволені види доступу або операції над запитуваним ресурсом);

- на підставі списків повноважень (під списком повноважень слід розуміти пов'язаний з ініціатором запиту набір атрибутів доступу у вигляді сукупності операцій, дозволених над заданою множиною запитуваних ресурсів);

- на підставі міток безпеки (під мітками слід розуміти атрибути доступу, пов'язані як з ініціатором запиту, так і з запитуваним ресурсом, рішення про надання доступу приймається на підставі оброблення міток ініціатора і ресурсу за заданими правилами).

Для прийняття рішення про можливість надання доступу ці механізми можуть використовувати:

- ідентифікатори відповідних об'єктів;
- ідентифікатори груп відповідних об'єктів;
- інформацію про права доступу до пасивних об'єктів у вигляді міток доступу, списків керування доступом або списків повноважень;
- інформацію про права володіння пасивним об'єктом;
- інформацію про час спроби доступу;
- інформацію про маршрут запиту доступу в розподілених системах;
- інформацію про тривалість доступу до ресурсу.

Засоби керування доступом, що приймають рішення про можливість задоволення або відхилення запиту, повинні бути реалізовані в тих компонентах КЗЗ, що входять до складу ядра КЗЗ і реалізують концепцію диспетчера доступу. Засоби, що дозволяють змінювати атрибути доступу, можуть бути реалізовані в довільних компонентах КЗЗ. Якщо зазначених засобів у складі КЗЗ немає, то це означає, що послуги довірчої та/або адміністративної цілісності засобами КЗЗ ОЕ не реалізуються і відповідати на запитання п. А.7.3-А.7.13 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ реалізуються послуги довірчої та/або адміністративної цілісності, їх політики і рівні можуть бути уточнені при відповіді на запитання п. А.7.3-А.7.13.

А.7.3 Чи дозволяють реалізовані у складі функціональних модулів ОЕ, що входять до складу КЗЗ, засоби (з урахуванням відповіді на п. А.7.2) змінювати атрибути доступу об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів, на підставі яких реалізується керування доступом:

А.7.3.1 будь-яким користувачам, що відносяться до кожної з ролей, наведених при відповіді на п. А.2.1.1, але лише для частини пасивних об'єктів певних типів, наведених при відповіді на п. А.2.3.1, що належать їх домену, тобто з урахуванням атрибутів, що визначають їх права володіння цими пасивними об'єктами;

А.7.3.2 будь-яким користувачам, що відносяться лише до певних ролей, наведених при відповіді на п. А.2.1.1, для всіх пасивних об'єктів певних типів, наведених при відповіді на п. А.2.3.1, без урахування атрибутів, що визначають їх права володіння цими пасивними об'єктами.

Примітка. У випадку позитивної відповіді на п. А.7.3.1 можна стверджувати, що засобами КЗЗ реалізуються послуги довірчої цілісності. У випадку позитивної відповіді на п. А.7.3.2 можна стверджувати, що засобами КЗЗ реалізуються послуги адміністративної цілісності. Політики і рівні відповідних послуг для пасивних об'єктів різного типу можуть бути уточнені при відповіді на запитання п. А.7.4-А.7.13.

А.7.4 Чи відноситься політика послуг довірчої або адміністративної цілісності, реалізована КЗЗ (чи забезпечується можливість керування доступом об'єктів-користувачів або об'єктів-процесів до пасивних об'єктів, з урахуванням відповідей на п. А.7.3.1, А.7.3.2):

А.7.4.1 до всіх типів об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів, наведених при відповіді на п. А.2.1.2, А.2.2.1, А.2.3.1;

А.7.4.2 лише до певних (укажіть до яких) типів об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів, наведених при відповіді на п. А.2.1.2, А.2.2.1, А.2.3.1.

Примітка. У випадку позитивної відповіді на п. А.7.4.1 можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої цілісності рівнів ЦД-3 чи ЦД-4 або адміністративної цілісності рівнів ЦА-3 чи ЦА-4. У цьому випадку політика і рівні відповідних послуг можуть бути уточнені при відповіді на запитання п. А.7.5.2, А.7.6-А.7.13. У випадку негативної відповіді на п. А.7.3.1 можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої цілісності рівнів ЦД-1 чи ЦД-2 або адміністративної цілісності рівнів ЦА-1 чи ЦА-2 стосовно об'єктів, наведених при відповіді на п. А.7.4.2. У цьому випадку політика і рівні відповідних послуг можуть бути уточнені при відповіді на запитання п. А.7.5.1, А.7.5.2, А.7.6-А.7.13.

А.7.5 На підставі яких атрибутів доступу:

А.7.5.1 об'єктів-користувачів і пасивних об'єктів різних типів (з урахуванням відповідей на п. А.2.1.3 і А.2.3.3) або

А.7.5.2 об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різних типів

(з урахуванням відповідей на п. А.2.1.3, А.2.2.3 і А.2.3.3),
і згідно з якими правилами реалізується розмежування доступу для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4, до яких відноситься політика послуг довірчої або адміністративної цілісності.

А.7.6 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.7.2) з використанням механізмів керування доступом, здійснюється оброблення запитів на надання доступу (розмежування доступу) згідно із зазначеними при відповіді на п. А.7.5 правилами для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4.

А.7.7 На підставі яких атрибутів пасивних об'єктів (з урахуванням відповіді на
п. А.2.3.3) та атрибутів доступу об'єктів-користувачів (з урахуванням відповіді на п. А.2.1.3), що визначають права володіння для послуги довірчої цілісності або адміністративні повноваження для послуги адміністративної цілісності, і згідно з якими правилами здійснюється оброблення запитів на зміну прав доступу до захищених об'єктів для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4.

А.7.8 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.7.2), здійснюється оброблення запитів на зміну прав доступу до захищених об'єктів згідно із зазначеними при відповіді на п. А.7.7 правилами для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4.

А.7.9 Чи існує у функціональних компонентах ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.7.8, з використанням атрибутів доступу, наведених при відповіді на п. А.7.5, А.7.7, для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4:

А.7.9.1 можливість визначення конкретних користувачів та/або груп користувачів, що мають право створювати/видаляти/модифікувати об'єкт;

А.7.9.2 можливість визначення конкретних процесів та/або груп процесів, що мають право створювати/видаляти/модифікувати об'єкт;

А.7.9.3 можливість визначення конкретних процесів (і груп процесів), що мають, а також тих, що не мають права створювати/видаляти/модифікувати об'єкт;

А.7.9.4 можливість визначення конкретних користувачів і процесів (і груп користувачів та процесів), що мають, а також тих, що не мають права модифікувати об'єкт.

Примітка. У випадку позитивної відповіді на п. А.7.9.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-1 або адміністративної цілісності рівня ЦА-1. У випадку позитивної відповіді на п. А.7.9.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-2 або адміністративної цілісності рівні ЦА-2. У випадку позитивної відповіді на п. А.7.9.3 можна стверджувати, що засобами КЗЗ може бути реалізована

послуга довірчої цілісності рівня ЦД-3 або адміністративної цілісності рівні ЦА-3. У випадку позитивної відповіді на п. А.7.9.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-4 або адміністративної цілісності рівні ЦА-4.

А.7.10 Чи існує у функціональних компонентах ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.7.8, з використанням атрибутів доступу, наведених при відповіді на п. А.7.5, А.7.7 для об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4:

А.7.10.1 можливість визначення конкретних користувачів та/або груп користувачів, що мають право ініціювати процес;

А.7.10.2 можливість визначення конкретних користувачів (і груп користувачів), що мають, а також тих, що не мають права ініціювати процес.

Примітка. У випадку позитивної відповіді на п. А.7.10.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга довірчої цілісності рівня ЦД-2 або адміністративної цілісності рівня ЦА-2. У випадку позитивної відповіді на п. А.7.10.2 можна стверджувати, що засобами КЗЗ можуть бути реалізовані послуги довірчої цілісності рівня ЦД-3 чи ЦД-4 або адміністративної цілісності рівня ЦА-3 чи ЦА-4.

А.7.11 Які атрибути доступу, наведені при відповіді на п. А.7.5, А.7.7, що характеризують права доступу до захищених пасивних об'єктів різного типу, наведених при відповіді на п. А.7.4, установлюються:

А.7.11.1 у момент створення пасивного об'єкта;

А.7.11.2 у момент ініціалізації об'єкта.

Укажіть, яке значення призначається кожному атрибуту, обґрунтуйте його безпечність.

А.7.12 Чи зберігаються, якщо так, то які, атрибути доступу пасивних об'єктів, наведені при відповіді на п. А.7.5, А.7.7, що характеризують права користувачів по модифікації цих об'єктів (укажіть для пасивних об'єктів кожного з типів, наведених при відповіді на п. А.7.4) при експорті об'єкта за межі ОЕ. Яким чином здійснюється зв'язування переданих наборів атрибутів доступу з експортованими пасивними об'єктами різного типу.

А.7.13 Чи зберігаються, якщо так, то які, атрибути доступу пасивних об'єктів, наведені при відповіді на п. А.7.5, А.7.7, що характеризують права користувачів по модифікації цих об'єктів (укажіть для пасивних об'єктів кожного з типів, наведених при відповіді на п. А.7.4) при імпорті пасивного об'єкта із-зі межі ОЕ. Яким чином здійснюється зв'язування прийнятих наборів атрибутів доступу з імпортованими пасивними об'єктами різного типу.

А.8 Відкат

Послуга "Відкат" забезпечує можливість скасування операції або послідовності операцій, виконаних над захищеним пасивним об'єктом, з поверненням захищеного об'єкта в попередній стан. Відповіді на наведені в розділі А.8 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ послуги "Відкату", перелік пасивних об'єктів різного типу, стосовно яких визначено політику і реалізовано цю функціональну послугу

безпеки. Сформульовані відповіді дозволять експерту визначити рівень, політику, засоби, механізми та особливості реалізації послуги "Відкату", а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.8.1 Чи існує в ОЕ для будь-якого з типів пасивних об'єктів, наведених при відповіді на запитання п. А.2.3.1, можливість автоматизованого виконання скасування окремих операцій або послідовності операцій, пов'язаних зі зміною самих об'єктів або їх атрибутів, з поверненням пасивного об'єкта в стан, що передував виконанню операції або набору операцій.

Примітка. Якщо такої можливості не існує, то це означає, що послуга "Відкат" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.8.2-А.8.4 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ реалізується послуга "Відкат", її політика і рівні можуть бути уточнені при відповіді на запитання п. А.8.2-А.8.4.

А.8.2 Наведіть перелік типів пасивних об'єктів, наведених при відповіді на п. А.2.3.1, для яких існує зазначена при відповіді на п. А.8.1 можливість автоматизованого виконання скасування окремих операцій або послідовності операцій, пов'язаних зі зміною самих об'єктів або їх атрибутів, з поверненням пасивного об'єкта в стан, що передував виконанню операції або набору операцій, а також множину відповідних операцій для пасивних об'єктів кожного типу.

А.8.3 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), з використанням яких механізмів реалізується можливість скасування наведеної при відповіді на п. А.8.2 множини операцій, виконаних над захищеними пасивними об'єктами різного типу.

А.8.4 Чи забезпечується наведеними при відповіді на п. А.8.3 механізмами, реалізованими у функціональних модулях ОЕ, що входять до складу КЗЗ, можливість:

А.8.4.1 скасування всіх операцій, проведених над захищеними об'єктами за певний (укажіть який) проміжок часу (вкажіть для кожного з типів об'єктів, наведених при відповіді на п. А.8.2);

А.8.4.2 скасування лише певного набору (множини) операцій, проведених над захищеними об'єктами за певний (укажіть який) проміжок часу (вкажіть для кожного з типів об'єктів, наведених при відповіді на п. А.8.2).

Примітка. У випадку позитивної відповіді на п. А.8.4.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відкат" рівня ЦО-2. У випадку негативної відповіді на п. А.8.4.1 і позитивної відповіді на п. А.8.4.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відкат" рівня ЦО-1.

А.9 Цілісність при обміні

Послуга "Цілісність при обміні" дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, при їх передачі

(експорті/імпорті) через незахищене середовище. Відповіді на наведені в розділі А.9 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.9.1 Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними компонентами ОЕ через незахищене середовище пасивними об'єктами будь-якого з типів, наведених при відповіді на запитання п. А.2.3.1. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об'єктів.

Примітка. У випадку позитивної відповіді на п. А.9.1 можна стверджувати, що в ОЕ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1, ЦВ-2 чи ЦВ-3. У цьому випадку факт реалізації послуги, її політика та рівень можуть бути уточнені при відповіді на запитання п. А.9.2-А.9.9. У випадку негативної відповіді на п. А.9.1 можна стверджувати, що послуга "Цілісність при обміні" в ОЕ не реалізується і відповідати на запитання п. А.9.2-А.9.9 не потрібно.

А.9.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми, які забезпечують:

А.9.2.1 виявлення фактів несанкціонованої модифікації інформації, що міститься в переданих пасивних об'єктах, наведених при відповіді на п. А.9.1, при їх передачі між різними компонентами ОЕ через незахищене середовище;

А.9.2.2 виявлення фактів несанкціонованого видалення або дублювання переданих пасивних об'єктів, наведених при відповіді на п. А.9.1, при їх передачі між різними компонентами ОЕ через незахищене середовище.

Примітка. Функціонування механізмів, що забезпечують реалізацію послуги "Цілісність при обміні", в частині, що стосується виявлення фактів несанкціонованої модифікації, може ґрунтуватися на одному з таких принципів:

- виявлення порушень цілісності шляхом вироблення/перевірки криптографічних (таких, що обчислюються з використанням ключових даних) кодів контролю цілісності (кодів автентифікації повідомлень);

- виявлення порушень цілісності шляхом вироблення/перевірки некриптографічних кодів контролю цілісності з їх подальшим зашифруванням/розшифруванням;

- виявлення порушень цілісності шляхом вироблення/перевірки електронного цифрового підпису;

- виявлення порушень цілісності шляхом зашифрування/розшифрування повідомлень, що містять надмірні дані (наприклад, текст оригінальною мовою), з подальшим контролем збереження надмірності.

Функціонування механізмів, що забезпечують реалізацію послуги "Цілісність при обміні", в частині, що стосується виявлення фактів

несанкціонованого видалення або дублювання переданих пасивних об'єктів, може ґрунтуватися на принципі використання погодженого контексту повідомлення (наприклад, порядкового номера або часової мітки) у комбінації з механізмами, що забезпечують виявлення фактів несанкціонованої модифікації.

Якщо засобів, що реалізують механізми, наведені при відповіді на п. А.9.2.1, у складі КЗЗ немає, то це означає, що послуга "Цілісність при обміні" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.9.3-А.9.9 не потрібно. Якщо ж такі засоби існують, то це означає, що засобами КЗЗ може бути реалізована послуга "Конфіденційність при обміні", остаточно факт її реалізації і політика можуть бути уточнені при відповіді на запитання п. А.9.3-А.9.9.

А.9.3 Наведіть перелік типів пасивних об'єктів (з урахуванням відповіді на п. А.9.1), а також використовуваних для їх приймання/передачі функціональних модулів ОЕ, що входять до складу КЗЗ (інтерфейсних процесів), стосовно яких визначена політика функціональної послуги "Цілісність при обміні", тобто, забезпечується можливість виявлення фактів несанкціонованої модифікації інформації, що міститься в переданих пасивних об'єктах, при їх передачі через незахищене середовище.

А.9.4 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.9.2.1), з використанням яких саме механізмів захисту реалізується виявлення фактів несанкціонованої модифікації інформації, що міститься в переданих пасивних об'єктах кожного з типів, наведених при відповіді на п. А.9.3. Який рівень захищеності забезпечується використовуваними механізмами. Якими параметрами (якими атрибутами доступу пасивних об'єктів або властивостями використовуваних механізмів) визначається рівень захищеності, забезпечуваний для пасивних об'єктів різного типу, наведених при відповіді на п. А.9.3. Чи існує можливість у користувачів та/або процесів (укажіть яких, з урахуванням відповідей на п. А.2.1.1, А.2.1.2, А.2.2.1, А.2.2.2), з використанням відповідних функціональних модулів ОЕ, що входять до складу КЗЗ (вкажіть яких, з урахуванням відповідей на п. А.1.2.1, А.1.2.2), керувати (шляхом зміни відповідних параметрів) рівнем захищеності, що забезпечується для пасивних об'єктів різного типу.

Примітка. У випадку позитивної відповіді на п. А.9.4 (в частині можливості керування рівнем захищеності) можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-2 чи ЦВ-3. У випадку негативної відповіді на п. А.9.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1, відповідати на запитання п. А.9.5-А.9.9 не потрібно.

А.9.5 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.9.2.2), з використанням яких саме механізмів захисту реалізується виявлення фактів видалення чи дублювання переданих пасивних об'єктів, наведених при відповіді на п. А.9.3. Який рівень захищеності забезпечується використовуваними механізмами. Якими параметрами (якими атрибутами доступу пасивних об'єктів або властивостями використовуваних механізмів) визначається рівень захищеності, забезпечуваний для пасивних

об'єктів різного типу, наведених при відповіді на п. А.9.3. Чи існує можливість у користувачів та/або процесів (укажіть яких, з урахуванням відповідей на п. А.2.1.1, А.2.1.2, А.2.2.1, А.2.2.2), з використанням відповідних функціональних модулів ОЕ, що входять до складу КЗЗ (укажіть яких, з урахуванням відповідей на п. А.1.2.1, А.1.2.2), керувати (шляхом зміни відповідних параметрів) рівнем захищеності, що забезпечується для пасивних об'єктів різного типу.

Примітка. У випадку позитивної відповіді на п. А.9.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-2 чи ЦВ-3. У випадку негативної відповіді на п. А.9.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1, відповідати на запитання п. А.9.6-А.9.9 не потрібно.

А.9.6 Чи існує можливість у наведених при відповіді на п. А.9.4, А.9.5 засобах керування рівнем захищеності, що забезпечується для пасивних об'єктів різного типу, оброблення запитів на присвоєння або зміну рівня захищеності лише у випадку, якщо вони надходять від користувачів, що відносяться лише до певних ролей, наведених при відповіді на п. А.2.1.1 (від адміністраторів або користувачів, яким надані відповідні повноваження). На підставі яких атрибутів об'єктів-користувачів (з урахуванням відповіді на п. А.2.1.3), що визначають їх повноваження, і за якими правилами виконується оброблення цих запитів.

Примітка. У випадку позитивної відповіді на п. А.9.6 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-2 чи ЦВ-3. У випадку негативної відповіді на п. А.9.6 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1, відповідати на запитання п. А.9.7-А.9.9 не потрібно.

А.9.7 Чи обробляються запити на експорт (передачу) захищеного пасивного об'єкта передавальним компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

А.9.7.1 атрибутів доступу інтерфейсного процесу, що здійснює передачу, і КЗЗ (компонента КЗЗ), що є приймачем об'єкта (вкажіть яких, з урахуванням відповіді на п. А.2.2.3);

А.9.7.2 лише атрибутів доступу інтерфейсного процесу, що здійснює передачу (вкажіть яких, з урахуванням відповіді на п. А.2.2.2).

Примітка. У випадку позитивної відповіді на п. А.9.7.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-3. У випадку негативної відповіді на п. А.9.7.1 і позитивної відповіді на п. А.9.7.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-2. У випадку негативної відповіді на п. А.9.7.1 і А.9.7.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1, відповідати на запитання п. А.9.8-А.9.9 не потрібно.

А.9.8 Чи обробляються запити на імпорт (приймання) захищеного пасивного об'єкта приймаючим компонентом (функціональним модулем ОЕ, що входить до складу КЗЗ) на підставі:

А.9.8.1 атрибутів доступу інтерфейсного процесу, що здійснює приймання, і КЗЗ (компонента КЗЗ), що є джерелом об'єкта (вкажіть яких, з урахуванням відповідей на п. А.2.2.3);

А.9.8.2 лише атрибутів доступу інтерфейсного процесу, що здійснює приймання (вкажіть яких, з урахуванням відповіді на п. А.2.2.3).

Примітка. У випадку позитивної відповіді на п. А.9.8.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-3. У випадку негативної відповіді на п. А.9.8.1 і позитивної відповіді на п. А.9.8.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-2, відповідати на запитання п. А.9.9 не потрібно. У випадку негативних відповідей на п. А.9.8.1 і А.9.8.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-1, відповідати на запитання п. А.9.9 не потрібно.

А.9.9 Чи є представлення захищеного переданого пасивного об'єкта функцією атрибутів доступу інтерфейсного процесу (з урахуванням відповідей на п. А.9.7.1, А.9.8.1), самого об'єкта (з урахуванням відповіді на п. А.2.3.3), а також його джерела і приймача (з урахуванням відповідей на п. А.9.7.1, А.9.8.1). Якщо так, то опишіть відповідну функціональну залежність.

Примітка. У випадку позитивної відповіді на п. А.9.9 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність при обміні" рівня ЦВ-3.

А.10 Використання ресурсів

Послуга "Використання ресурсів" дозволяє забезпечити доступність послуг і ресурсів ОЕ шляхом керування обсягом ресурсів, що виділяються користувачам. Відповіді на наведені в розділі А.10 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги та перелік об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.10.1 Чи існує в ОЕ можливість керування обсягом поділюваних ресурсів, що надаються користувачу і використовуються в процесі оброблення, збереження або передачі пасивних об'єктів будь-якого з типів, наведених при відповіді на запитання п. А.2.3.1.

Примітка. Як приклади поділюваних ресурсів, використовуваних для збереження, оброблення або передачі пасивних об'єктів різних типів, можна навести:

- дисковий простір (для збереження об'єктів у вигляді файлів);
- табличний простір СКБД (для збереження об'єктів у вигляді записів таблиць СКБД);
- мережеві з'єднання (для передачі пасивних об'єктів);

- процесорний час, що виділяється певному користувачу для виконання ініційованих ним процесів, тощо.

Якщо можливості керування обсягом поділюваних ресурсів, що надаються користувачу, в ОЕ не існує, то це означає, що послуга "Використання ресурсів" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.10.2-А.10.9 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.10.2-А.10.9.

А.10.2 Чи відноситься політика послуги (можливість керування обсягом ресурсів, що виділяються користувачу) до поділюваних ресурсів, використовуваних для оброблення, збереження і передачі:

А.10.2.1 пасивних об'єктів усіх типів, наведених при відповіді на п. А.2.3.1;

А.10.2.2 пасивних об'єктів лише деяких (укажіть яких) типів, наведених при відповіді на п. А.2.3.1.

Примітка. У випадку позитивної відповіді на п. А.10.2.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-2 чи ДР-3. У випадку негативної відповіді на п. А.10.2.1 і позитивної відповіді на п. А.10.2.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-1.

А.10.3 Наведіть перелік обмежень (з урахуванням відповіді на п. А.10.2) на обсяг поділюваних ресурсів, що виділяються користувачу і використовуються для оброблення, збереження і передачі пасивних об'єктів різного типу.

А.10.4 Чи існує можливість у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), установлювати наведені при відповіді на п. А.10.3 обмеження для:

А.10.4.1 окремих користувачів і довільних груп користувачів різного типу (з урахуванням відповідей на п. А.2.1.1, А.2.1.2);

А.10.4.2 лише окремих користувачів різного типу (з урахуванням відповідей на п. А.2.1.1, А.2.1.2).

Примітка. У випадку позитивної відповіді на п. А.10.4.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-3. У випадку негативної відповіді на п. А.10.4.1 і позитивної відповіді на п. А.10.4.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-1 чи ДР-2.

А.10.5 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), з використанням яких саме механізмів реалізується контроль за дотриманням встановлених обмежень, наведених при відповіді на п. А.10.3, на обсяг поділюваних ресурсів, що виділяються користувачам різного типу (з урахуванням відповіді на п. А.10.4) і використовуються для оброблення, збереження і передачі пасивних об'єктів різного типу. На підставі яких атрибутів користувачів і груп користувачів (з урахуванням відповіді на п. А.2.1.3), пасивних об'єктів (з урахуванням відповіді

на п. А.2.3.3) і за якими правилами виконується прийняття рішення про виділення або невиділення користувачу (групі) необхідного обсягу ресурсу.

А.10.6 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), здійснюється оброблення запитів на зміну встановлених обмежень, наведених при відповіді на п. А.10.3, на обсяг поділюваних ресурсів, що виділяються користувачам різного типу (з урахуванням відповіді на п. А.10.4) і використовуються для оброблення, збереження і передачі пасивних об'єктів різного типу.

А.10.7 Чи існує можливість у засобах, наведених при відповіді на п. А.10.6, оброблення запитів на зміну встановлених обмежень лише у випадку, якщо вони надходять від користувачів, що відносяться лише до певних ролей, наведених при відповіді на п. А.2.1.1 (від адміністраторів або користувачів, яким надані відповідні повноваження). На підставі яких атрибутів об'єктів-користувачів (з урахуванням відповіді на п. А.2.1.3), що визначають їх повноваження, і за якими правилами виконується оброблення цих запитів.

Примітка. У випадку позитивної відповіді на п. А.10.7 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-1, ДР-2 чи ДР-3. У випадку негативної відповіді на п. А.10.7 можна стверджувати, що послуга "Використання ресурсів" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.10.8-А.10.9 не потрібно.

А.10.8 Чи існує можливість у вказаних у п. А.10.7 засобах установлювати зазначені в п. А.10.3 обмеження таким чином, щоб засоби КЗЗ мали можливість запобігти діям, які можуть призвести до недоступності функцій (послуг) ОЕ для інших користувачів:

А.10.8.1 з боку окремого користувача і довільних груп користувачів;

А.10.8.2 лише з боку окремого користувача.

Примітка. У випадку позитивної відповіді на п. А.10.8.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-3. У випадку негативної відповіді на п. А.10.8.1 і позитивної відповіді на п. А.10.8.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Використання ресурсів" рівня ДР-2.

А.10.9 Наведіть правила, згідно з якими, на підставі атрибутів пасивних об'єктів і використовуваних для їх оброблення, збереження і передачі поділюваних ресурсів, наведених при відповіді на п. А.10.2, А.10.3, атрибутів користувачів або груп користувачів різного типу, наведених при відповіді на п. А.10.4, у функціональних компонентах ОЕ, що входять до складу КЗЗ і задіяні у реалізації послуги (з урахуванням відповіді на п. А.10.5), реалізуються можливості встановлення обмежень, наведених при відповіді на п. А.10.8.

А.11 Стійкість до відмов

Послуга "Стійкість до відмов" дозволяє забезпечити доступність послуг і ресурсів ОЕ шляхом забезпечення використання окремих функцій ОЕ чи ОЕ в цілому після відмови його компонента. Відповіді на наведені в розділі А.11 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в

ОЕ цієї послуги, перелік компонентів і типів відмов, стосовно яких вона реалізована. Сформульовані відповіді дозволять експерту визначити політику, засоби та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.11.1 Чи існує в ОЕ можливість збереження часткової або повної працездатності та продовження виконання функцій з оброблення інформації при відмові (виході з ладу) будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на запитання п. А.1.2.1, А.1.2.2, або компонентів обчислювальної системи, на базі яких функціонують відповідні функціональні модулі, наведені при відповіді на запитання п. А.1.1.3.

Примітка. Якщо можливість збереження часткової або повної працездатності при відмові функціональних модулів ОЕ, що входять до складу КЗЗ, або компонентів обчислювальної системи, на базі яких функціонують відповідні функціональні модулі, відсутня, то це означає, що послуга "Стійкість до відмов" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.11.2-А.11.5 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Стійкість до відмов", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.11.2-А.11.5.

А.11.2 Наведіть (з урахуванням відповідей на п. А.1.1.3, А.1.2.1, А.1.2.2) результати аналізу відмов функціональних модулів ОЕ, що входять до складу КЗЗ, і компонентів обчислювальної системи, на базі яких функціонують відповідні функціональні модулі, з наведенням модулів (компонентів) і типів відмов, після яких ОЕ в стані продовжувати функціонування, нехай і зі зниженням характеристик обслуговування (вкажіть яких), а також компонентів і типів відмов, що призводять до недоступності певних функцій (послуг) ОЕ (вкажіть, яких). У наведених результатах аналізу повинні бути чітко вказані (для всіх проаналізованих функціональних модулів ОЕ, що входять до складу КЗЗ, і компонентів обчислювальної системи) рівні відмов, які призводять до зниження характеристик обслуговування або до недоступності певних функцій (послуг) ОЕ.

А.11.3 Чи відносяться результати аналізу, наведені при відповіді на п. А.11.2:

А.11.3.1 до всіх функціональних модулів ОЕ, що входять до складу КЗЗ;

А.11.3.2 лише до частини функціональних модулів ОЕ (вкажіть яких), що входять до складу КЗЗ.

Примітка. У випадку позитивної відповіді на п. А.11.3.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Стійкість до відмов" рівня ДС-2 чи ДС-3. У випадку негативної відповіді на п. А.11.3.1 і позитивної відповіді на п. А.11.3.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Стійкість до відмов" рівня ДС-1.

А.11.4 Чи забезпечується умова збереження доступності (працездатності) при відмові будь-якого функціонального модуля ОЕ, введеного до складу КЗЗ, або компонента обчислювальної системи, на базі якого функціонує відповідний

модуль, з наведених при відповіді на п. А.11.2, А.11.3, для всіх інших функціональних модулів ОЕ, внесених до складу КЗЗ:

А.11.4.1 без зниження характеристик обслуговування;

А.11.4.2 зі зниженням характеристик обслуговування (вкажіть яких).

Примітка. У випадку позитивної відповіді на п. А.11.4.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Стійкість до відмов" рівня ДС-3. У випадку негативної відповіді на п. А.11.4.1 і позитивної відповіді на п. А.11.4.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Стійкість до відмов" рівня ДС-1 чи ДС-2.

А.11.5 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), з використанням яких саме механізмів реалізується можливість оповіщення користувачів, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів), про відмову будь-якого захищеного компонента з наведених при відповіді на п. А.11.3.

Примітка. У випадку, якщо відповідні механізми оповіщення адміністратора реалізовані, можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Стійкість до відмов" рівня ДС-1, ДС-2 чи ДС-3. У випадку відсутності таких механізмів можна стверджувати, що послуга "Стійкість до відмов" засобами КЗЗ ОЕ не реалізується.

А.12 Гаряча заміна

Послуга "Гаряча заміна" дозволяє забезпечити доступність послуг і ресурсів ОЕ в процесі заміни окремих його компонентів. Відповіді на наведені в розділі А.12 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік компонентів, стосовно яких вона реалізована. Сформульовані відповіді дозволять експерту визначити політику, засоби та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.12.1 Чи існує в ОЕ можливість проведення заміни (модернізації) будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на запитання п. А.1.2.1, А.1.2.2, без необхідності заново проводити інсталяцію ОЕ або настроювання відповідних функціональних модулів.

Примітка. Якщо можливість проведення заміни (модернізації) будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, без необхідності заново проводити інсталяцію ОЕ або настроювання відповідних функціональних модулів, відсутня, то це означає, що послуга "Гаряча заміна" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.12.2-А.12.5 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Гаряча заміна", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.12.2-А.12.5.

А.12.2 Наведіть (з урахуванням відповідей на п. А.1.2.1, А.1.2.2, А.12.1) перелік функціональних модулів ОЕ, що входять до складу КЗЗ, які можуть бути замінені (модернізовані) без необхідності заново проводити інсталяцію ОЕ або настроювання відповідних функціональних модулів. Чи складає зазначений

перелік:

12.2.1 всю множину функціональних модулів ОЕ, що входять до складу КЗЗ;

12.2.2 лише частину множини функціональних модулів ОЕ, що входять до складу КЗЗ.

Примітка. У випадку позитивної відповіді на п. А.12.2.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Гаряча заміна" рівня ДЗ-3 чи ДЗ-2. У випадку негативної відповіді на п. А.12.2.1 і позитивної відповіді на п. А.12.2.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Гаряча заміна" рівня ДЗ-1.

А.12.3 Чи існує можливість проведення, з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), заміни (модернізації) усіх функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.12.2, лише користувачами, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторами або користувачами, яким надані відповідні повноваження).

Примітка. У випадку позитивної відповіді на п. А.12.3 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Гаряча заміна" рівня ДЗ-1, ДЗ-2 чи ДЗ-3. У випадку негативної відповіді на п. А.12.3 можна стверджувати, що послуга "Гаряча заміна" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.12.4-А.12.5 не потрібно.

А.12.4 Чи існує можливість проведення користувачами, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторами або користувачами, яким надані відповідні повноваження), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2, А.12.3), заміни (модернізації) без переривання обслуговування (без зупинки і наступного запуску ОЕ):

А.12.4.1 кожного з функціональних модулів ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.12.2;

А.12.4.2 лише деяких функціональних модулів ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.12.2 (вкажіть яких).

Примітка. У випадку позитивної відповіді на п. А.12.4.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Гаряча заміна" рівня ДЗ-3. У випадку негативної відповіді на п. А.12.4.1 і позитивної відповіді на п. А.12.4.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Гаряча заміна" рівня ДЗ-2.

А.12.5 На підставі яких атрибутів доступу об'єктів-користувачів, наведених при відповіді на п. А.2.1.3, що визначають їх приналежність до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2, А.12.3), і згідно з якими правилами здійснюється оброблення запитів на виконання заміни (модернізації) різних функціональних модулів ОЕ, що

входять до складу КЗЗ та наведені при відповіді на п. А.12.2.

А.13 Відновлення після збоїв

Послуга "Відновлення після збоїв" дозволяє забезпечити доступність послуг і ресурсів ОЕ шляхом переведення ОЕ у відомий захищений стан після відмови або переривання обслуговування. Відповіді на наведені в розділі А.13 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік компонентів, стосовно яких вона реалізована. Сформульовані відповіді дозволять експерту визначити політику, засоби та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.13.1 Чи існує в ОЕ можливість повернення у визначений захищений стан у випадку відмови або збою будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на запитання п. А.1.2.1, А.1.2.2.

Примітка. Якщо можливість повернення у визначений захищений стан у випадку відмови або збою будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ, відсутня, то це означає, що послуга "Відновлення після збоїв" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.13.2-А.13.11 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.13.2-А.13.11.

А.13.2 Наведіть (з урахуванням відповідей на п. А.1.1.3, А.1.2.1, А.1.2.2) результати аналізу відмов функціональних модулів ОЕ, що входять до складу КЗЗ, з наведенням функціональних модулів, типів відмов і переривань обслуговування, після яких можливе повернення у визначений захищений стан без порушення політики безпеки. У наведених результатах аналізу повинні бути чітко вказані (для всіх проаналізованих функціональних модулів ОЕ, що входять до складу КЗЗ) рівні відмов, при перевищенні яких необхідна повторна інсталяція ОЕ.

А.13.3 Чи існує можливість при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (вкажіть яких, з урахуванням відповідей на п. А.1.2.1, А.1.2.2), переведення ОЕ у стан з припиненням обслуговування, з якого повернути його до нормального функціонування можуть лише користувачі, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністратори або користувачі, яким надані відповідні повноваження). За якими правилами приймається рішення про необхідність переведення ОЕ у такий стан при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2), які характеристики цього стану.

Примітка. У випадку позитивної відповіді на п. А.13.3 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв" рівня ДВ-1, ДВ-2 чи ДВ-3. У випадку негативної відповіді на п.

А.13.3 можна стверджувати, що послуга "Відновлення після збоїв" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.13.4-А.13.11 не потрібно.

А.13.4 Чи існує можливість при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), визначення можливості використання автоматизованих процедур для повернення безпечним чином ОЕ до нормального функціонування. За якими правилами приймається рішення про можливість використання автоматизованих процедур для повернення ОЕ до нормального функціонування для різних типів відмов різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2).

Примітка. У випадку позитивної відповіді на п. А.13.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв" рівня ДВ-2 чи ДВ-3.

А.13.5 Чи існує можливість при відмові різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2), з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), визначення можливості використання автоматизованих процедур для повернення безпечним чином ОЕ до функціонування в режимі з погіршеними характеристиками обслуговування. За якими правилами приймається рішення про можливість використання автоматизованих процедур для повернення ОЕ до функціонування в режимі з погіршеними характеристиками обслуговування для різних типів відмов різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2).

Примітка. У випадку позитивної відповіді на п. А.13.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв" рівня ДВ-3.

А.13.6 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані автоматизовані процедури для повернення безпечним чином функціональних модулів ОЕ, що входять до складу КЗЗ, після відмови або переривання обслуговування (з урахуванням відповідей на п. А.13.4, А.13.5) до нормального функціонування або функціонування в режимі з погіршеними характеристиками обслуговування. Яким чином (за якими правилами та у якій послідовності) виконується повернення після відмови або переривання обслуговування до нормального функціонування або функціонування в режимі з погіршеними характеристиками обслуговування при різних типах відмов різних функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.13.2).

А.13.7 Чи існує можливість з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (укажіть яких, для різних типів відмов, з урахуванням відповідей на п. А.1.2.1, А.1.2.2 і

А.13.2), у випадку, якщо автоматизовані процедури, наведені при відповіді на п. А.13.4, А.13.5, не можуть бути використані, переведення ОЕ у стан з припиненням обслуговування, з якого повернути його до нормального функціонування можуть лише користувачі, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністратори або користувачі, яким надані відповідні повноваження).

Примітка. У випадку позитивної відповіді на п. А.13.7 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв" рівня ДВ-2 чи ДВ-3.

А.13.8 Чи існує можливість з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (укажіть яких, для різних типів відмов, з урахуванням відповідей на п. А.1.2.1, А.1.2.2 і А.13.2), повернення користувачами, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторами або користувачами, яким надані відповідні повноваження), ОЕ зі стану з припиненням обслуговування (з урахуванням відповідей на п. А.13.3, А.13.7) до нормального функціонування.

Примітка. У випадку позитивної відповіді на п. А.13.8 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв" рівня ДВ-1, ДВ-2 чи ДВ-3.

А.13.9 Чи існує можливість з використанням засобів, реалізованих у відповідних функціональних модулях ОЕ, що входять до складу КЗЗ (укажіть яких, для різних типів відмов, з урахуванням відповідей на п. А.1.2.1, А.1.2.2 і А.13.2), повернення користувачами, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторами або користувачами, яким надані відповідні повноваження), ОЕ з режиму з погіршеними характеристиками обслуговування (з урахуванням відповіді на п. А.13.5) до нормального функціонування.

Примітка. У випадку позитивної відповіді на п. А.13.9 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Відновлення після збоїв" рівня ДВ-3.

А.13.10 На підставі яких атрибутів доступу об'єктів-користувачів, наведених при відповіді на п. А.2.1.3, що визначають їх приналежність до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), і згідно з якими правилами здійснюється оброблення запитів на повернення ОЕ зі стану з припиненням обслуговування (з урахуванням відповідей на п. А.13.3, А.13.8) до нормального функціонування.

А.13.11 На підставі яких атрибутів доступу об'єктів-користувачів, наведених при відповіді на п. А.2.1.3, що визначають їх приналежність до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), і згідно з якими правилами здійснюється оброблення запитів на повернення ОЕ зі стану з погіршеними характеристиками обслуговування (з

урахуванням відповідей на п. А.13.5, А.13.9) до нормального функціонування.

А.14 Реєстрація

Послуга "Реєстрація" дозволяє контролювати небезпечні для ОЕ дії. Відповіді на наведені в розділі А.14 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, визначити політику, засоби та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.14.1 Чи існує в ОЕ можливість реєстрації подій, пов'язаних зі спробами або фактами виконання певних дій, що мають безпосереднє або непряме відношення до безпеки оброблюваної інформації.

Примітка. Під можливістю реєстрації подій слід розуміти наявність засобів, що дозволяють, як мінімум, виконувати такі дії:

- виявляти (реєструвати) факти виникнення подій;
- генерувати записи в журналі реєстрації;
- накопичувати і зберігати дані журналів реєстрації або передавати їх в інші системи.

Під подіями, що мають відношення до безпеки, слід розуміти події, пов'язані зі спробами або фактами певних дій, які стосуються виконання функціональними модулями ОЕ, що входять до складу КЗЗ, операцій згідно з вимогами політики різних функціональних послуг безпеки. Якщо така можливість відсутня, то це означає, що послуга "Реєстрація" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.14.2-А.14.17 не потрібно. Якщо така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Реєстрація", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.14.2-А.14.17.

А.14.2 Наведіть перелік подій, пов'язаних зі спробами або фактами виконання певних дій, що мають безпосереднє або непряме відношення до безпеки оброблюваної інформації, реєстрація яких можлива засобами, реалізованими у складі ОЕ.

Примітка. Чіткого визначення поняття події, що має безпосереднє відношення до безпеки, не існує, однак, зазвичай під такою подією слід розуміти подію, пов'язану зі зверненням до засобів КЗЗ, які реалізують будь-яку функціональну послугу безпеки, наприклад:

- надання доступу;
- відмова в доступі;
- виконання автентифікації;
- зміна атрибутів доступу;
- створення об'єкта;
- модифікація об'єкта;
- видалення об'єкта;
- використання привілеїв тощо.

Під подіями, що мають непряме відношення до безпеки, слід розуміти події, які, хоча прямо і не пов'язані з функціонуванням засобів КЗЗ, що реалізують будь-яку функціональну послугу безпеки, але можуть призвести до порушення безпеки оброблюваної інформації.

А.14.3 Наведіть перелік реєстраційних подій (як частину всього переліку реєстраційних подій, наведеного при відповіді на п. А.14.2), що мають безпосереднє відношення до безпеки.

А.14.4 Наведіть перелік реєстраційних подій (як частину всього переліку реєстраційних подій, наведеного при відповіді на п. А.14.2), що мають непряме відношення до безпеки.

Примітка. У випадку, якщо до переліку подій, що мають непряме відношення до безпеки, внесено хоча б одну подію, можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Реєстрація" рівня НР-4 чи НР-5, у протилежному випадку можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Реєстрація" рівнів НР-1, НР-2 чи НР-3.

А.14.5 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані засоби реєстрації фактів виникнення подій різного типу, наведених при відповіді на п. А.14.2. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані засоби запису (занесення) в журнал реєстрації інформації про події різного типу, наведені при відповіді на п. А.14.2. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані засоби збереження журналів реєстрації, в якому вигляді та в якому сховищі зберігаються журнали.

А.14.6 Наведіть структуру запису журналу реєстрації. Чи дозволяє структура запису журналу реєстрації зберегти інформацію про дату, час, місце, тип та успішність або неуспішність кожної зареєстрованої події. Чи дозволяє структура запису журналу реєстрації зберегти інформацію, достатню для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Примітка. У випадку позитивної відповіді на п. А.14.6 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівнів НР-1 – НР-5. У випадку негативної відповіді на п.А.14.6 можна стверджувати, що послуга "Реєстрація" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.14.7-А.14.17 не потрібно.

А.14.7 Чи існує можливість з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), передачі збереженого журналу реєстрації (з урахуванням відповіді на п. А.14.5) в інші системи з використанням певних механізмів захисту переданого журналу від несанкціонованого доступу з метою модифікації або руйнування.

Примітка. У випадку позитивної відповіді на п. А.14.6 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга

"Реєстрація" рівня НР-1.

А.14.8 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.14.7), реалізовані засоби передачі збереженого журналу реєстрації (з урахуванням відповіді на п. А.14.5) в інші системи. З використанням яких саме механізмів реалізується захист переданого журналу від несанкціонованого доступу з метою модифікації або руйнування. Який порядок функціонування цих механізмів.

А.14.9 Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), захисту збереженого журналу реєстрації (з урахуванням відповіді на п. А.14.5) від несанкціонованого доступу з метою модифікації або руйнування.

Примітка. У випадку позитивної відповіді на п. А.14.9 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівнів НР-2 – НР-5. У випадку негативної відповіді на п. А.14.9 можна стверджувати, що, за умови позитивної відповіді на п. А.14.7, засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівня НР-1.

А.14.10 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.14.9), реалізовані засоби захисту збереженого журналу реєстрації (з урахуванням відповіді на п. А.14.5) від несанкціонованого доступу з метою модифікації або руйнування. З використанням яких саме механізмів реалізується захист збереженого журналу від несанкціонованого доступу з метою модифікації або руйнування. Який порядок функціонування цих механізмів.

А.14.11 Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), перегляду та аналізу збереженого (з урахуванням відповіді на п. А.14.5) журналу реєстрації.

Примітка. У випадку позитивної відповіді на п. А.14.11 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівнів НР-2 – НР-5. У випадку негативної відповіді на п. А.14.11 можна стверджувати, що, за умови позитивної відповіді на п. А.14.7, засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівня НР-1, відповідати на запитання п. А.14.12-А.14.17 не потрібно.

А.14.12 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.14.11), реалізовані засоби перегляду та аналізу збережених (з урахуванням відповіді на п. А.14.5) журналів реєстрації. Які саме функції перегляду та аналізу журналів реєстрації вони реалізують.

А.14.13 Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), контролю одиничних або повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки.

Примітка. Як підходи до забезпечення контролю реєстраційних подій можуть використовуватися, наприклад, такі:

- порівняння результатів дій деякого користувача або об'єкта-процесу із заздалегідь заданим набором правил (профілем);

- виявлення факту виникнення подій одного або декількох типів протягом заданого періоду часу;

- виявлення факту відсутності подій одного або декількох типів протягом заданого періоду часу.

У випадку позитивної відповіді на п. А.14.13 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівнів НР-3, НР-4 чи НР-5.

А.14.14 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.14.13), реалізовані засоби контролю одиничних або повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки. Виникнення яких подій, наведених при відповіді на п. А.14.3, А.14.4, вони дозволяють контролювати. Який порядок функціонування цих засобів.

А.14.15 Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), негайного інформування адміністратора про події, які свідчать про перевищення порогів безпеки, і здійснення неруйнівних дій щодо припинення повторення цих подій.

Примітка. У випадку позитивної відповіді на п. А.14.15 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівнів НР-3, НР-4 чи НР-5.

А.14.16 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.14.15), реалізовані засоби негайного інформування адміністратора про події, які свідчать про перевищення порогів безпеки, і здійснення неруйнівних дії щодо припинення повторення цих подій. Про виникнення яких подій, наведених при відповіді на п. А.14.3, А.14.4, вони дозволяють негайно інформувати адміністратора. Який порядок функціонування цих засобів, які механізми використовуються для негайного інформування адміністратора та для здійснення неруйнівних дії щодо припинення повторення критичних подій.

А.14.17 Чи забезпечується функціонування реалізованих у складі функціональних модулів ОЕ, що входять до складу КЗЗ, засобів, які реалізують реєстрацію подій різного типу, запис (занесення) інформації в журнал реєстрації (з урахуванням відповіді на А.14.5), контроль одиничних або повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки (з урахуванням відповіді на п. А.14.14), негайне інформування адміністратора про події, які свідчать про перевищення порогів безпеки, і здійснення неруйнівних дії щодо припинення повторення цих подій (з урахуванням відповіді на п. А.14.16) у режимі реального часу.

Примітка. У випадку позитивної відповіді на п. А.14.17 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Реєстрація" рівня НР-5.

А.15 Ідентифікація та автентифікація

Послуга "Ідентифікація та автентифікація" дозволяє КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до ОЕ. Відповіді на наведені в розділі А.15 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.15.1 Чи існує в ОЕ можливість однозначної ідентифікації користувачів, що відносяться до різних ролей, наведених при відповіді на п. А.2.1.1, і виконують різні операції, на підставі призначених їм унікальних (у межах ОЕ) ідентифікаторів або інших атрибутів, наведених при відповіді на п. А.2.1.3.

Примітка. Якщо можливості однозначної ідентифікації користувачів на підставі призначених їм унікальних (у межах ОЕ) ідентифікаторів або інших атрибутів у ОЕ не існує, то це означає, що послуга "Ідентифікація та автентифікація" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.15.2-А.15.9 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.15.2-А.15.9.

А.15.2 Наведіть перелік функціональних послуг безпеки, реалізованих функціональними модулями ОЕ, введеними до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), для реалізації яких необхідні атрибути користувачів, наведені при відповіді на п. А.15.1.

А.15.3 Чи існує можливість з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), одержання (перш ніж дозволити будь-якому користувачу виконувати будь-які інші контрольовані КЗЗ дії) від деякого зовнішнього джерела з використанням захищеного механізму автентифікованого ідентифікатора цього користувача.

Примітка. У випадку позитивної відповіді на п. А.15.3 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Ідентифікація та автентифікація" рівня НИ-1, її політика може бути уточнена при відповіді на запитання п. А.15.4.

А.15.4 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.15.3), реалізовані засоби одержання від зовнішнього джерела (вкажіть якого) автентифікованого ідентифікатора користувача. Який порядок функціонування цих засобів, які механізми використовуються для захисту переданих ідентифікаторів.

А.15.5 Чи існує можливість з використанням засобів, реалізованих у

функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), установлення, за результатами виконання перевірки дійсності з використанням відповідних механізмів (автентифікації), однозначної відповідності між користувачем і унікальним ідентифікатором, яким користувач представляється в ОЕ.

Примітка. Функціонування механізмів, що забезпечують виконання автентифікації користувачів, може ґрунтуватися на одному з таких принципів:

- принцип "знання чогось" (наприклад, паролів або криптографічних ключів);

- принцип "володіння чимось" (карткою з магнітною смугою, смарт-карткою, переносним ідентифікатором тощо);

- принцип "притаманність невід'ємних характеристик" (рукописний підпис, відбиток пальця, голосові характеристики, характеристики сітківки ока, динамічні характеристики при роботі з клавіатурою тощо).

Якщо засобів, що реалізують механізми, які функціонують на підставі зазначених принципів, у складі КЗЗ немає, то це означає, що послуга "Ідентифікація та автентифікація" рівня НИ-2 чи НИ-3 засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.15.6-А.15.9 не потрібно. Якщо ж такі засоби існують, то це означає, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація" рівня НИ-2 чи НИ-3, остаточно факт її реалізації і політика можуть бути уточнені при відповіді на запитання п. А.15.6-А.15.9.

А.15.6 Чи використовуються в наведених при відповіді на п. А.15.5 засобах автентифікації, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ, у процесі виконання перевірки дійсності (автентифікації) користувача:

А.15.6.1 механізми різного типу (вкажіть якого), тобто такі, що функціонують на підставі різних принципів;

А.15.6.2 механізми лише одного типу (вкажіть якого), тобто такі, що функціонують на підставі однакових принципів.

Примітка. У випадку позитивної відповіді на п. А.15.6.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація" рівня НИ-3. У випадку негативної відповіді на п. А.15.6.1 і позитивної відповіді на п. А.15.6.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація" рівня НИ-2.

А.15.7 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.15.5), реалізовані засоби перевірки дійсності (автентифікації) користувачів з використанням кожного з механізмів автентифікації, наведених при відповіді на п. А.15.6. Які атрибути користувачів, наведені при відповіді на п. А.2.1.3, при цьому використовуються. Наведіть опис протоколу виконання автентифікації та структуру наборів даних автентифікації, використовуваних при цьому, для кожного з механізмів автентифікації, наведених при відповіді на п. А.15.6.

А.15.8 Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), захисту даних автентифікації, наведених при відповіді на п. А.15.7, від несанкціонованого доступу з метою перегляду, модифікації, руйнування для кожного з використовуваних механізмів автентифікації.

Примітка. У випадку позитивної відповіді на п. А.15.8 можна стверджувати, що засобами КЗЗ ОЕ може бути реалізована послуга "Ідентифікація та автентифікація" рівня НИ-2 чи НИ-3. У випадку негативної відповіді на п. А.15.9 можна стверджувати, що послуга "Ідентифікація та автентифікація" рівня НИ-2 чи НИ-3 засобами КЗЗ не реалізується і відповідати на запитання п. А.15.9 не потрібно.

А.15.9 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані засоби захисту даних автентифікації, наведених при відповіді на п. А.15.8, від несанкціонованого доступу з метою перегляду, модифікації, руйнування для кожного з використовуваних механізмів автентифікації. З використанням яких саме механізмів реалізується захист даних автентифікації від несанкціонованого доступу з метою перегляду, модифікації, руйнування. Який порядок функціонування цих механізмів.

А.16 Достовірний канал

Послуга "Достовірний канал" дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Відповіді на наведені в розділі А.16 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.16.1 Чи існує в ОЕ можливість створення захищеного шляху передачі інформації між користувачем і функціональними компонентами ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), який не може бути імітований, а інформація, що передається по ньому, не може бути отримана або модифікована стороннім користувачем або процесом (достовірного каналу).

Примітка. Зазначена можливість, ініційована користувачем, повинна забезпечувати захист від шкідливих програмних засобів типу "троянський кінь". Якщо зазначеної можливості в ОЕ не існує, то це означає, що послуга "Достовірний канал" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.16.2-А.16.6 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Достовірний канал", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання
п. А.16.2-А.16.6.

А.16.2 Чи використовується створюваний засобами ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.16.1), достовірний канал:

А.16.2.1 лише при виконанні початкової ідентифікації та автентифікації користувачів різних типів (укажіть яких);

А.16.2.2 при виконанні початкової ідентифікації та автентифікації користувачів різних типів (укажіть яких) та в інших випадках (укажіть в яких), коли необхідна безпосередня взаємодія користувача із засобами КЗЗ.

Примітка. У випадку позитивної відповіді на п. А.16.2.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Достовірний канал" рівня НК-1. У випадку позитивної відповіді на п. А.16.2.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Достовірний канал" рівня НК-2.

А.16.3 Чи ініціюється зв'язок з використанням достовірного каналу при виконанні операцій, наведених при відповіді на п. А.16.2.1, А.16.2.2:

А.16.3.1 лише користувачем;

А.16.3.2 як користувачем, так і засобами КЗЗ.

Примітка. У випадку позитивної відповіді на п. А.16.3.1 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Достовірний канал" рівня НК-1. У випадку позитивної відповіді на п. А.16.2.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Достовірний канал" рівня НК-2.

А.16.4 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані засоби створення достовірного каналу, використовуваного для початкової ідентифікації та автентифікації користувача (з урахуванням відповідей на п. А.16.2.1, А.16.3.1). З використанням яких саме механізмів реалізується створення достовірного каналу, використовуваного для початкової ідентифікації та автентифікації користувача, які атрибути користувачів (з урахуванням відповіді на п. А.2.1.3) і властивості компонентів КЗЗ при цьому використовуються. Наведіть протокол установлення достовірного каналу, використовуваного для початкової ідентифікації та автентифікації користувача, і опис порядку передачі інформації з використанням цього каналу.

А.16.5 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані засоби створення достовірного каналу, використовуваного з метою, відмінною від початкової ідентифікації та автентифікації користувача (з урахуванням відповідей на п. А.16.2.2, А.16.3.2). З використанням яких саме механізмів реалізується створення достовірного каналу, використовуваного з метою, відмінною від початкової ідентифікації та автентифікації користувача, які атрибути користувачів (з урахуванням відповіді на п. А.2.1.3) і властивості компонентів КЗЗ при цьому використовуються. Наведіть протокол установлення достовірного каналу, використовуваного з метою, відмінною від початкової ідентифікації та автентифікації користувача, і опис порядку обміну інформації з використанням цього каналу (для всіх випадків його використання).

А.16.6 Чи забезпечує наведений при відповіді на п. А.16.5 протокол можливість однозначної ідентифікації факту обміну з використанням

достовірного каналу, ініційованого засобами КЗЗ, а також можливість початку обміну лише після позитивного підтвердження користувачем готовності до обміну. Яким чином забезпечується ця можливість.

Примітка. У випадку позитивної відповіді на п. А.16.6 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Достовірний канал" рівня НК-2.

А.17 Розмежування обов'язків

Послуга "Розмежування обов'язків" дозволяє зменшити потенційний збиток від навмисних або помилкових дій користувачів і обмежити авторитарність керування. Відповіді на наведені в розділі А.17 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, визначити політику, засоби та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.17.1 Чи існує серед переліку ролей користувачів, підтримуваних у ОЕ та наведених при відповіді на п. А.2.2.1, хоча б одна роль, яка передбачає можливість виконання користувачем операцій з адміністрування і керування будь-якими засобами, що входять до складу КЗЗ (з урахуванням відповіді на п. А.2.1.1).

Примітка. Якщо серед переліку ролей, підтримуваних в ОЕ, ролі, які передбачають можливість виконання користувачем операцій з адміністрування і керування будь-якими засобами, що входять до складу КЗЗ, відсутні, то це означає, що послуга "Розмежування обов'язків" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.17.2-А.17.7 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Розмежування обов'язків" рівнів НО-1, НО-2 чи НО-3, факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.17.2-А.17.7.

А.17.2 Наведіть (з урахуванням відповіді на п. А.2.1.1) перелік адміністративних ролей (ролей користувачів, які мають можливість виконання операцій з адміністрування і керування будь-якими засобами, що входять до складу КЗЗ) і ролей звичайних користувачів (ролей користувачів, які не мають можливості виконання операцій з керування будь-якими засобами, що входять до складу КЗЗ).

А.17.3 Чи існує серед переліку адміністративних ролей користувачів, підтримуваних у ОЕ та наведених при відповіді на п. А.17.2, одна чи декілька ролей. Наведіть перелік функцій, притаманних різним адміністративним ролям.

Примітка. У випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є декілька адміністративних ролей, то це означає, що засобами КЗЗ може бути реалізована послуга "Розмежування обов'язків" рівня НО-2 чи НО-3. У протилежному випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є лише одна адміністративна роль, то це означає, що засобами КЗЗ може бути реалізована послуга "Розмежування обов'язків" рівня НО-1.

А.17.4 Чи існує серед переліку ролей звичайних користувачів,

підтримуваних в ОЕ та наведених при відповіді на п. А.17.2, одна чи декілька ролей. Наведіть перелік функцій, притаманних різним ролям звичайних користувачів.

Примітка. У випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є декілька ролей звичайних користувачів, то це означає, що засобами КЗЗ може бути реалізована послуга "Розмежування обов'язків" рівня НО-3. У протилежному випадку, якщо серед переліку ролей, підтримуваних в ОЕ, є лише одна роль користувача, то це означає, що засобами КЗЗ може бути реалізована послуга "Розмежування обов'язків" рівня НО-1 чи НО-2.

А.17.5 На підставі яких атрибутів доступу об'єктів-користувачів (з урахуванням відповідей на п. А.2.1.2, А.2.1.3) і згідно з якими правилами здійснюється призначення користувачів на ролі, наведені при відповіді на п. А.17.3, А.17.4.

А.17.6 В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), підтримується призначення користувачів на ролі, наведені при відповіді на п. А.17.3, А.17.4, на підставі атрибутів, наведених при відповіді на п. А.17.5.

А.17.7 Які дії при роботі з різними функціональними модулями ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), повинен виконати користувач для підтвердження прийняття ним певної ролі (для всіх ролей, наведених при відповіді на п. А.17.3, А.17.4).

А.18 Цілісність комплексу засобів захисту

Послуга "Цілісність комплексу засобів захисту" визначає міру здатності КЗЗ захищати себе і гарантувати свою здатність керувати захищеними об'єктами. Відповіді на наведені в розділі А.18 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.18.1 Чи існують в ОЕ можливість і відповідні засоби захисту всіх функціональних модулів, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), від несприятливих зовнішніх впливів, метою яких є порушення цілісності компонентів КЗЗ.

Примітка. Під захистом цілісності компонентів КЗЗ слід розуміти або виявлення фактів порушення цілісності компонентів з подальшим її відновленням, або запобігання самій можливості порушення цілісності компонентів КЗЗ. Функціонування механізмів, що забезпечують реалізацію послуги "Цілісність комплексу засобів захисту", в частині, яка стосується виявлення фактів порушення цілісності компонентів КЗЗ, може ґрунтуватися на одному з таких принципів:

- виявлення порушень цілісності шляхом порівняння із заздалегідь створеною еталонною копією;

- виявлення порушень цілісності шляхом вироблення/перевірки криптографічних (таких, що обчислюються з використанням ключових даних) кодів контролю цілісності (кодів автентифікації повідомлень);

- виявлення порушень цілісності шляхом вироблення/перевірки некриптографічних кодів контролю цілісності з їх подальшим зашифруванням/розшифруваннням;

- виявлення порушень цілісності шляхом вироблення/перевірки електронного цифрового підпису.

Функціонування механізмів, що забезпечують реалізацію послуги "Цілісність комплексу засобів захисту", в частині, яка стосується запобігання самій можливості порушення цілісності компонентів КЗЗ, може ґрунтуватися на одному з таких принципів:

- з використанням механізму керування доступом для захисту компонентів КЗЗ, що знаходяться у стані зберігання;

- на підставі апаратно реалізованих засобів обмеження доступної різним процесам оперативної пам'яті (кільця захисту, захищені сегменти пам'яті, захищені комірки пам'яті) для захисту компонентів КЗЗ, що знаходяться у стані виконання.

Якщо зазначеної можливості та відповідних засобів в ОЕ не існує, то це означає, що послуга "Цілісність комплексу засобів захисту" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.18.2-А.18.11 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Цілісність комплексу засобів захисту", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.18.2-А.18.11.

А.18.2 Чи існує можливість забезпечення з використанням засобів, наведених при відповіді на п. А.18.1, контролю цілісності (виявлення фактів порушення цілісності) всіх функціональних модулів ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.1.2.1, А.1.2.2.

Примітка. У випадку позитивної відповіді на п. А.18.2 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність комплексу засобів захисту" рівня НЦ-1, політика послуги може бути уточнена при відповіді на запитання п. А.18.3-А.18.6, А.18.10. Якщо такі засоби відсутні, то відповідати на запитання п. А.18.3-А.18.6 не потрібно, можна переходити до відповіді на запитання п. А.18.7.

А.18.3 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.18.1, реалізовані засоби контролю цілісності (виявлення фактів порушення цілісності) всіх функціональних модулів ОЕ, що входять до складу КЗЗ та наведені при відповіді на п. А.1.2.1, А.1.2.2. Який порядок функціонування цих засобів, які механізми використовуються для виявлення фактів порушення цілісності різних функціональних модулів ОЕ, що входять до складу КЗЗ.

А.18.4 Чи існує можливість забезпечення з використанням засобів,

реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), оповіщення адміністратора про виявлені факти порушення цілісності компонентів КЗЗ. У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані ці засоби. Який порядок функціонування цих засобів, які механізми використовуються для оповіщення адміністратора про виявлені факти порушення цілісності компонентів КЗЗ.

Примітка. У випадку позитивної відповіді на п. А.18.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність комплексу засобів захисту" рівня НЦ-1, політика послуги може бути уточнена при відповіді на запитання п. А.18.5-А.18.6, А.18.10.

А.18.5 Чи існує можливість забезпечення з використанням засобів, реалізованих у функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), автоматичного відновлення відповідності компонентів КЗЗ з порушеною цілісністю еталону або переведення ОЕ у випадку виявлення порушення цілісності будь-якого з компонентів КЗЗ у стан з припиненням обслуговування, з якого повернути його до нормального функціонування зможуть лише користувачі, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністратори або користувачі, яким надані відповідні повноваження). У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), реалізовані ці засоби. Який порядок функціонування цих засобів.

Примітка. У випадку позитивної відповіді на п. А.18.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність комплексу засобів захисту" рівня НЦ-1.

А.18.6 На підставі яких атрибутів доступу об'єктів-користувачів, наведених при відповіді на п. А.2.1.3, що визначають їх приналежність до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), і згідно з якими правилами здійснюється оброблення запитів на повернення ОЕ зі стану з припиненням обслуговування, в який він був переведений після виявлення порушення цілісності компонентів КЗЗ, до нормального функціонування (з урахуванням відповіді на п. А.18.5).

А.18.7 Чи існує можливість забезпечення з використанням засобів, наведених при відповіді на п. А.18.1, розподілу домену КЗЗ та інших доменів шляхом виділення для збереження і виконання функціональних модулів ОЕ, що входять до складу КЗЗ, ізольованої логічної області всередині ОЕ з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

Примітка. У випадку позитивної відповіді на п. А.18.7 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність комплексу засобів захисту" рівня НЦ-2 чи НЦ-3.

А.18.8 На підставі яких атрибутів компонентів КЗЗ і відповідних процесів (як пасивних об'єктів у стані зберігання та об'єктів-процесів у стані виконання, з урахуванням відповідей на п. А.2.2.3, А.2.3.3) реалізується виділення домену КЗЗ з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

А.18.9 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.18.1, реалізовані засоби виділення домену КЗЗ з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування на підставі атрибутів, наведених при відповіді на п. А.18.8. Який порядок функціонування цих засобів, які механізми використовуються для виділення домену КЗЗ з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

А.18.10 Наведіть опис обмежень, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

А.18.11 Чи забезпечують реалізовані у складі КЗЗ засоби і механізми виділення домену КЗЗ з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування, наведені при відповіді на п. А.18.9, гарантію того, що всі послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Наведіть обґрунтування цього твердження.

Примітка. У випадку позитивної відповіді на п. А.18.11 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Цілісність комплексу засобів захисту" рівня НЦ-3.

А.19 Самотестування

Послуга "Самотестування" дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ОЕ. Відповіді на наведені в розділі А.19 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги, визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.19.1 Чи існують в ОЕ можливість і відповідні засоби перевірки (з використанням певних процедур) правильності функціонування компонентів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), при виконанні певних операцій.

Примітка. Якщо зазначеної можливості і відповідних засобів в ОЕ не існує, то це означає, що послуга "Самотестування" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.19.2-А.19.7 не потрібно. Якщо ж така можливість існує, то це означає, що засобами КЗЗ може бути реалізована послуга "Самотестування", факт її реалізації, політика і рівень можуть бути уточнені при відповіді на запитання п. А.19.2-А.19.7.

А.19.2 Наведіть перелік властивостей ОЕ та процедур, реалізованих у

функціональних компонентах ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), які можуть бути використані для оцінювання правильності функціонування КЗЗ.

А.19.3 Наведіть перелік тестів (у вигляді опису перевірок і очікуваних результатів), використовуваних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, при виконанні різних операцій (з урахуванням відповіді на п. А.19.2).

А.19.4 Чи існує можливість виконання тестів, використовуваних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, за запитами користувачів, що відносяться до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів або користувачів, яким надані відповідні повноваження).

Примітка. У випадку позитивної відповіді на п. А.19.4 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Самотестування" рівнів НТ-1, НТ-2 чи НТ-3. У випадку негативної відповіді на п. А.19.4 можна стверджувати, що послуга "Самотестування" засобами КЗЗ не реалізується і відповідати на запитання п. А.19.5-А.19.7 не потрібно.

А.19.5 На підставі яких атрибутів доступу об'єктів-користувачів, що визначають їх приналежність до певних ролей, наведених при відповіді на п. А.2.1.1 (адміністраторів або користувачів, яким надані відповідні повноваження), в яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), і згідно з якими правилами здійснюється оброблення запитів на виконання тестування різних функціональних компонентів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.19.2, А.19.3, А.19.4).

А.19.6 Чи існує можливість виконання тестів, використовуваних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, при старті ОЕ. В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), і згідно з якими правилами здійснюється виконання тестів, використовуваних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.19.2, А.19.3), при старті ОЕ.

Примітка. У випадку позитивної відповіді на п. А.19.6 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Самотестування" рівня НТ-2 чи НТ-3.

А.19.7 Чи існує можливість виконання тестів, використовуваних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, у процесі штатного функціонування ОЕ. В яких функціональних модулях ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), і згідно з якими правилами здійснюється виконання тестів,

використовуваних для оцінювання правильності функціонування різних функціональних компонентів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.19.2, А.19.3), у процесі штатного функціонування ОЕ.

Примітка. У випадку позитивної відповіді на п. А.19.7 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Самотестування" рівня НТ-3.

А.20 Ідентифікація та автентифікація при обміні

Послуга "Ідентифікація та автентифікація при обміні" дозволяє КЗЗ (компонентам КЗЗ) установити і перевірити ідентичність іншого КЗЗ (компонента КЗЗ) перед початком або у процесі взаємодії. Відповіді на наведені в розділі А.20 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.20.1 Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними компонентами ОЕ через незахищене середовище пасивними об'єктами будь-якого з типів, наведених при відповіді на запитання п. А.2.3.1. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об'єктів.

Примітка. У випадку позитивної відповіді на п. А.20.1 можна стверджувати, що в ОЕ може бути реалізована послуга "Ідентифікація та автентифікація при обміні" рівнів НВ-1, НВ-2 чи НВ-3. У цьому випадку факт реалізації послуги, її політика і рівень можуть бути уточнені при відповіді на запитання п. А.20.2-А.20.9. У випадку негативної відповіді на п. А.20.1 можна стверджувати, що послуга "Ідентифікація та автентифікація при обміні" в ОЕ не реалізується і відповідати на запитання п. А.20.2-А.20.9 не потрібно.

А.20.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми, що забезпечують виконання взаємної ідентифікації та автентифікації різних КЗЗ (компонентів КЗЗ) перед ініціалізацією (початком) обміну даними з іншим КЗЗ (компонентом КЗЗ).

Примітка. Функціонування засобів, що забезпечують реалізацію послуги "Ідентифікація та автентифікація при обміні", повинно обов'язково передбачати виконання таких дій:

- одержання інформації автентифікації, необхідної для генерації/перевірки запитів автентифікації сторонами взаємодії (ініціатором і верифікатором);
- генерація і передача запитів автентифікації стороною-ініціатором;
- перевірка та оброблення запитів автентифікації стороною-верифікатором.

При цьому функціонування механізмів, що реалізують послугу, може

ґрунтуватися на одному з таких принципів:

- знання загального секрету;
- підтвердження довіреною третьою стороною;
- контекст запиту автентифікації.

Якщо засобів, що реалізують механізми, які функціонують на підставі зазначених принципів, у складі КЗЗ немає, то це означає, що послуга "Ідентифікація та автентифікація при обміні" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.20.3-А.20.9 не потрібно. Якщо ж такі засоби існують, то це означає, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація при обміні" рівнів НВ-1, НВ-2 чи НВ-3, остаточно факт її реалізації, рівень і політика можуть бути уточнені при відповіді на запитання п. А.20.3-А.20.9.

А.20.3 З використанням яких атрибутів КЗЗ (компонентів КЗЗ), наведених при відповіді на п. А.2.2.3, виконується взаємна ідентифікація та автентифікація різних КЗЗ (компонентів КЗЗ) перед ініціалізацією (початком) обміну даними з іншим КЗЗ (компонентом КЗЗ).

А.20.4 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.20.2), з використанням яких саме механізмів реалізовані засоби виконання взаємної ідентифікації та автентифікації різних КЗЗ (компонентів КЗЗ) перед ініціалізацією (початком) обміну даними з іншим КЗЗ (компонентом КЗЗ) із застосуванням наведених при відповіді на п. А.20.3 атрибутів. Наведіть опис протоколу виконання автентифікації та структуру наборів даних автентифікації, що використовуються при цьому.

А.20.5 Чи існує можливість забезпечення, з використанням засобів, наведених при відповіді на п. А.20.4, встановлення джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта кожного з наведених при відповіді на п. А.20.1 типу.

Примітка. У випадку позитивної відповіді на п. А.20.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація при обміні" рівня НВ-2 чи НВ-3.

А.20.6 З використанням яких атрибутів переданих пасивних об'єктів, наведених при відповіді на п. А.2.3.3, а також КЗЗ (компонентів КЗЗ), наведених при відповіді на п. А.2.2.3, реалізується зазначена при відповіді на п. А.20.5 можливість установлення джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта кожного типу.

А.20.7 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.20.2), з використанням яких саме механізмів реалізовані засоби встановлення джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта при обміні даними з іншим КЗЗ (компонентом КЗЗ) з використанням наведених при відповіді на п. А.20.6 атрибутів. Наведіть опис протоколу встановлення джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта при обміні даними з іншим КЗЗ (компонентом КЗЗ) і структуру наборів даних, що

використовуються при цьому.

А.20.8 Чи існує можливість забезпечення, з використанням засобів і протоколів, наведених при відповіді на п. А.20.7, однозначного підтвердження джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта незалежною третьою стороною.

Примітка. У випадку позитивної відповіді на п. А.20.8 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Ідентифікація та автентифікація при обміні" рівня НВ-3.

А.20.9 З використанням яких атрибутів переданих пасивних об'єктів і КЗЗ (компонентів КЗЗ), наведених при відповіді на п. А.20.6, реалізується зазначена при відповіді на п. А.20.8 можливість однозначного підтвердження джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта незалежною третьою стороною. Наведіть опис протоколу підтвердження джерела кожного експортованого (переданого) та імпортованого (прийнятого) об'єкта незалежною третьою стороною і структуру наборів даних, що використовуються при цьому.

А.21 Автентифікація відправника

Послуга "Автентифікація відправника" дозволяє однозначно встановити приналежність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений цим користувачем. Відповіді на наведені в розділі А.21 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.21.1 Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними користувачами через незахищене середовище пасивними об'єктами будь-якого з типів, наведених при відповіді на запитання п. А.2.3.1. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об'єктів.

Примітка. У випадку позитивної відповіді на п. А.21.1 можна стверджувати, що в ОЕ може бути реалізована послуга "Автентифікація відправника" рівня НА-1 чи НА-2. У цьому випадку факт реалізації послуги, її політика і рівень можуть бути уточнені при відповіді на запитання п. А.21.2-А.21.6. У випадку негативної відповіді на п. А.21.1 можна стверджувати, що послуга "Автентифікація відправника" в ОЕ не реалізується і відповідати на запитання п. А.21.2-А.21.6 не потрібно.

А.21.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми, що забезпечують можливість однозначно встановити приналежність певного об'єкта певного типу (з урахуванням відповіді на п. А.21.1) певному користувачу, тобто той факт, що об'єкт був створений або відправлений цим користувачем.

Примітка. Функціонування засобів, що забезпечують реалізацію послуги "Автентифікація відправника", повинно обов'язково передбачати виконання таких дій:

- генерація підтверджень авторства (маркерів причетності), однозначно пов'язаних з переданими об'єктами (повідомленнями);
- передача і збереження підтверджень авторства (маркерів причетності);
- перевірка підтверджень авторства (маркерів причетності).

При цьому обов'язковим є застосування механізмів, заснованих на використанні криптографічних перетворень. Використовуваний вигляд підтверджень (маркерів причетності) визначається типом використовуваних криптографічних алгоритмів і містить:

- захищені конверти повідомлень, у процесі генерації та перевірки яких використовуються симетричні криптографічні алгоритми;
- електронні цифрові підписи повідомлень, у процесі генерації та перевірки яких використовуються несиметричні криптографічні алгоритми.

Якщо засобів, що реалізують механізми, які функціонують на підставі зазначених принципів, у складі КЗЗ немає, то це означає, що послуга "Автентифікація відправника" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.21.3-А.21.6 не потрібно. Якщо ж такі засоби існують, то це означає, що засобами КЗЗ може бути реалізована послуга "Автентифікація відправника" рівня НА-1 чи НА-2, остаточно її рівень і політика можуть бути уточнені при відповіді на запитання п. А.21.3-А.21.6.

А.21.3 З використанням яких атрибутів користувачів (з урахуванням відповіді на п. А.2.1.3), переданих пасивних об'єктів (з урахуванням відповіді на п. А.2.3.3) та інтерфейсних процесів (з урахуванням відповіді на п. А.2.2.3) виконується зазначене при відповіді на п. А.21.1 встановлення приналежності певного об'єкта певного типу певному користувачу.

А.21.4 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.21.2), з використанням яких саме механізмів реалізовані засоби встановлення приналежності певного об'єкта певному користувачу з використанням наведених при відповіді на п. А.21.3 атрибутів. Наведіть опис протоколу виконання встановлення приналежності певного об'єкта певному користувачу і структуру наборів даних, що використовуються при цьому.

А.21.5 Чи існує можливість забезпечення, з використанням засобів і протоколів, наведених при відповіді на п. А.21.4, однозначного підтвердження приналежності певного об'єкта певного типу певному користувачу незалежною третьою стороною.

Примітка. У випадку позитивної відповіді на п. А.21.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Автентифікація відправника" рівня НА-2.

А.21.6 З використанням яких атрибутів користувачів, переданих пасивних

об'єктів і інтерфейсних процесів, наведених при відповіді на п. А.21.3, реалізується зазначена при відповіді на п. А.21.5 можливість однозначного підтвердження приналежності певного об'єкта певного типу певному користувачу незалежною третьою стороною. Наведіть опис протоколу підтвердження приналежності об'єкта певному користувачу незалежною третьою стороною і структуру наборів даних, що використовуються при цьому.

А.22 Автентифікація одержувача

Послуга "Автентифікація одержувача" дозволяє однозначно установити факт одержання певного об'єкта певним користувачем. Відповіді на наведені в розділі А.22 Додатка А запитання повинні допомогти експерту з'ясувати факт реалізації в ОЕ цієї послуги і перелік об'єктів різного типу, стосовно яких визначено її політику. Сформульовані відповіді дозволять експерту визначити політику, засоби, механізми та особливості реалізації послуги, а також одержати вхідні дані для розроблення програми і методики випробувань цієї послуги.

А.22.1 Чи існує в ОЕ можливість обміну (з використанням відповідних інтерфейсних процесів) між різними користувачами через незахищене середовище пасивними об'єктами будь-якого з типів, наведених при відповіді на запитання п. А.2.3.1. Якщо така можливість існує, то наведіть цю підмножину типів пасивних об'єктів.

Примітка. У випадку позитивної відповіді на п. А.22.1 можна стверджувати, що в ОЕ може бути реалізована послуга "Автентифікація одержувача" рівня НП-1 чи НП-2. У цьому випадку факт реалізації послуги, її політика і рівень можуть бути уточнені при відповіді на запитання п. А.22.2-А.22.6. У випадку негативної відповіді на п. А.22.1 можна стверджувати, що послуга "Автентифікація одержувача" в ОЕ не реалізується і відповідати на запитання п. А.22.2-А.22.6 не потрібно.

А.22.2 Чи існують у складі будь-яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповідей на п. А.1.2.1, А.1.2.2), засоби і відповідні механізми, що забезпечують можливість однозначно установити факт одержання певного об'єкта певного типу (з урахуванням відповіді на п. А.22.1) певним користувачем.

Примітка. Функціонування засобів, що забезпечують реалізацію послуги "Автентифікація одержувача", повинно обов'язково передбачати виконання таких дій:

- генерація підтверджень одержання (маркерів причетності), однозначно пов'язаних з отриманими об'єктами (повідомленнями);
- передача і збереження підтверджень одержання (маркерів причетності);
- перевірка підтверджень одержання (маркерів причетності).

При цьому обов'язковим є застосування механізмів, заснованих на використанні криптографічних перетворень. Використовуваний вигляд підтверджень (маркерів причетності) визначається типом використовуваних криптографічних алгоритмів і містить:

- захищені конверти повідомлень про одержання, у процесі генерації та перевірки яких використовуються симетричні криптографічні алгоритми;

- електронні цифрові підписи повідомлень про одержання, у процесі генерації та перевірки яких використовуються несиметричні криптографічні алгоритми.

Якщо засобів, що реалізують механізми, які функціонують на підставі зазначених принципів, у складі КЗЗ немає, то це означає, що послуга "Автентифікація одержувача" засобами КЗЗ ОЕ не реалізується і відповідати на запитання п. А.22.3-А.22.6 не потрібно. Якщо ж такі засоби існують, то це означає, що засобами КЗЗ може бути реалізована послуга "Автентифікація одержувача" рівня НП-1 чи НП-2, остаточно її рівень і політика можуть бути уточнені при відповіді на запитання п. А.22.3-А.22.6.

А.22.3 З використанням яких атрибутів користувачів (з урахуванням відповіді на п. А.2.1.3), переданих пасивних об'єктів (з урахуванням відповіді на п. А.2.3.3) та інтерфейсних процесів (з урахуванням відповіді на п. А.2.2.3) виконується зазначене при відповіді на п. А.22.1 встановлення факту одержання певного об'єкта певного типу певним користувачем.

А.22.4 У складі яких функціональних модулів ОЕ, що входять до складу КЗЗ (з урахуванням відповіді на п. А.22.2), з використанням яких саме механізмів реалізовані засоби встановлення факту одержання певного об'єкта певного типу певним користувачем з використанням наведених при відповіді на п. А.22.3 атрибутів. Наведіть опис протоколу виконання встановлення факту одержання певного об'єкта певним користувачем і структуру наборів даних, що використовуються при цьому.

А.22.5 Чи існує можливість забезпечення, з використанням засобів і протоколів, наведених при відповіді на п. А.22.4, однозначного підтвердження факту одержання певного об'єкта певного типу певним користувачем незалежною третьою стороною.

Примітка. У випадку позитивної відповіді на п. А.22.5 можна стверджувати, що засобами КЗЗ може бути реалізована послуга "Автентифікація відправника" рівня НП-2.

А.22.6 З використанням яких атрибутів користувачів, переданих пасивних об'єктів і інтерфейсних процесів, наведених при відповіді на п. А.22.3, реалізується зазначена при відповіді на п. А.22.5 можливість однозначного підтвердження факту одержання певного об'єкта певного типу певним користувачем незалежною третьою стороною. Наведіть опис протоколу підтвердження факту одержання певного об'єкта певним користувачем незалежною третьою стороною і структуру наборів даних, що використовуються при цьому.

Додаток Б
Вимоги щодо змісту програми випробувань функціональних послуг безпеки різних типів і різних рівнів
(рекомендований)

У Додатку Б викладені специфічні вимоги щодо змісту програми випробувань функціональних послуг безпеки різних типів і різних рівнів. Вимоги викладені з урахуванням вимог НД ТЗІ 2.5-004-99 до політики функціональних послуг безпеки різних типів і різних рівнів, а також з урахуванням результатів ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики, отриманих експертом з використанням переліку спеціальних запитань, наведених у Додатку А.

Б.1 Вимоги до програми випробувань функціональної послуги безпеки "Довірча конфіденційність"

Б.1.1 Вимоги до програми випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-1 – "Мінімальна довірча конфіденційність"

Програма випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-1 має передбачати перевірку таких вимог:

Б.1.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.2.

Б.1.1.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.1, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.1.1.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8.

Б.1.1.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів, процесів та об'єктів різного типу, наведених при відповіді на п. А.3.5.1, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретні процеси та/або групи процесів, що мають право одержувати інформацію від об'єкта.

Б.1.1.5 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.1.1.6 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.1.1.7 Атрибути користувачів різного типу, які ініціюють запити з метою

зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.1.2 Вимоги до програми випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-2 – "Базова довірча конфіденційність"

Програма випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-2 має передбачати перевірку таких вимог:

Б.1.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.2.

Б.1.2.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.2, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.1.2.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8.

Б.1.2.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретних користувачів та/або групи користувачів, що мають право одержувати інформацію від об'єкта.

Б.1.2.5 КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Б.1.2.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.1.2.7 Як частина політики послуги представлені правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.1.2.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.1.3 Вимоги до програми випробувань функціональної послуги

безпеки "Довірча конфіденційність" рівня КД-3 – "Повна довірча конфіденційність"

Програма випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-3 має передбачати перевірку таких вимог:

Б.1.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.1.

Б.1.3.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.2, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.1.3.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8.

Б.1.3.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретних користувачів (і групи користувачів), що мають, а також тих, що не мають права одержувати інформацію від об'єкта.

Б.1.3.5 КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретних користувачів (і групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.1.3.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.1.3.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.1.3.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.1.3.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.1.4 Вимоги до програми випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-4 – "Абсолютна довірча

конфіденційність"

Програма випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-4 має передбачати перевірку таких вимог:

Б.1.4.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.1.

Б.1.4.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів, процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.2, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.1.4.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8.

Б.1.4.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів, процесів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають, а також тих, що не мають права одержувати інформацію від об'єкта.

Б.1.4.5 КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.1.4.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.1.4.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.1.4.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.1.4.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.2 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна конфіденційність"

Б.2.1 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-1 – "Мінімальна адміністративна конфіденційність"

Програма випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-1 має передбачати перевірку таких вимог:

Б.2.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.2.

Б.2.1.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.1, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.2.1.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.2.1.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів, процесів та об'єктів різного типу, наведених при відповіді на п. А.3.5.1, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю процесів та об'єктів до відповідних доменів визначити конкретні процеси та/або групи процесів, що мають право одержувати інформацію від об'єкта.

Б.2.1.5 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.2.1.6 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.2.1.7 Атрибути користувачів різного типу, які ініціюють запити з метою зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.2.2 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-2 – "Базова адміністративна конфіденційність"

Програма випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-2 має передбачати перевірку таких вимог:

Б.2.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.2.

Б.2.2.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів

доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.2, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.2.2.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.2.2.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю користувачів, процесів та об'єктів до відповідних доменів визначити конкретних користувачів та/або групи користувачів, що мають право одержувати інформацію від об'єкта.

Б.2.2.5 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Б.2.2.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.2.2.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.2.2.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.2.3 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-3 – "Повна адміністративна конфіденційність"

Програма випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-3 має передбачати перевірку таких вимог:

Б.2.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.1.

Б.2.3.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при

відповіді на п. А.3.5.2, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.2.3.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.2.3.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю користувачів, процесів та об'єктів до відповідних доменів визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права одержувати інформацію від об'єкта.

Б.2.3.5 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.2.3.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.2.3.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.2.3.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.2.3.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.2.4 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-4 – "Абсолютна адміністративна конфіденційність"

Програма випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-4 має передбачати перевірку таких вимог:

Б.2.4.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.3.4.1.

Б.2.4.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів, процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.3.5.2, за правилами, наведеними при відповіді на п. А.3.5, з використанням засобів, наведених при відповіді на п. А.3.6.

Б.2.4.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.3.7, з використанням засобів, наведених при відповіді на п. А.3.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.2.4.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів, процесів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю користувачів, процесів та об'єктів до відповідних доменів визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають, а також тих, що не мають права одержувати інформацію від об'єкта.

Б.2.4.5 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів, процесів та об'єктів різного типу, наведених при відповіді на п. А.3.5.2, А.3.7, а також засобів, наведених при відповіді на п. А.3.8, шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.2.4.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.3.11 для об'єктів різного типу.

Б.2.4.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.3.12, А.3.13.

Б.2.4.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.2.4.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.3 Вимоги до програми випробувань функціональної послуги безпеки "Повторне використання об'єктів"

Б.3.1 Вимоги до програми випробувань функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1

Програма випробувань функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 має передбачати перевірку таких вимог:

Б.3.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситися до всіх поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, зазначених при відповіді на п. А.4.2.

Б.3.1.2 Перш ніж користувач або процес зможе одержати у своє розпорядження звільнений іншим користувачем або процесом об'єкт певного типу, встановлені для попереднього користувача або процесу права доступу до цього об'єкта скасовуються з використанням механізмів, наведених при відповіді на п. А.4.3.

Б.3.1.3 Перш ніж користувач або процес зможе одержати у своє розпорядження звільнений іншим користувачем або процесом об'єкт певного типу, вся інформація, що міститься в цьому об'єкті, з використанням механізмів, наведених при відповіді на п. А.4.4, робиться недоступною.

Б.4 Вимоги до програми випробувань функціональної послуги безпеки "Аналіз прихованих каналів"

Б.4.1 Вимоги до програми випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-1 – "Виявлення прихованих каналів"

Програма випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-1 має передбачати перевірку таких вимог:

Б.4.1.1 Виконано аналіз прихованих каналів, відповідні результати наведені при відповіді на п. А.5.1.

Б.4.1.2 Усі приховані канали, що існують в апаратному і програмному забезпеченні, а також у програмах ПЗП, документовані, відповідні результати наведені при відповіді на п. А.5.2.

Б.4.1.3 Документовано максимальну пропускну здатність кожного виявленого прихованого каналу, отриману на підставі теоретичної оцінки або вимірів, відповідні результати наведені при відповіді на п. А.5.4.

Б.4.1.4 Для прихованих каналів, що можуть використовуватися спільно, документовано сукупну пропускну здатність, відповідні результати наведені при відповіді на п. А.5.4.

Б.4.1.5 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, послуга "Повторне використання об'єктів" рівня КО-1 реалізується стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для яких визначені політики послуг довірчої та/або адміністративної конфіденційності.

Б.4.1.6 Проектування і реалізація ОЕ виконувалися з дотриманням вимог НД ТЗІ 2.5-004-99 до рівня гарантій коректності реалізації функціональних послуг безпеки не нижче, ніж Г-3.

Б.4.2 Вимоги до програми випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-2 – "Контроль прихованих каналів"

Програма випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-2 має передбачати перевірку таких вимог:

Б.4.2.1 Виконано аналіз прихованих каналів, відповідні результати наведені при відповіді на п. А.5.1.

Б.4.2.2 Усі приховані канали, що існують в апаратному і програмному забезпеченні, а також у програмах ПЗП, документовані, відповідні результати наведені при відповіді на п. А.5.2.

Б.4.2.3 Документовано максимальну пропускну здатність кожного виявленого прихованого каналу, отриману на підставі теоретичної оцінки або вимірів, відповідні результати наведені при відповіді на п. А.5.4.

Б.4.2.4 Для прихованих каналів, що можуть використовуватися спільно, документовано сукупну пропускну здатність, відповідні результати наведені при відповіді на п. А.5.4.

Б.4.2.5 КЗЗ ОЕ, згідно з переліком реєстраційних подій, наведеним при відповіді на п. А.14.2-А.14.4, забезпечує реєстрацію фактів використання затвердженої підмножини виявлених прихованих каналів за допомогою засобів реалізації послуги "Реєстрація" рівня НР-1 або вище з використанням засобів і механізмів, наведених при відповіді на п. А.5.5.

Б.4.2.6 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, послуга "Повторне використання об'єктів" рівня КО-1 реалізується стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для яких визначені політики послуг довірчої та/або адміністративної конфіденційності.

Б.4.2.7 Проектування і реалізація ОЕ виконувалися з дотриманням вимог НД ТЗІ 2.5-004-99 до рівня гарантій коректності реалізації функціональних послуг безпеки не нижче, ніж Г-3.

Б.4.3 Вимоги до програми випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-3 – "Перекриття прихованих каналів"

Програма випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-3 має передбачати перевірку таких вимог:

Б.4.3.1 Виконано аналіз прихованих каналів, відповідні результати наведені при відповіді на п. А.5.1.

Б.4.3.2 Затверджену підмножину виявлених при аналізі прихованих каналів, наведену при відповіді на п. А.5.2, усунуто з використанням засобів і механізмів, наведених при відповіді на п. А.5.3.

Б.4.3.3 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, послуга "Повторне використання об'єктів" рівня КО-1 реалізується

стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для яких визначені політики послуг довірчої та/або адміністративної конфіденційності.

Б.4.3.4 Проектування і реалізація ОЕ виконувалися з дотриманням вимоги НД ТЗІ 2.5-004-99 до рівня гарантій коректності реалізації функціональних послуг безпеки не нижче, ніж Г-3.

Б.5 Вимоги до програми випробувань функціональної послуги безпеки "Конфіденційність при обміні"

Б.5.1 Вимоги до програми випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-1 – "Мінімальна конфіденційність при обміні"

Програма випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-1 має передбачати перевірку таких вимог:

Б.5.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.2.

Б.5.1.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, зазначений при відповіді на п. А.6.4, який забезпечується використовуваними механізмами.

Б.5.1.3 КЗЗ ОЕ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4.

Б.5.2 Вимоги до програми випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-2 – "Базова конфіденційність при обміні"

Програма випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-2 має передбачати перевірку таких вимог:

Б.5.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.2.

Б.5.2.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на п. А.6.4, який забезпечується використовуваними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно з правилами, наведеними при відповіді на п. А.6.4.

Б.5.2.3 КЗЗ ОЕ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4.

Б.5.2.4 Запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.6.4, за правилами, наведеними при відповіді на п. А.6.5, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних

ролей згідно з політикою реалізованої КЗЗ ОЕ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.5.2.5 Запити на експорт захищеного об'єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.6.2.

Б.5.2.6 Запити на імпорт захищеного об'єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.7.2.

Б.5.3 Вимоги до програми випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-3 – "Повна конфіденційність при обміні"

Програма випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-3 має передбачати перевірку таких вимог:

Б.5.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.1.

Б.5.3.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на п. А.6.4, який забезпечується використовуваними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно з правилами, наведеними при відповіді на п. А.6.4.

Б.5.3.3 КЗЗ ОЕ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4.

Б.5.3.4 Запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.6.4, за правилами, наведеними при відповіді на п. А.6.5, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ ОЕ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.5.3.5 Запити на експорт захищеного об'єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.6.1, і атрибутів приймача об'єкта, наведених при відповіді на п. А.6.6.1 і автентифікованих з використанням засобів реалізації послуги "Ідентифікація та автентифікація при обміні" рівня НВ-1 або вище згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.20.2-20.4.

Б.5.3.6 Запити на імпорт захищеного об'єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу,

наведених при відповіді на п. А.6.7.1, та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1 і автентифікованих з використанням засобів реалізації послуги "Ідентифікація та автентифікація при обміні" рівня НВ-1 або вище згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.20.2-20.4.

Б.5.3.7 Подання захищеного об'єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об'єкта, а також його джерела і приймача згідно з описом, наведеним при відповіді на п. А.6.8.

Б.5.4 Вимоги до програми випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-4 – "Абсолютна конфіденційність при обміні"

Програма випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-4 має передбачати перевірку таких вимог:

Б.5.4.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.1.

Б.5.4.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на п. А.6.4, який забезпечується використовуваними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно з правилами, наведеними при відповіді на п. А.6.4.

Б.5.4.3 КЗЗ ОЕ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4.

Б.5.4.4 Запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.6.4, за правилами, наведеними при відповіді на п. А.6.5, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ ОЕ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.5.4.5 Запити на експорт захищеного об'єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.6.1, і атрибутів приймача об'єкта, наведених при відповіді на п. А.6.6.1 і автентифікованих з використанням засобів реалізації послуги "Ідентифікація та автентифікація при обміні" рівня НВ-1 або вище згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.20.2-20.4.

Б.5.4.6 Запити на імпорт захищеного об'єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.7.1, і атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1 і автентифікованих з використанням засобів

реалізації послуги "Ідентифікація та автентифікація при обміні" рівня НВ-1 або вище згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.20.2-20.4.

Б.5.4.7 Подання захищеного об'єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об'єкта, а також його джерела і приймача, згідно з описом, наведеним при відповіді на п. А.6.8.

Б.5.4.8 Політика послуги містить опис інформації, яку можна одержати шляхом спільного аналізу ряду отриманих об'єктів певного типу, результати, наведені при відповіді на п. А.6.9, містять цей опис.

Б.5.4.9 Виконано аналіз прихованих каналів обміну, всі виявлені приховані канали обміну і максимальна пропускна здатність кожного з них документовані, дані, наведені при відповіді на п. А.6.9, А.6.10, А.6.11, містять результати виконаного аналізу.

Б.5.4.10 КЗЗ ОЕ, згідно з переліком реєстраційних подій, наведеним при відповіді на п. А.14.2-А.14.4, забезпечує реєстрацію фактів використання затвердженої підмножини виявлених прихованих каналів, наведеної при відповіді на п. А.6.12, за допомогою засобів реалізації послуги "Реєстрація" рівня НР-1 або вище з використанням засобів і механізмів, наведених при відповіді на п. А.6.12.

Б.5.4.11 Забезпечено часткове перекриття або виключення множини виявлених прихованих каналів обміну, наведеної при відповіді на п. А.6.9, з використанням засобів і механізмів, наведених при відповіді на п. А.6.13.

Б.5.4.12 Проектування і реалізація ОЕ виконувалися з дотриманням вимог НД ТЗІ 2.5-004-99 до рівня гарантій коректності реалізації функціональних послуг безпеки не нижче, ніж Г-3.

Б.6 Вимоги до програми випробувань функціональної послуги безпеки "Довірча цілісність"

Б.6.1 Вимоги до програми випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-1 – "Мінімальна довірча цілісність"

Програма випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-1 має передбачати перевірку таких вимог:

Б.6.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.2.

Б.6.1.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.1, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.6.1.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного

типу за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8.

Б.6.1.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів та об'єктів різного типу, наведених при відповіді на п. А.7.5.1, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів та/або групи користувачів, що мають право модифікувати об'єкт.

Б.6.1.5 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.6.1.6 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.6.1.7 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.6.2 Вимоги до програми випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-2 – "Базова довірча цілісність"

Програма випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-2 має передбачати перевірку таких вимог:

Б.6.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.2.

Б.6.2.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.2, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.6.2.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8.

Б.6.2.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу процесів та об'єктів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретні процеси та/або групи процесів, що мають право модифікувати об'єкт.

Б.6.2.5 КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і

процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Б.6.2.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.6.2.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.6.2.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.6.3 Вимоги до програми випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-3 – "Повна довірча цілісність"

Програма випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-3 має передбачати перевірку таких вимог:

Б.6.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.1.

Б.6.3.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.2, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.6.3.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8.

Б.6.3.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу процесів та об'єктів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретні процеси (групи процесів), що мають, а також тих, що не мають права модифікувати об'єкт.

Б.6.3.5 КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.6.3.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.6.3.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.6.3.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.6.3.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.6.4 Вимоги до програми випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-4 – "Абсолютна довірча цілісність"

Програма випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-4 має передбачати перевірку таких вимог:

Б.6.4.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.1.

Б.6.4.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів, користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.2, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.6.4.3 Запити на зміну прав доступу до об'єкта обробляються КЗЗ ОЕ на підставі атрибутів доступу користувачів, які ініціюють запит, та об'єктів різного типу за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8.

Б.6.4.4 КЗЗ ОЕ надає користувачу можливість для захищеного об'єкта кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають, а також тих, що не мають права модифікувати об'єкт.

Б.6.4.5 КЗЗ ОЕ надає користувачу можливість для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.6.4.6 Права доступу до кожного захищеного об'єкта встановлюються в

момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.6.4.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.6.4.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.6.4.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.7 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна цілісність"

Б.7.1 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-1 – "Мінімальна адміністративна цілісність"

Програма випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-1 має передбачати перевірку таких вимог:

Б.7.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.2.

Б.7.1.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.1, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.7.1.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.7.1.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів та об'єктів різного типу, наведених при відповіді на п. А.7.5.1, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів та/або групи користувачів, що мають право модифікувати об'єкт.

Б.7.1.5 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.7.1.6 Як частина політики послуги подані правила збереження атрибутів

доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.7.1.7 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.7.2 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-2 – "Базова адміністративна цілісність"

Програма випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-2 має передбачати перевірку таких вимог:

Б.7.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.2.

Б.7.2.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.2, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.7.2.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.7.2.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу процесів та об'єктів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретні процеси та/або групи процесів, що мають право модифікувати об'єкт.

Б.7.2.5 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, що належить його домену, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів та/або групи користувачів, що мають право ініціювати процес.

Б.7.2.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.7.2.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді

на п. А.7.12, А.7.13.

Б.7.2.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.7.3 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-3 – "Повна адміністративна цілісність"

Програма випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-3 має передбачати перевірку таких вимог:

Б.7.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.1.

Б.7.3.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.2, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.7.3.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.7.3.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу процесів та об'єктів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретні процеси та/або групи процесів, що мають право модифікувати об'єкт.

Б.7.3.5 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.7.3.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.7.3.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.7.3.8 Атрибути користувачів різного типу, які ініціюють запити з метою

доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.7.3.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.7.4 Вимоги до програми випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-4 – "Абсолютна адміністративна цілісність"

Програма випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-4 має передбачати перевірку таких вимог:

Б.7.4.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.7.4.1.

Б.7.4.2 КЗЗ ОЕ здійснює розмежування доступу на підставі атрибутів доступу процесів, користувачів і захищених об'єктів різного типу, наведених при відповіді на п. А.7.5.2, за правилами, наведеними при відповіді на п. А.7.5, з використанням засобів, наведених при відповіді на п. А.7.6.

Б.7.4.3 Запити на зміну прав доступу обробляються КЗЗ ОЕ за правилами, наведеними при відповіді на п. А.7.7, з використанням засобів, наведених при відповіді на п. А.7.8, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.7.4.4 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для захищеного об'єкта кожного типу, з використанням атрибутів доступу користувачів, процесів та об'єктів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів і процеси (групи користувачів і процесів), що мають право модифікувати об'єкт.

Б.7.4.5 КЗЗ ОЕ надає можливість адміністратору або користувачу, що має відповідні повноваження, для процесу кожного типу, з використанням атрибутів доступу користувачів і процесів різного типу, наведених при відповіді на п. А.7.5.2, А.7.7, а також засобів, наведених при відповіді на п. А.7.8, визначити конкретних користувачів (групи користувачів), що мають, а також тих, що не мають права ініціювати процес.

Б.7.4.6 Права доступу до кожного захищеного об'єкта встановлюються в момент його створення або ініціалізації за правилами, наведеними при відповіді на п. А.7.11 для об'єктів різного типу.

Б.7.4.7 Як частина політики послуги подані правила збереження атрибутів доступу об'єктів різного типу при їх експорті та імпорті, наведені при відповіді на п. А.7.12, А.7.13.

Б.7.4.8 Атрибути користувачів різного типу, які ініціюють запити з метою доступу до об'єкта, запуску процесу або зміни прав доступу до об'єкта, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.7.4.9 Згідно з політикою і правилами, наведеними при відповіді на п. А.4.2-А.4.4, стосовно поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, реалізується послуга "Повторне використання об'єктів" рівня КО-1.

Б.8 Вимоги до програми випробувань функціональної послуги безпеки "Відкат"

Б.8.1 Вимоги до програми випробувань функціональної послуги безпеки "Відкат" рівня ЦО-1 – "Обмежений відкат"

Програма випробувань функціональної послуги безпеки "Відкат" рівня ЦО-1 має передбачати перевірку таких вимог:

Б.8.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.8.2.

Б.8.1.2 Існують автоматизовані засоби, що дозволяють авторизованому користувачу, атрибути якого автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2, або процесу "відкатити" чи скасувати певний набір (множину) операцій, виконаних над захищеним об'єктом певного типу за певний проміжок часу, з використанням засобів, механізмів і правил, наведених при відповіді на п. А.8.3, А.8.4.2.

Б.8.2 Вимоги до програми випробувань функціональної послуги безпеки "Відкат" рівня ЦО-2 – "Повний відкат"

Програма випробувань функціональної послуги безпеки "Відкат" рівня ЦО-2 має передбачати перевірку таких вимог:

Б.8.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А.8.2.

Б.8.2.2 Існують автоматизовані засоби, що дозволяють авторизованому користувачу, атрибути якого автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2, або процесу "відкатити" чи скасувати всі операції, виконані над захищеним об'єктом певного типу за певний проміжок часу, з використанням засобів, механізмів і правил, наведених при відповіді на п. А.8.3, А.8.4.1.

Б.9 Вимоги до програми випробувань функціональної послуги безпеки

"Цілісність при обміні"

Б.9.1 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-1 – "Мінімальна цілісність при обміні"

Програма випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-1 має передбачати перевірку таких вимог:

Б.9.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3.

Б.9.1.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на п. А.9.4, який забезпечується використовуваними механізмами.

Б.9.1.3 КЗЗ ОЕ забезпечує можливість виявлення порушення цілісності інформації, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.1, А.9.4.

Б.9.2 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-2 – "Базова цілісність при обміні"

Програма випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-2 має передбачати перевірку таких вимог:

Б.9.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3.

Б.9.2.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на п. А.9.4, А.9.5, який забезпечується використовуваними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно з правилами, наведеними при відповіді на п. А.9.4, А.9.5.

Б.9.2.3 КЗЗ ОЕ забезпечує можливість виявлення порушення цілісності інформації, що міститься в переданих об'єктах різного типу, а також фактів їх видалення або дублювання, з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.1, А.9.2.2, А.9.4, А.9.5.

Б.9.2.4 Запити на експорт захищеного об'єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.9.4, А.9.5, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.9.7.2.

Б.9.2.5 Запити на імпорт захищеного об'єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.9.4, А.9.5, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.9.8.2.

Б.9.2.6 Запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.9.4, А.9.5, за правилами, наведеними при відповіді на п. А.9.6, лише в тому випадку, якщо вони

надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.9.3 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-3 – "Повна цілісність при обміні"

Програма випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-3 має передбачати перевірку таких вимог:

Б.9.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів та існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3.

Б.9.3.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає рівень захищеності, наведений при відповіді на п. А.9.4, А.9.5, який забезпечується використовуваними механізмами, і здатність користувачів та/або процесів керувати рівнем захищеності згідно з правилами, наведеними при відповіді на п. А.9.4, А.9.5.

Б.9.3.3 КЗЗ ОЕ забезпечує можливість виявлення порушення цілісності інформації, що міститься в переданих об'єктах різного типу, а також фактів їх видалення або дублювання, з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.1, А.9.2.2, А.9.4, А.9.5.

Б.9.3.4 Запити на експорт захищеного об'єкта певного типу обробляються передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.9.4, А.9.5, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.9.7.1, та атрибутів приймача об'єкта, наведених при відповіді на п. А.9.7.1 і автентифікованих з використанням засобів реалізації послуги "Ідентифікація та автентифікація при обміні" рівня НВ-1 або вище згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.20.2-20.4.

Б.9.3.5 Запити на імпорт захищеного об'єкта певного типу обробляються приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.9.4, А.9.5, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.9.8.1, та атрибутів джерела об'єкта, наведених при відповіді на п. А.9.8.1 і автентифікованих з використанням засобів реалізації послуги "Ідентифікація та автентифікація при обміні" рівня НВ-1 або вище згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.20.2-20.4.

Б.9.3.6 Запити на присвоєння або зміну рівня захищеності обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.9.4, А.9.5, за правилами, наведеними при відповіді на п. А.9.6, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.9.3.7 Подання захищеного об'єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об'єкта, а також його джерела і приймача згідно з описом, наведеним при відповіді на п. А.9.9.

Б.10 Вимоги до програми випробувань функціональної послуги безпеки "Використання ресурсів"

Б.10.1 Вимоги до програми випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-1 – "Квоти"

Програма випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-1 має передбачати перевірку таких вимог:

Б.10.1.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А10.2.2.

Б.10.1.2 Політика послуги визначає обмеження, наведені при відповіді на п. А.10.3, А.10.4.2, які можна накладати на кількість об'єктів (обсяг ресурсів) певного типу, що виділяються окремому користувачу.

Б.10.1.3 Запити на зміну встановлених обмежень обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.10.6, за правилами, наведеними при відповіді на п. А.10.7, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.10.1.4 КЗЗ ОЕ забезпечує можливість контролю за дотриманням встановлених обмежень з боку окремого користувача з використанням засобів, механізмів і правил, наведених при відповіді на п. А.10.5.

Б.10.2 Вимоги до програми випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-2 – "Недопущення захоплення ресурсів"

Програма випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-2 має передбачати перевірку таких вимог:

Б.10.2.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А10.2.1.

Б.10.2.2 Політика послуги визначає обмеження, наведені при відповіді на п. А.10.3, А.10.4.2, які можна накладати на кількість об'єктів (обсяг ресурсів) певного типу, що виділяються окремому користувачу.

Б.10.2.3 Запити на зміну встановлених обмежень обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.10.6, за правилами, наведеними при відповіді на п. А.10.7, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.10.2.4 Існує можливість у засобах, наведених при відповіді на п. А.10.6, за правилами, наведеними при відповіді на п. А.10.9, встановлювати обмеження

таким чином, щоб КЗЗ ОЕ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ ОЕ або захищених об'єктів.

Б.10.2.5 КЗЗ ОЕ забезпечує можливість контролю за дотриманням встановлених обмежень з боку окремого користувача з використанням засобів, механізмів і правил, наведених при відповіді на п. А.10.5.

Б.10.3 Вимоги до програми випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-3 – "Пріоритетність використання ресурсів"

Програма випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-3 має передбачати перевірку таких вимог:

Б.10.3.1 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до об'єктів ОЕ всіх типів, наведених при відповіді на п. А10.2.1.

Б.10.3.2 Політика послуги визначає обмеження, наведені при відповіді на п. А.10.3, А.10.4.1, які можна накладати на кількість об'єктів (обсяг ресурсів) певного типу, що виділяються окремому користувачу і довільним групам користувачів.

Б.10.3.3 Запити на зміну встановлених обмежень обробляються КЗЗ ОЕ у засобах, наведених при відповіді на п. А.10.6, за правилами, наведеними при відповіді на п. А.10.7, лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.10.3.4 Існує можливість у засобах, наведених при відповіді на п. А.10.6, за правилами, наведеними при відповіді на п. А.10.9, встановлювати обмеження таким чином, щоб КЗЗ ОЕ мав можливість запобігти діям, що можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ ОЕ або захищених об'єктів.

Б.10.3.5 КЗЗ ОЕ забезпечує можливість контролю за дотриманням встановлених обмежень з боку окремого користувача і довільних груп користувачів з використанням засобів, механізмів і правил, наведених при відповіді на п. А.10.5.

Б.11 Вимоги до програми випробувань функціональної послуги безпеки "Стійкість до відмов"

Б.11.1 Вимоги до програми випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-1 – "Стійкість при обмежених відмовах"

Програма випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-1 має передбачати перевірку таких вимог:

Б.11.1.1 Розробником проведено аналіз відмов компонентів ОЕ, відповідні результати наведені при відповіді на п. А.11.2.

Б.11.1.2 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину

компонентів ОЕ, до яких вона відноситься, наведену при відповіді на п. А.11.3.2, і типи їх відмов, наведені при відповіді на п. А.11.2, після яких ОЕ в стані продовжувати функціонування.

Б.11.1.3 В результатах аналізу, наведених при відповіді на п. А.11.2, чітко вказані рівні відмов різних компонентів ОЕ, наведених при відповіді на п. А.11.3.2, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

Б.11.1.4 Відмова одного захищеного компонента з наведених при відповіді на
п. А.11.3.2 не призводить до недоступності всіх послуг, а в гіршому випадку проявляється в зниженні характеристик обслуговування, наведених при відповіді на п. А.11.4.2.

Б.11.1.5 КЗЗ ОЕ здатний, з використанням засобів і механізмів, наведених при відповіді на п. А.11.5, повідомляти про відмову будь-якого захищеного компонента адміністратора, який відноситься до певної ролі згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.11.2 Вимоги до програми випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-2 – "Стійкість з погіршенням характеристик обслуговування"

Програма випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-2 має передбачати перевірку таких вимог:

Б.11.2.1 Розробником проведено аналіз відмов компонентів ОЕ, відповідні результати наведені при відповіді на п. А.11.2.

Б.11.2.2 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до всіх компонентів ОЕ, наведених при відповіді на п. А.11.3.1, і визначає типи їх відмов, наведені при відповіді на п. А.11.2, після яких ОЕ в стані продовжувати функціонування.

Б.11.2.3 У результатах аналізу, наведених при відповіді на п. А.11.2, чітко вказані рівні відмов різних компонентів ОЕ, наведених при відповіді на п. А.11.3.1, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

Б.11.2.4 Відмова одного захищеного компонента з наведених при відповіді на
п. А.11.3.1 не призводить до недоступності всіх послуг, а в гіршому випадку проявляється в зниженні характеристик обслуговування, наведених при відповіді на п. А.11.4.2.

Б.11.2.5 КЗЗ ОЕ здатний, з використанням засобів і механізмів, наведених при відповіді на п. А.11.5, повідомляти про відмову будь-якого захищеного компонента адміністратора, який відноситься до певної ролі згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.11.3 Вимоги до програми випробувань функціональної послуги

безпеки "Стійкість до відмов" рівня ДС-3 – "Стійкість без погіршення характеристик обслуговування"

Програма випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-3 має передбачати перевірку таких вимог:

Б.11.3.1 Розробником проведено аналіз відмов компонентів ОЕ, відповідні результати наведені при відповіді на п. А.11.2.

Б.11.3.2 Політика послуги, що реалізується КЗЗ ОЕ, відноситься до всіх компонентів ОЕ, наведених при відповіді на п. А.11.3.1, і визначає типи їх відмов, наведені при відповіді на п. А.11.2, після яких ОЕ в стані продовжувати функціонування.

Б.11.3.3 У результатах аналізу, наведених при відповіді на п. А.11.2, чітко вказані рівні відмов різних компонентів ОЕ, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

Б.11.3.4 Відмова одного захищеного компонента не призводить до недоступності всіх послуг або до зниження характеристик обслуговування.

Б.11.3.5 КЗЗ ОЕ здатний, з використанням засобів і механізмів, наведених при відповіді на п. А.11.5, повідомляти про відмову будь-якого захищеного компонента адміністратора, який відноситься до певної ролі згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.12 Вимоги до програми випробувань функціональної послуги безпеки "Гаряча заміна"

Б.12.1 Вимоги до програми випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-1 – "Модернізація"

Програма випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-1 має передбачати перевірку таких вимог:

Б.12.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає політику проведення модернізації певної множини компонентів ОЕ, що входять до складу КЗЗ ОЕ, наведену при відповіді на п. А.12.2.2, А.12.3.

Б.12.1.2 Адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають можливість провести модернізацію (upgrade) відповідних компонентів ОЕ, що входять до складу КЗЗ ОЕ, з використанням засобів і за правилами, наведеними при відповіді на п. А.12.2.2, А.12.3, А12.5, що не призводить до необхідності заново робити інсталяцію ОЕ або до переривання виконання КЗЗ ОЕ функцій захисту.

Б.12.2 Вимоги до програми випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-2 – "Обмежена гаряча заміна"

Програма випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-2 має передбачати перевірку таких вимог:

Б.12.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину

компонентів ОЕ, що входять до складу КЗЗ ОЕ, які можуть бути замінені без переривання обслуговування, наведену при відповіді на п. А.12.4.2.

Б.12.2.2 Стосовно компонентів ОЕ, що входять до складу КЗЗ ОЕ та можуть бути замінені без переривання обслуговування, наведених при відповіді на п. А.12.4.2, згідно з політикою, наведеною при відповіді на п. А.11.2, А.11.3, реалізовано послугу "Стійкість до відмов" рівня ДС-1 або вище.

Б.12.2.3 Адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають можливість замінити будь-який захищений компонент ОЕ, що входить до складу КЗЗ ОЕ, з використанням засобів і за правилами, наведеними при відповіді на п. А.12.2, А.12.3, А12.5.

Б.12.3 Вимоги до програми випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-3 – "Гаряча заміна будь-якого компонента"

Програма випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-3 має передбачати перевірку таких вимог:

Б.12.3.1 Політика послуги, що реалізується КЗЗ ОЕ, забезпечує можливість заміни будь-якого компонента ОЕ, що входить до складу КЗЗ ОЕ, наведеного при відповіді на п. А.12.4.1, без переривання обслуговування.

Б.12.3.2 Стосовно компонентів ОЕ, що входять до складу КЗЗ ОЕ та можуть бути замінені без переривання обслуговування, наведених при відповіді на п. А.12.4.1, згідно з політикою, наведеною при відповіді на п. А.11.2, А.11.3, реалізовано послугу "Стійкість до відмов" рівня ДС-1 або вище.

Б.12.3.3 Адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають можливість замінити будь-який захищений компонент ОЕ, що входить до складу КЗЗ ОЕ, з використанням засобів і за правилами, наведеними при відповіді на п. А.12.2, А.12.3, А12.5.

Б.13 Вимоги до програми випробувань функціональної послуги безпеки "Відновлення після збоїв"

Б.13.1 Вимоги до програми випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-1 – "Ручне відновлення"

Програма випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-1 має передбачати перевірку таких вимог:

Б.13.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину типів відмов ОЕ та переривань обслуговування, наведену при відповіді на п. А.13.2, після яких можливе повернення у відомий захищений стан без порушення політики безпеки, чітко вказані рівні відмов різних компонентів ОЕ,

що входять до складу КЗЗ ОЕ, при перевищенні яких необхідна повторна інсталяція ОЕ.

Б.13.1.2 Після відмови ОЕ або переривання обслуговування КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на п. А.13.3, А.13.10, перевести ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.13.1.3 Існують ручні процедури, що дозволяють з використанням засобів, наведених при відповіді на п. А.13.8, з використанням атрибутів і за правилами, наведеними при відповіді на п. А.13.10, безпечним чином повернути ОЕ зі стану з припиненням обслуговування до нормального функціонування.

Б.13.2 Вимоги до програми випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-2 – "Автоматизоване відновлення"

Програма випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-2 має передбачати перевірку таких вимог:

Б.13.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину типів відмов ОЕ та переривань обслуговування, наведену при відповіді на п. А.13.2, після яких можливе повернення у відомий захищений стан без порушення політики безпеки, чітко вказані рівні відмов різних компонентів ОЕ, що входять до складу КЗЗ ОЕ, при перевищенні яких необхідна повторна інсталяція ОЕ.

Б.13.2.2 Після відмови ОЕ або переривання обслуговування певного типу КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на п. А.13.4, визначити, чи можуть бути використані автоматизовані процедури для повернення ОЕ до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ ОЕ здатний виконати їх та з використанням засобів і за правилами, наведеними при відповіді на п. А.13.6, повернути ОЕ до нормального функціонування.

Б.13.2.3 Якщо автоматизовані процедури не можуть бути використані, КЗЗ ОЕ здатний з використанням засобів і за правилами, наведеними при відповіді на п. А.13.7, перевести ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.13.2.4 Існують ручні процедури, що дозволяють з використанням засобів, наведених при відповіді на п. А.13.8, атрибутів і за правилами, наведеними при відповіді на п. А.13.10, безпечним чином повернути ОЕ зі стану з припиненням обслуговування до нормального функціонування.

Б.13.3 Вимоги до програми випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-3 – "Вибіркове відновлення"

Програма випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-3 має передбачати перевірку таких вимог:

Б.13.3.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину типів відмов ОЕ та переривань обслуговування, наведену при відповіді на п. А.13.2, після яких можливе повернення у відомий захищений стан без порушення політики безпеки, чітко вказані рівні відмов різних компонентів ОЕ, при перевищенні яких необхідна повторна інсталяція ОЕ.

Б.13.3.2 Після будь-якої відмови ОЕ або переривання обслуговування, що не призводять до необхідності заново інсталювати ОЕ, КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на п. А.13.4, А.13.5, А.13.6, виконати необхідні процедури і безпечним чином повернути ОЕ до нормального функціонування або, у гіршому випадку, до функціонування в режимі з погіршеними характеристиками обслуговування, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.13.3.3 Якщо автоматизовані процедури не можуть бути використані, КЗЗ ОЕ здатний з використанням засобів і за правилами, наведеними при відповіді на п. А.13.7, перевести ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.13.3.4 Існують ручні процедури, що дозволяють з використанням засобів, наведених при відповіді на п. А.13.8, А.13.9, атрибутів і за правилами, наведеними при відповіді на п. А.13.10, А.13.11, безпечним чином повернути ОЕ з режиму з погіршеними характеристиками обслуговування або стану з припиненням обслуговування до нормального функціонування.

Б.14. Вимоги до програми випробувань функціональної послуги безпеки "Реєстрація"

Б.14.1 Вимоги до програми випробувань функціональної послуги безпеки "Реєстрація" рівня НР-1 – "Зовнішній аналіз"

Програма випробувань функціональної послуги безпеки "Реєстрація" рівня НР-1 має передбачати перевірку таких вимог:

Б.14.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає перелік реєстраційних подій, наведений при відповіді на п. А.14.2.

Б.14.1.2 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.3, що мають безпосереднє відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.1.3 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події.

Б.14.1.4 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію, достатню для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Б.14.1.5 Атрибути користувачів різного типу, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.14.1.6 КЗЗ ОЕ здатний передавати журнал реєстрації в інші системи з використанням засобів і механізмів захисту, наведених при відповіді на п. А.14.8.

Б.14.2 Вимоги до програми випробувань функціональної послуги безпеки "Реєстрація" рівня НР-2 – "Захищений журнал"

Програма випробувань функціональної послуги безпеки "Реєстрація" рівня НР-2 має передбачати перевірку таких вимог:

Б.14.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає перелік реєстраційних подій, наведений при відповіді на п. А.14.2.

Б.14.2.2 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.3, що мають безпосереднє відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.2.3 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події.

Б.14.2.4 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію, достатню для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Б.14.2.5 Атрибути користувачів різного типу, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.14.2.6 КЗЗ ОЕ забезпечує захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на п. А.14.10.

Б.14.2.7 Адміністратори і користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають у своєму розпорядженні

засоби перегляду та аналізу журналу реєстрації, наведені при відповіді на п. А.14.12.

Б.14.3 Вимоги до програми випробувань функціональної послуги безпеки "Реєстрація" рівня НР-3 – "Сигналізація про небезпеку"

Програма випробувань функціональної послуги безпеки "Реєстрація" рівня НР-3 має передбачати перевірку таких вимог:

Б.14.3.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає перелік реєстраційних подій, наведений при відповіді на п. А.14.2.

Б.14.3.2 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.3, що мають безпосереднє відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.3.3 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події.

Б.14.3.4 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію, достатню для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Б.14.3.5 Атрибути користувачів різного типу, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.14.3.6 КЗЗ ОЕ забезпечує захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на п. А.14.10.

Б.14.3.7 Адміністратори і користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають у своєму розпорядженні засоби перегляду та аналізу журналу реєстрації, наведені при відповіді на п. А.14.12.

Б.14.3.8 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.14, контролювати одиничні або повторювані реєстраційні події, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ, наведені при відповіді на п. А.14.14.

Б.14.3.9 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.16, негайно інформувати адміністратора про перевищення порогів безпеки і за умови, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій.

Б.14.4 Вимоги до програми випробувань функціональної послуги безпеки "Реєстрація" рівня НР-4 – "Детальна реєстрація"

Програма випробувань функціональної послуги безпеки "Реєстрація" рівня НР-4 має передбачати перевірку таких вимог:

Б.14.4.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає перелік реєстраційних подій, наведений при відповіді на п. А.14.2.

Б.14.4.2 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.3, що мають безпосереднє відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.4.3 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.4, що мають непряме відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.4.4 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події.

Б.14.4.5 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.6, містить інформацію, достатню для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Б.14.4.6 Атрибути користувачів різного типу, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.14.4.7 КЗЗ ОЕ забезпечує захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на п. А.14.10.

Б.14.4.8 Адміністратори і користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають у своєму розпорядженні засоби перегляду та аналізу журналу реєстрації, наведені при відповіді на п. А.14.12.

Б.14.4.9 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.14, контролювати одиничні або повторювані реєстраційні події, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ, наведені при відповіді на п. А.14.14.

Б.14.4.10 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.16, негайно інформувати адміністратора про перевищення порогів безпеки і у разі, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії з припинення повторення цих подій.

Б.14.5 Вимоги до програми випробувань функціональної послуги безпеки "Реєстрація" рівня НР-5 – "Аналіз у реальному часі"

Програма випробувань функціональної послуги безпеки "Реєстрація" рівня НР-5 має передбачати перевірку таких вимог:

Б.14.5.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає перелік реєстраційних подій, наведений при відповіді на п. А.14.2.

Б.14.5.2 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.3, що мають безпосереднє відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.5.3 КЗЗ ОЕ здатний здійснювати реєстрацію подій, наведених при відповіді на п. А.14.4, що мають непряме відношення до безпеки, з використанням засобів, наведених при відповіді на п. А.14.5.

Б.14.5.4 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.5, містить інформацію про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події.

Б.14.5.5 Журнал реєстрації, згідно з описом структури його записів, наведеним при відповіді на п. А.14.5, містить інформацію, достатню для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Б.14.5.6 Атрибути користувачів різного типу, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.14.5.7 КЗЗ ОЕ забезпечує захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на п. А.14.10.

Б.14.5.8 Адміністратори і користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, мають у своєму розпорядженні засоби перегляду та аналізу журналу реєстрації, наведені при відповіді на п. А.14.12.

Б.14.5.9 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.14, контролювати одиничні або повторювані реєстраційні події, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ, наведені при відповіді на п. А.14.14.

Б.14.5.10 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.16, негайно інформувати адміністратора про перевищення порогів безпеки і у разі, якщо реєстраційні небезпечні події повторюються, здійснити

неруйнівні дії щодо припинення повторення цих подій.

Б.14.5.11 КЗЗ ОЕ здатний, з використанням засобів, наведених при відповіді на п. А.14.14, А.14.16, виявляти та аналізувати несанкціоновані дії в реальному часі.

Б.15 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація"

Б.15.1 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-1 – "Зовнішня ідентифікація та автентифікація"

Програма випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-1 має передбачати перевірку таких вимог:

Б.15.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає атрибути, якими характеризуються користувачі різного типу, наведені при відповіді на п. А.15.1, і послуги, для використання яких необхідні ці атрибути, наведені при відповіді на п. А.15.2.

Б.15.1.2 Кожен користувач кожного типу однозначно ідентифікується КЗЗ ОЕ на підставі атрибутів, наведених при відповіді на п. А.15.1.

Б.15.1.3 Перш ніж дозволити будь-якому користувачу будь-якого типу виконувати будь-які інші, контрольовані КЗЗ ОЕ дії, КЗЗ ОЕ здатний з використанням засобів і захищених механізмів, наведених при відповіді на п. А.15.4, одержати від зовнішнього джерела, наведеного при відповіді на п. А.15.4, автентифікований ідентифікатор цього користувача.

Б.15.2 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-2 – "Одиночна ідентифікація та автентифікація"

Програма випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-2 має передбачати перевірку таких вимог:

Б.15.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає атрибути, якими характеризуються користувачі різного типу, наведені при відповіді на п. А.15.1, і послуги, для використання яких необхідні ці атрибути, наведені при відповіді на п. А.15.2.

Б.15.2.2 Кожен користувач кожного типу однозначно ідентифікується КЗЗ ОЕ на підставі атрибутів, наведених при відповіді на п. А.15.1.

Б.15.2.3 Перш ніж дозволити будь-якому користувачу будь-якого типу виконувати будь-які інші, контрольовані КЗЗ ОЕ дії, КЗЗ ОЕ здатний автентифікувати цього користувача з використанням механізму і засобів, наведених при відповіді на п. А.15.6.2, А.15.7.

Б.15.2.4 КЗЗ ОЕ забезпечує захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування з використанням засобів і механізмів, наведених при відповіді на п. А.15.9.

Б.15.2.5 Взаємодія користувача будь-якого типу з КЗЗ ОЕ в процесі виконання автентифікації здійснюється з використанням засобів реалізації

послуги "Достовірний канал" рівня НК-1 або вище, які функціонують згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.16.2-А.16.4.

Б.15.3 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-3 – "Множинна ідентифікація та автентифікація"

Програма випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-3 має передбачати перевірку таких вимог:

Б.15.3.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає атрибути, якими характеризуються користувачі різного типу, наведені при відповіді на п. А.15.1, і послуги, для використання яких необхідні ці атрибути, наведені при відповіді на п. А.15.2.

Б.15.3.2 Кожен користувач кожного типу однозначно ідентифікується КЗЗ ОЕ на підставі атрибутів, наведених при відповіді на п. А.15.1.

Б.15.3.3 Перш ніж дозволити будь-якому користувачу будь-якого типу виконувати будь-які інші, контрольовані КЗЗ ОЕ дії, КЗЗ ОЕ здатний автентифікувати цього користувача з використанням засобів і механізмів декількох типів, наведених при відповіді на п. А.15.6.1, А.15.7.

Б.15.3.4 КЗЗ ОЕ забезпечує захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування з використанням механізмів і засобів, наведених при відповіді на п. А.15.9.

Б.15.3.5 Взаємодія користувача будь-якого типу з КЗЗ ОЕ в процесі виконання автентифікації за допомогою кожного з механізмів здійснюється з використанням засобів реалізації послуги "Достовірний канал" рівня НК-1 або вище, які функціонують згідно з політикою цієї послуги і правилами, наведеними при відповіді на п. А.16.2-А.16.4.

Б.16 Вимоги до програми випробувань функціональної послуги безпеки "Достовірний канал"

Б.16.1 Вимоги до програми випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-1 – "Однонаправлений достовірний канал"

Програма випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-1 має передбачати перевірку таких вимог:

Б.16.1.1 Політика послуги, реалізована КЗЗ ОЕ та наведена при відповіді на п. А.16.2-А.16.3, визначає механізми встановлення достовірного зв'язку між користувачем і КЗЗ ОЕ, наведені при відповіді на п. А.16.4.

Б.16.1.2 Достовірний канал використовуватися для початкової ідентифікації та автентифікації, зв'язок з використанням цього каналу ініціюється винятково користувачем з використанням засобів та протоколу, наведених при відповіді на п. А.16.4.

Б.16.2 Вимоги до програми випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-2 – "Двонаправлений достовірний

канал"

Програма випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-2 має передбачати перевірку таких вимог:

Б.16.2.1 Політика послуги, реалізована КЗЗ ОЕ та наведена при відповіді на п. А.16.2-А.16.3, визначає механізми встановлення достовірного зв'язку між користувачем і КЗЗ ОЕ, наведені при відповіді на п. А.16.4, А.16.5.

Б.16.2.2 Достовірний канал певного типу використовується для початкової ідентифікації та автентифікації, а також в інших випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач, зв'язок з використанням цього каналу ініціюється користувачем, з використанням засобів та протоколу, наведених при відповіді на п. А.16.4, або КЗЗ ОЕ, з використанням засобів та протоколу, наведених при відповіді на п. А.16.5.

Б.16.2.3 Обмін з використанням достовірного каналу, ініційований КЗЗ ОЕ, однозначно ідентифікований як такий, і може відбуватися лише після позитивного підтвердження готовності до обміну з боку користувача за правилами, наведеними при відповіді на п. А.16.6.

Б.17 Вимоги до програми випробувань функціональної послуги безпеки "Розмежування обов'язків"

Б.17.1 Вимоги до програми випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-1 – "Виділення адміністратора"

Програма випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-1 має передбачати перевірку таких вимог:

Б.17.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає ролі адміністратора та звичайного користувача, наведені при відповіді на п. А.17.2, і притаманні їм функції, наведені при відповіді на п. А.17.3, А.17.4.

Б.17.1.2 Засоби КЗЗ ОЕ, наведені при відповіді на п. А.17.6, підтримують призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на п. А.17.5.

Б.17.1.3 Користувачі при роботі із засобами КЗЗ ОЕ, наведеними при відповіді на п. А.17.6, мають можливість виступати у певній ролі лише після того, як вони виконають певні дії, наведені при відповіді на п. А17.7, що підтверджують прийняття ними цієї ролі.

Б.17.1.4 Перед виконанням призначення на роль атрибути користувачів автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.17.2 Вимоги до програми випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-2 – "Розмежування

обов'язків адміністраторів"

Програма випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-2 має передбачати перевірку таких вимог:

Б.17.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає ролі адміністраторів і звичайного користувача, наведені при відповіді на п. А.17.2, і притаманні їм функції, наведені при відповіді на п. А.17.3, А.17.4.

Б.17.2.2 Політика послуги визначає мінімум дві різні адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній з ролей та наведені при відповіді на п. А.17.3, мінімізовані так, щоб включати лише ті функції, що необхідні для виконання цієї ролі.

Б.17.2.3 Засоби КЗЗ ОЕ, наведені при відповіді на п. А.17.6, підтримують призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на п. А.17.5.

Б.17.2.4 Користувачі при роботі із засобами КЗЗ ОЕ, наведеними при відповіді на п. А.17.6, мають можливість виступати у певній ролі лише після того, як вони виконають певні дії, наведені при відповіді на п. А17.7, що підтверджують прийняття ними цієї ролі.

Б.17.2.5 Перед виконанням призначення на роль атрибути користувачів автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.17.3 Вимоги до програми випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-3 – "Розмежування обов'язків на підставі привілеїв"

Програма випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-3 має передбачати перевірку таких вимог:

Б.17.3.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає ролі адміністраторів і звичайних користувачів, наведені при відповіді на п. А.17.2, і притаманні їм функції, наведені при відповіді на п. А.17.3, А.17.4.

Б.17.3.2 Політика послуги визначає мінімум дві різні адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній з ролей та наведені при відповіді на п. А.17.3, мінімізовані так, щоб включати лише ті функції, що необхідні для виконання цієї ролі.

Б.17.3.3 Політика послуги визначає множину різних ролей користувачів, наведену при відповіді на п. А.17.2, А.17.4.

Б.17.3.4 Засоби КЗЗ ОЕ, наведені при відповіді на п. А.17.6, підтримують призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на п. А.17.5.

Б.17.3.5 Користувачі при роботі із засобами КЗЗ ОЕ, наведеними при відповіді на п. А.17.6, мають можливість виступати у певній ролі лише після того, як вони виконають певні дії, наведені при відповіді на п. А17.7, що підтверджують прийняття ними цієї ролі.

Б.17.3.6 Перед виконанням призначення на роль атрибути користувачів автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.18 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту"

Б.18.1 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-1 – "КЗЗ з контролем цілісності"

Програма випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-1 має передбачати перевірку таких вимог:

Б.18.1.1 Політика послуги визначає склад КЗЗ ОЕ та механізми контролю цілісності всіх компонентів, що входять до складу КЗЗ ОЕ, наведені при відповіді на п. А.18.2, А.18.3.

Б.18.1.2 У випадку виявлення засобами контролю цілісності, наведеними при відповіді на п. А.18.3, порушення цілісності будь-якого зі своїх компонентів, КЗЗ ОЕ, з використанням засобів, наведених при відповіді на п. А18.4, здатний зареєструвати факт порушення, за допомогою засобів реалізації послуги "Реєстрація" рівня НР-1 або вище повідомити адміністратора та з використанням засобів, наведених при відповіді на п. А18.5, або автоматично відновити відповідність компонента еталону, або перевести ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.18.1.3 Описані обмеження, наведені при відповіді на п. А.18.10, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Б.18.2 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-2 – "КЗЗ з гарантованою цілісністю"

Програма випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-2 має передбачати перевірку таких вимог:

Б.18.2.1 Політика послуги визначає домен КЗЗ ОЕ та інші домени, а також механізми захисту, що використовуються для реалізації розподілу доменів, наведені при відповіді на п. А.18.9.

Б.18.2.2 КЗЗ ОЕ з використанням атрибутів, наведених при відповіді на п. А.18.8, та засобів і механізмів, наведених при відповіді на п. А.18.9, підтримує домен для свого власного виконання з метою захисту всіх засобів КЗЗ від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

Б.18.2.3 Описані обмеження, наведені при відповіді на п. А.18.10,

дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Б.18.3 Вимоги до програми випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-3 – "КЗЗ з функціями диспетчера доступу"

Програма випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-3 має передбачати перевірку таких вимог:

Б.18.3.1 Політика послуги визначає домен КЗЗ ОЕ та інші домени, а також механізми захисту, що використовуються для реалізації розподілу доменів, наведені при відповіді на п. А.18.9.

Б.18.3.2 КЗЗ ОЕ з використанням атрибутів, наведених при відповіді на п. А.18.8, та засобів і механізмів, наведених при відповіді на п. А.18.9, підтримує домен для свого власного виконання з метою захисту всіх засобів КЗЗ від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування

Б.18.3.3 КЗЗ ОЕ з урахуванням правил, наведених при відповіді на п. А.18.11, гарантує, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Б.19 Вимоги до програми випробувань функціональної послуги безпеки "Самотестування"

Б.19.1 Вимоги до програми випробувань функціональної послуги безпеки "Самотестування" рівня НТ-1 – "Самотестування за запитом"

Програма випробувань функціональної послуги безпеки "Самотестування" рівня НТ-1 має передбачати перевірку таких вимог:

Б.19.1.1 Політика послуги, що реалізується КЗЗ ОЕ, описує властивості ОЕ та реалізовані процедури, наведені при відповіді на п. А.19.2, що можуть бути використані для оцінювання правильності функціонування КЗЗ.

Б.19.1.2 КЗЗ ОЕ здатний, з використанням засобів і згідно з правилами, наведеними при відповіді на п. А.19.5, виконувати наведений при відповіді на п.А.19.3 набір тестів з метою оцінювання правильності функціонування своїх критичних функцій за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.19.2 Вимоги до програми випробувань функціональної послуги безпеки "Самотестування" рівня НТ-2 – "Самотестування при старті"

Програма випробувань функціональної послуги безпеки "Самотестування" рівня НТ-2 має передбачати перевірку таких вимог:

Б.19.2.1 Політика послуги, що реалізується КЗЗ ОЕ, описує властивості ОЕ та реалізовані процедури, наведені при відповіді на п. А.19.2, що можуть бути використані для оцінювання правильності функціонування КЗЗ.

Б.19.2.2 КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на п. А.19.5, виконувати наведений при відповіді на п. А.19.3 набір тестів з метою оцінювання правильності функціонування своїх критичних функцій за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.19.2.3 КЗЗ ОЕ здатний при старті виконувати наведений при відповіді на п. А.19.3 набір тестів з метою оцінювання правильності функціонування своїх критичних функцій з використанням засобів і за правилами, наведеними при відповіді на п. А.19.6.

Б.19.3 Вимоги до програми випробувань функціональної послуги безпеки "Самотестування" рівня НТ-3 – "Самотестування в реальному часі"

Програма випробувань функціональної послуги безпеки "Самотестування" рівня НТ-3 має передбачати перевірку таких вимог:

Б.19.3.1 Політика послуги, що реалізується КЗЗ ОЕ, описує властивості ОЕ та реалізовані процедури, наведені при відповіді на п. А.19.2, що можуть бути використані для оцінювання правильності функціонування КЗЗ ОЕ.

Б.19.3.2 КЗЗ ОЕ здатний, з використанням засобів і за правилами, наведеними при відповіді на п. А.19.5, виконувати наведений при відповіді на п. А.19.3 набір тестів з метою оцінювання правильності функціонування своїх критичних функцій за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Б.19.3.3 КЗЗ ОЕ здатний при старті виконувати наведений при відповіді на п. А.19.3 набір тестів з метою оцінювання правильності функціонування своїх критичних функцій з використанням засобів і за правилами, наведеними при відповіді на п. А.19.6.

Б.19.3.4 КЗЗ ОЕ здатний в процесі штатного функціонування виконувати наведений при відповіді на п. А.19.3 набір тестів з метою оцінювання правильності функціонування своїх критичних функцій з використанням засобів і за правилами, наведеними при відповіді на п. А.19.7.

Б.20 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні"

Б.20.1 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-1 – "Автентифікація вузла"

Програма випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-1 має передбачати перевірку таких вимог:

Б.20.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину атрибутів КЗЗ, наведену при відповіді на п. А.20.3, і процедури, які необхідні

для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ (компонентом КЗЗ), наведені при відповіді на п. А.20.4.

Б.20.1.2 КЗЗ (компонент КЗЗ), перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), здатний ідентифікувати та автентифікувати цей КЗЗ (компонент КЗЗ) з використанням захищеного механізму і засобів, наведених при відповіді на п. А.20.4.

Б.20.1.3 Підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації, наведеного при відповіді на п. А.20.4.

Б.20.2 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-2 – "Автентифікація джерела даних"

Програма випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-2 має передбачати перевірку таких вимог:

Б.20.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину атрибутів КЗЗ, наведену при відповіді на п. А.20.3, і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ (компонентом КЗЗ), наведені при відповіді на п. А.20.4.

Б.20.2.2 КЗЗ (компонент КЗЗ), перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), здатний ідентифікувати та автентифікувати цей КЗЗ (компонент КЗЗ) з використанням захищеного механізму і засобів, наведених при відповіді на п. А.20.4.

Б.20.2.3 Підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації, наведеного при відповіді на п. А.20.4.

Б.20.2.4 КЗЗ ОЕ використовує захищені механізми і протокол, наведені при відповіді на п. А.20.7, для встановлення, з використанням атрибутів, наведених при відповіді на п. А.20.6, джерела кожного експортованого та імпортованого об'єкта кожного з наведених при відповіді на п. А.20.1 типів.

Б.20.3 Вимоги до програми випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-3 – "Автентифікація з підтвердженням"

Програма випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-3 має передбачати перевірку таких вимог:

Б.20.3.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину атрибутів КЗЗ, наведену при відповіді на п. А.20.3, і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ (компонентом КЗЗ), наведені при відповіді на п. А.20.4.

Б.20.3.2 КЗЗ (компонент КЗЗ), перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), здатний ідентифікувати та автентифікувати цей КЗЗ (компонент КЗЗ) з використанням захищеного механізму і засобів, наведених при відповіді на п. А.20.4.

Б.20.3.3 Підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації, наведеного при відповіді на п. А.20.4.

Б.20.3.4 КЗЗ ОЕ використовує захищені механізми і протокол, наведені при відповіді на п. А.20.7, для встановлення, з використанням атрибутів, наведених при відповіді на п. А.20.6, джерела кожного експортованого та імпортованого об'єкта кожного з наведених при відповіді на п. А.20.1 типів.

Б.20.3.5 Використовуваний протокол, опис якого наведено при відповіді на п. А.20.9, забезпечує можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною.

Б.21 Вимоги до програми випробувань функціональної послуги безпеки "Автентифікація відправника"

Б.21.1 Вимоги до програми випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-1 – "Базова автентифікація відправника"

Програма випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-1 має передбачати перевірку таких вимог:

Б.21.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину властивостей і атрибутів переданих об'єктів, користувачів-відправників та інтерфейсних процесів різного типу, наведену при відповіді на п. А.21.3, а також процедури, наведені при відповіді на п. А.21.4, які дозволяють однозначно встановити, що об'єкт кожного з наведених при відповіді на п. А.21.1 типів був відправлений (створений) певним користувачем.

Б.21.1.2 Установлення приналежності виконується на підставі затвердженого протоколу, опис якого наведено при відповіді на п. А.21.4, з використанням механізмів і засобів, наведених при відповіді на п. А.21.4.

Б.21.1.3 Атрибути користувача-відправника, використовувані в протоколі встановлення приналежності, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.21.2 Вимоги до програми випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-2 – "Автентифікація відправника з підтвердженням"

Програма випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-2 має передбачати перевірку таких вимог:

Б.21.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину властивостей і атрибутів переданих об'єктів, користувачів-відправників та інтерфейсних процесів різного типу, наведену при відповіді на п. А.21.3, а також процедури, наведені при відповіді на п. А.21.4, які дозволяють однозначно встановити, що об'єкт кожного з наведених при відповіді на п. А.21.1 типів був відправлений (створений) певним користувачем.

Б.21.2.2 Установлення приналежності виконується на підставі

затвердженого протоколу, опис якого наведено при відповіді на п. А.21.4, з використанням механізмів і засобів, наведених при відповіді на п. А.21.4.

Б.21.2.3 Додатково визначені властивості, атрибути і процедури, наведені при відповіді на п. А.21.6, що можуть використовуватися для однозначного підтвердження приналежності об'єкта певного типу незалежною третьою стороною.

Б.21.2.4 Використовуваний протокол підтвердження приналежності, опис якого наведено при відповіді на п. А.21.6, забезпечує можливість однозначного підтвердження приналежності об'єкта певного типу незалежною третьою стороною.

Б.21.2.5 Атрибути користувача-відправника, використовувані в протоколі встановлення приналежності, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.22 Вимоги до програми випробувань функціональної послуги безпеки "Автентифікація одержувача"

Б.22.1 Вимоги до програми випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-1 – "Базова автентифікація одержувача"

Програма випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-1 має передбачати перевірку таких вимог:

Б.22.1.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину властивостей і атрибутів переданих об'єктів, користувачів-одержувачів та інтерфейсних процесів різного типу, наведену при відповіді на п. А.22.3, а також процедури, наведені при відповіді на п. А.22.4, які дозволяють однозначно встановити, що об'єкт кожного з наведених при відповіді на п. А.22.1 типів був отриманий певним користувачем.

Б.22.1.2 Установлення одержувача виконується на підставі затвердженого протоколу, опис якого наведено при відповіді на п. А.22.4, з використанням механізмів і засобів, наведених при відповіді на п. А.22.4.

Б.22.1.3 Атрибути користувача-одержувача, використовувані в протоколі встановлення одержувача, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Б.22.2 Вимоги до програми випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-2 – "Автентифікація одержувача з підтвердженням"

Програма випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-2 має передбачати перевірку таких вимог:

Б.22.2.1 Політика послуги, що реалізується КЗЗ ОЕ, визначає множину властивостей і атрибутів переданих об'єктів, користувачів-одержувачів та

інтерфейсних процесів різного типу, наведену при відповіді на п. А.22.3, а також процедури, наведені при відповіді на п. А.22.4, які дозволяють однозначно встановити, що об'єкт кожного з наведених при відповіді на п. А.22.1 типів був отриманий певним користувачем.

Б.22.2.2 Установлення одержувача виконується на підставі затвердженого протоколу, опис якого наведено при відповіді на п. А.22.4, з використанням механізмів і засобів, наведених при відповіді на п. А.22.4.

Б.22.2.3 Додатково визначені властивості, атрибути і процедури, наведені при відповіді на п. А.22.6, що можуть використовуватися для однозначного підтвердження факту одержання об'єкта певного типу незалежною третьою стороною.

Б.22.2.4 Використовуваний протокол підтвердження одержувача, опис якого наведено при відповіді на п. А.22.6, забезпечує можливість однозначного підтвердження факту одержання об'єкта певного типу незалежною третьою стороною.

Б.22.2.5 Атрибути користувача-одержувача, використовувані в протоколі встановлення одержувача, автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація" рівня НИ-1 або вище згідно з політикою цієї послуги, наведеною при відповіді на п. А.15.2.

Додаток В
Вимоги щодо змісту методики випробувань функціональних послуг безпеки різних типів і різних рівнів (рекомендований)

У Додатку В викладені специфічні вимоги до змісту методики випробувань для функціональних послуг безпеки різних типів і різних рівнів. Вимоги викладені з урахуванням вимог НД ТЗІ 2.5-004-99 до політики функціональних послуг безпеки різних типів і різних рівнів, а також з урахуванням результатів ідентифікації функціональних послуг безпеки, уточнення їх рівнів і політики, отриманих експертом з використанням переліку спеціальних запитань, наведених у Додатку А, та вимог до змісту програми випробувань функціональних послуг безпеки різних типів і різних рівнів, викладених у Додатку Б.

В.1 Вимоги до методики випробувань функціональної послуги безпеки "Довірча конфіденційність"

В.1.1 Вимоги до методики випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-1 – "Мінімальна довірча конфіденційність"

Методика випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.1.1.1-Б.1.1.7, має містити:

В.1.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.1.7, шляхом попереднього (перед виконанням перевірок згідно з п. В.1.1.2-В.1.1.5) виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15..

В.1.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.1.1, Б.1.1.2, шляхом виконання запитів з метою доступу з використанням процесів усіх типів, наведених при відповіді на п. А.3.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.3.5.1 і таких, що визначають для кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у процесу прав одержання інформації від об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6. Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.1.3 Опис порядку перевірки вимог програми випробувань,

сформульованих з урахуванням п. Б.1.1.1, Б.1.1.3, Б.1.1.4, шляхом виконання запитів користувачами усіх типів, наведених при відповіді на п. А.3.4.2, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу процесів усіх типів, наведених при відповіді на п. А.3.4.2, до об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.1, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.1.1.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.1.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.1.1, Б.1.1.5, шляхом часткового повтору відповідних перевірок згідно з п. В.1.1.2 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.2. Опис порядку перевірки має містити опис, з урахуванням правил встановлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.1.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.1.1, Б.1.1.6, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.2 Вимоги до методики випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-2 – "Базова довірча конфіденційність"

Методика випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.1.2, має містити:

В.1.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.2.8, шляхом попереднього (перед виконанням перевірок згідно п. В.1.2.2-В.1.2.5) виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.1.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.2.1, Б.1.2.2, шляхом:

- виконання, з використанням відповідних засобів випробувань, запитів з метою доступу користувачами усіх типів, наведених при відповіді на п. А.3.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав одержання інформації від об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.3.4.2, користувачами усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.2.1, Б.1.2.3, Б.1.2.4, Б.1.2.5, шляхом:

- виконання запитів користувачами усіх типів, наведених при відповіді на п. А.3.4.2, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.3.4.2, до захищених об'єктів усіх типів (з метою одержання інформації від об'єкта), наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів користувачами усіх типів, наведених при відповіді на п. А.3.4.2, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п.

А.3.4.2, процесів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.1.2.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.2.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.2.1, Б.1.2.6, шляхом часткового повтору відповідних перевірок згідно з п. В.1.2.2 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.2.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.2.1, Б.1.2.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.3 Вимоги до методики випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-3 – "Повна довірча конфіденційність"

Методика випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.1.3, має містити:

В.1.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.3.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.1.3.2-В.1.3.7) виконання для всіх типів користувачів, наведених при

відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.1.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.3.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.1.3.3-В.1.3.7) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.1.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.3.1, Б.1.3.2, шляхом:

- виконання, з використанням відповідних засобів випробувань, запитів з метою доступу з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав одержання інформації від об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.3.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1 для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.3.1, Б.1.3.3, Б.1.3.4, Б.1.3.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.3.4.1 (та їх груп), до захищених об'єктів усіх типів (з метою одержання інформації від об'єкта), наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і

відсутність у користувача прав володіння захищеним об'єктом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.3.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.1.3.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.3.1, Б.1.3.6, шляхом часткового повтору відповідних перевірок згідно з п. В.1.3.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.3.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.3.1, Б.1.3.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.4 Вимоги до методики випробувань функціональної послуги безпеки "Довірча конфіденційність" рівня КД-4 – "Абсолютна довірча конфіденційність"

Методика випробувань функціональної послуги безпеки "Довірча

конфіденційність" рівня КД-4 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.1.4, має містити:

В.1.4.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.4.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.1.4.2-В.1.4.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.1.4.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.4.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.1.4.3-В.1.4.6) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.1.4.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.4.1, Б.1.4.2, шляхом:

- виконання запитів з метою доступу до об'єкта з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням процесів усіх типів, наведених при відповіді на п. А.3.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів і захищених об'єктів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав одержання інформації від об'єкта з використанням цього процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.3.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.4.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.4.1, Б.1.4.3, Б.1.4.4, Б.1.4.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.3.4.1 (та їх груп), і процесів усіх типів, наведених при відповіді на п. А.3.4.1 (та їх груп), до захищених об'єктів усіх типів (з метою одержання інформації від об'єкта), наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів та захищених об'єктів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом або процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.3.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.1.4.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.4.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.4.1, Б.1.4.6, шляхом часткового повтору відповідних перевірок згідно з п. В.1.4.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.1.4.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.1.4.1, Б.1.4.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на

п. А.3.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна конфіденційність"

В.2.1 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-1 – "Мінімальна адміністративна конфіденційність"

Методика випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.2.1.1-Б.2.1.7, має містити:

В.2.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.1.7, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.1.2-В.2.1.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.2.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.1.3, Б.2.1.4, в частині, що стосується оброблення запитів на зміну прав доступу лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.1.3-В.2.1.6) виконання для відповідних типів користувачів, наведених при відповіді на п. А.3.4.2, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.3.7, у засобах, наведених при відповіді на п. А.3.8.

В.2.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.1.1, Б.2.1.2, шляхом виконання запитів з метою доступу з використанням процесів усіх типів, наведених при відповіді на п. А.3.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.3.5.1 і таких, що визначають для кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у процесу прав одержання інформації від об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при

відповіді на п. А.3.6. Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.1.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.1.1, Б.2.1.3, Б.2.1.4, шляхом виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.2, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу процесів усіх типів, наведених при відповіді на п. А.3.4.2, до об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.1, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів адміністраторів або користувачів, яким надані відповідні повноваження, на зміну прав доступу до захищених об'єктів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.2.1.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.1.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.1.1, Б.2.1.5, шляхом часткового повтору відповідних перевірок згідно з п. В.2.1.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.1.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.1.1, Б.2.1.6, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.2 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-2 – "Базова

адміністративна конфіденційність"

Методика випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.2.2.1-Б.2.2.8, має містити:

В.2.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.2.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.2.2-В.2.2.7) виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.2.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.2.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.2.3-В.2.2.7) виконання для відповідних типів користувачів, наведених при відповіді на п. А.3.4.2, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.3.7, у засобах, наведених при відповіді на п. А.3.8.

В.2.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.2.1, Б.2.2.2, шляхом:

- виконання, з використанням відповідних засобів випробувань, запитів з метою доступу з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав одержання інформації від об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.3.4.2, з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.2.4 Опис порядку перевірки вимог програми випробувань,

сформульованих з урахуванням п. Б.2.2.1, Б.2.2.3, Б.2.2.4, Б.2.2.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.2, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.3.4.2, до захищених об'єктів усіх типів (з метою одержання інформації від об'єкта), наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.2, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.3.4.2, процесів усіх типів, наведених при відповіді на п. А.3.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів адміністраторів або користувачів, яким надані відповідні повноваження, на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.3.7, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.2.2.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.2.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.2.1, Б.2.2.6, шляхом часткового повтору відповідних перевірок згідно з п. В.2.2.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.2.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.2.1, Б.2.2.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.2, з подальшим контролем результатів збереження атрибутів доступу

захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.3 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-3 – "Повна адміністративна конфіденційність"

Методика випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.2.3.1-Б.2.3.9, має містити:

В.2.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.8, шляхом попереднього, перед виконанням перевірок згідно з п. В.2.3.2-В.2.3.7, виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.2.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.3.3-В.2.3.7, виконання для відповідних типів користувачів, наведених при відповіді на п. А.3.4) випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.3.7, у засобах, наведених при відповіді на п. А.3.8.

В.2.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.3.4-В.2.3.7) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.2.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.1, Б.2.3.2, шляхом:

- виконання, з використанням відповідних засобів випробувань, запитів з метою доступу з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так

і відсутність у користувача прав одержання інформації від об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.3.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.1, Б.2.3.3, Б.2.3.4, Б.2.3.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.3.4.1 (та їх груп), до захищених об'єктів усіх типів (з метою одержання інформації від об'єкта), наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.3.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів адміністраторів або користувачів, яким надані відповідні повноваження, на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних

перевірок згідно з п. В.2.3.4), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.3.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.1, Б.2.3.6, шляхом часткового повтору відповідних перевірок згідно з п. В.2.3.4 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.3.7 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.1, Б.2.3.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.4 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-4 – "Абсолютна адміністративна конфіденційність"

Методика випробувань функціональної послуги безпеки "Адміністративна конфіденційність" рівня КА-4 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.2.4.1-Б.2.4.9, має містити:

В.2.4.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.4.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.4.2-В.2.4.7) виконання для всіх типів користувачів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.2.4.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.3.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.4.3-В.2.4.7) виконання для відповідних типів користувачів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.3.7, у засобах, наведених при відповіді на п. А.3.8.

В.2.4.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.4.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.2.4.4-В.2.4.7) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.2.4.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.4.1, Б.2.4.2, шляхом:

- виконання запитів з метою доступу до об'єкта з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням процесів усіх типів, наведених при відповіді на п. А.3.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів і захищених об'єктів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав одержання інформації від об'єкта з використанням цього процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.3.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.3.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.3.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.4.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.4.1, Б.2.4.3, Б.2.4.4, Б.2.4.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.3.4.1 (та їх груп), і процесів усіх типів, наведених при відповіді на п. А.3.4.1 (та їх груп), до захищених об'єктів усіх типів (з метою одержання інформації від об'єкта), наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів та захищених об'єктів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як

наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.3.4.1, з використанням засобів, наведених при відповіді на п. А.3.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.3.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.3.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.3.5.2, А.3.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів адміністраторів або користувачів, яким надані відповідні повноваження, на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.3.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.2.4.4), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.4.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.4.1, Б.2.4.6, шляхом часткового повтору відповідних перевірок згідно з п. В.2.4.4 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.3.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.2.4.7 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.2.4.1, Б.2.4.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.3.12, А.3.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.3 Вимоги до методики випробувань функціональної послуги безпеки "Повторне використання об'єктів"

В.3.1 Вимоги до методики випробувань функціональної послуги

безпеки "Повторне використання об'єктів" рівня КО-1

Методика випробувань функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.3.1.1-Б.3.1.3, має містити:

В.3.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.3.1.1, Б.3.1.2, шляхом виконання, з використанням відповідних засобів випробувань, перевірки факту забезпечення, з використанням засобів і механізмів, наведених при відповіді на п. А.4.3, неможливості успадкування атрибутів доступу, встановлених для раніше видалених об'єктів, знову створюваними на тому ж самому поділюваному ресурсі пасивними об'єктами всіх типів, наведених при відповіді на п. А.4.2. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби створення нового об'єкта замість раніше видаленого, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.3.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.3.1.1, Б.3.1.3, шляхом виконання, з використанням відповідних засобів випробувань, перевірки факту знищення з використанням засобів і механізмів, наведених при відповіді на п. А.4.4, залишкової інформації, яка містилася в раніше видалених об'єктах, що зберігалися на поділюваному ресурсі, наприклад, методом низькорівневого повторного читання ресурсу, раніше займаного видаленим об'єктом, для ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.4.2. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби перевірки факту знищення залишкової інформації, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4 Вимоги до методики випробувань функціональної послуги безпеки "Аналіз прихованих каналів"

В.4.1 Вимоги до методики випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-1 – "Виявлення прихованих каналів"

Методика випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.4.1.1-Б.4.1.6, має містити:

В.4.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.1.1-Б.4.1.4, шляхом виконання перевірки результатів аналізу прихованих каналів, наведених при відповіді на п. А.5.1-А.5.4. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.1.2 Опис порядку перевірки вимог програми випробувань,

сформульованих з урахуванням п. Б.4.1.6, шляхом виконання перевірки заявленого розробником і зазначеного в проектній документації на ОЕ рівня гарантій коректності реалізації функціональних послуг безпеки, а також шляхом аналізу результатів експертизи в частині, що стосується підтвердження заявленого рівня гарантій. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.1.5, шляхом виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.4.2 Вимоги до методики випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-2 – "Контроль прихованих каналів"

Методика випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.4.2.1-Б.4.2.7, має містити:

В.4.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.2.1-Б.4.2.4, шляхом виконання перевірки результатів аналізу прихованих каналів, наведених при відповіді на п. А.5.1-А.5.4. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.2.7, шляхом виконання перевірки заявленого розробником і зазначеного в проектній документації на ОЕ рівня гарантій коректності реалізації функціональних послуг безпеки, а також шляхом аналізу результатів експертизи в частині, що стосується підтвердження заявленого рівня гарантій. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.2.6, шляхом виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.4.2.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.2.5, шляхом виконання, з використанням відповідних засобів випробувань, спроб ініціювання використання кожного з

документованих прихованих каналів, що входить до наведеної при відповіді на п. А.5.5 затвердженої підмножини, з контролем фактів реєстрації відповідних подій засобами і механізмами, наведеними при відповіді на п. А.5.5, а також засобами реалізації послуги "Реєстрація" певного рівня. Перевірка засобів реалізації послуги "Реєстрація" в частині, що стосується реєстрації відповідних подій, може виконуватися шляхом випробувань згідно з п. В.14. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.3 Вимоги до методики випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-3 – "Перекриття прихованих каналів"

Методика випробувань функціональної послуги безпеки "Аналіз прихованих каналів" рівня КК-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.4.3.1-4.3.4, має містити:

В.4.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.3.1, шляхом виконання перевірки результатів аналізу прихованих каналів, наведених при відповіді на п. А.5.1. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.3.4, шляхом виконання перевірки заявленого розробником і зазначеного в проектній документації на ОЕ рівня гарантій коректності реалізації функціональних послуг безпеки, а також шляхом аналізу результатів експертизи в частині, що стосується підтвердження заявленого рівня гарантій. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.4.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.3.3, шляхом виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.3.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.4.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.4.3.2, шляхом виконання, з використанням відповідних засобів випробувань, спроб ініціювання використання кожного з документованих прихованих каналів, що входить до наведеної при відповіді на п. А.5.2 множини, з контролем фактів запобігання можливості їх використання засобами і механізмами, наведеними при відповіді на п. А.5.3. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5 Вимоги до методики випробувань функціональної послуги безпеки "Конфіденційність при обміні"

В.5.1 Вимоги до методики випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-1 – "Мінімальна конфіденційність при обміні"

Методика випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.5.1.1-Б.5.1.3, має містити:

В.5.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.1.1-Б.5.1.3, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.2, об'єктів усіх типів, наведених при відповіді на п. А.6.3.2, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою підтвердження можливості забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.2 Вимоги до методики випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-2 – "Базова конфіденційність при обміні"

Методика випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.5.2.1-Б.5.2.6, має містити:

В.5.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.2.2, Б.5.2.4, шляхом попереднього (перед виконанням перевірок згідно з п. В.5.2.2-В.5.2.3) виконання для відповідних типів користувачів, наведених при відповіді на п. А.6.5, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.6.5, у засобах, наведених при відповіді на п. А.6.4.

В.5.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.2.1, Б.5.2.3, Б.5.2.5, Б.5.2.6, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.2, об'єктів усіх типів, наведених при відповіді на п. А.6.3.2, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на

п. А.6.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, наведених при відповіді на п. А.6.6.2, атрибутів інтерфейсних процесів, що здійснюють приймання, наведених при відповіді на п. А.6.7.2, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою:

- підтвердження можливості забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4;

- підтвердження можливості оброблення запитів на експорт захищеного об'єкта певного типу передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.6.2;

- підтвердження можливості оброблення запитів на імпорт захищеного об'єкта певного типу приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.6.7.2.

Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.2.1, Б.5.2.2, Б.5.2.4, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.6.4, з метою зміни рівня захищеності переданих об'єктів усіх типів, наведених при відповіді на п. А.6.3.2, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.6.5 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну рівня захищеності переданих об'єктів різного типу, наведених при відповіді на п. А.6.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни рівня захищеності, опис порядку перевірки факту зміни рівня захищеності (шляхом часткового повтору відповідних перевірок згідно з п. В.5.2.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.3 Вимоги до методики випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-3 – "Повна конфіденційність при обміні"

Методика випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п.

Б.5.3.1-Б.5.3.7, має містити:

В.5.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.3.2, Б.5.3.4, шляхом попереднього (перед виконанням перевірок згідно з п. В.5.3.2-В.5.3.5) виконання для відповідних типів користувачів, наведених при відповіді на п. А.6.5, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.6.5, у засобах, наведених при відповіді на п. А.6.4.

В.5.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.3.5, Б.5.3.6, у частині, що стосується автентифікації атрибутів джерела і приймача об'єкта, шляхом попереднього (перед виконанням перевірок згідно з п. В.5.3.3-В.5.3.5) виконання стосовно приймача об'єкта і його атрибутів, наведених при відповіді на п. А.6.6.1, та джерела об'єкта і його атрибутів, наведених при відповіді на п. А.6.7.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" певного рівня згідно з п. В.20, у засобах, наведених при відповіді на п. А.6.4.

В.5.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.3.1, Б.5.3.3, Б.5.3.5, Б.5.3.6, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.1, об'єктів усіх типів, наведених при відповіді на п. А.6.3.2, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.6.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу та атрибутів приймача об'єкта, наведених при відповіді на п. А.6.6.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою:

- підтвердження можливості забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4;

- підтвердження можливості оброблення запитів на експорт захищеного об'єкта певного типу передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу та атрибутів одержувача об'єкта, наведених при відповіді на п. А.6.6.1;

- підтвердження можливості оброблення запитів на імпорт захищеного об'єкта певного типу приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1.

Опис порядку перевірки має містити опис очікуваних результатів для

кожної спроби передачі (експорту) та приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу і різних атрибутів одержувача або джерела об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.3.1, Б.5.3.2, Б.5.3.4, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.6.4, з метою зміни рівня захищеності переданих об'єктів усіх типів, наведених при відповіді на п. А.6.3.1, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.6.5 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну рівня захищеності переданих об'єктів різного типу, наведених при відповіді на п. А.6.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни рівня захищеності, опис порядку перевірки факту зміни рівня захищеності (шляхом часткового повтору відповідних перевірок згідно з п. В.5.3.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.3.1, Б.5.3.7, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.1, об'єктів усіх типів, наведених при відповіді на п. А.6.3.1, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.6.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, та атрибутів приймача об'єкта, наведених при відповіді на п. А.6.6.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою підтвердження того, що представлення захищеного об'єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об'єкта, а також його джерела і приймача, згідно з описом, наведеним при відповіді на п. А.6.8. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу і різних атрибутів одержувача або джерела об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4 Вимоги до методики випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-4 – "Абсолютна конфіденційність при обміні"

Методика випробувань функціональної послуги безпеки "Конфіденційність при обміні" рівня КВ-4 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п.

Б.5.4.1-Б.5.4.12, має містити:

В.5.4.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.2, Б.5.4.4, шляхом попереднього (перед виконанням перевірок згідно з п. В.5.4.2-В.5.4.9) виконання для відповідних типів користувачів, наведених при відповіді на п. А.6.5, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.6.5, у засобах, наведених при відповіді на п. А.6.4.

В.5.4.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.5, Б.5.4.6, у частині, що стосується автентифікації атрибутів джерела і приймача об'єкта, шляхом попереднього (перед виконанням перевірок згідно з п. В.5.4.3-В.5.4.9) виконання стосовно приймача об'єкта і його атрибутів, наведених при відповіді на п. А.6.6.1, та джерела об'єкта і його атрибутів, наведених при відповіді на п. А.6.7.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" певного рівня згідно з п. В.20 у засобах, наведених при відповіді на п. А.6.4.

В.5.4.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.12, шляхом виконання перевірки заявленого розробником і зазначеного в проектній документації на ОЕ рівня гарантій коректності реалізації функціональних послуг безпеки, а також шляхом аналізу результатів експертизи в частині, що стосується підтвердження заявленого рівня гарантій. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.1, Б.5.4.3, Б.5.4.5, Б.5.4.6, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.1, об'єктів усіх типів, наведених при відповіді на п. А.6.3.1, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.6.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, та атрибутів приймача об'єкта, наведених при відповіді на п. А.6.6.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою:

- підтвердження можливості забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.6.4;

- підтвердження можливості оброблення запитів на експорт захищеного об'єкта певного типу передавальним КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу

інтерфейсного процесу відповідного типу та атрибутів одержувача об'єкта, наведених при відповіді на п. А.6.6.1;

- підтвердження можливості оброблення запитів на імпорт захищеного об'єкта певного типу приймаючим КЗЗ (компонентом КЗЗ) у засобах, наведених при відповіді на п. А.6.4, на підставі атрибутів доступу інтерфейсного процесу відповідного типу та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1.

Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу і різних атрибутів одержувача або джерела об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.1, Б.5.4.2, Б.5.4.4, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.6.4, з метою зміни рівня захищеності переданих об'єктів усіх типів, наведених при відповіді на п. А.6.3.1, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.6.5 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну рівня захищеності переданих об'єктів різного типу, наведених при відповіді на п. А.6.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни рівня захищеності, опис порядку перевірки факту зміни рівня захищеності (шляхом часткового повтору відповідних перевірок згідно з п. В.5.4.4), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.1, Б.5.4.7, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.6.3.1, об'єктів усіх типів, наведених при відповіді на п. А.6.3.1, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.6.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, та атрибутів приймача об'єкта, наведених при відповіді на п. А.6.6.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.6.7.1, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою підтвердження того, що представлення захищеного об'єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об'єкта, а також його джерела і приймача, згідно з описом, наведеним при відповіді на п. А.6.8. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу і

різних атрибутів одержувача або джерела об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4.7 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.8, Б.5.4.9, шляхом виконання перевірки опису інформації, яку можна одержати шляхом спільного аналізу ряду отриманих об'єктів певного типу, наведеного при відповіді на п. А.6.9, а також результатів аналізу прихованих каналів обміну, наведених при відповіді на п. А.6.9, А.6.10, А.6.11. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4.8 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.10, шляхом виконання, з використанням відповідних засобів випробувань, спроб ініціювання використання кожного з документованих прихованих каналів обміну, що входить до наведеної при відповіді на п. А.6.12 затвердженої підмножини, з контролем фактів реєстрації відповідних подій засобами і механізмами, наведеними при відповіді на п. А.6.12, а також засобами реалізації послуги "Реєстрація" певного рівня. Перевірка засобів реалізації послуги "Реєстрація" в частині, що стосується реєстрації відповідних подій, може виконуватися, шляхом випробувань згідно з п. В.14. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.5.4.9 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.5.4.11, шляхом виконання, з використанням відповідних засобів випробувань, спроб ініціювання використання кожного з документованих прихованих каналів обміну, що входить до наведеної при відповіді на п. А.6.9 множини, з контролем фактів їх часткового перекриття або запобігання можливості їх використання засобами і механізмами, наведеними при відповіді на п. А.6.13. Опис порядку перевірки має містити опис очікуваних результатів перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6 Вимоги до методики випробувань функціональної послуги безпеки "Довірча цілісність"

В.6.1 Вимоги до методики випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-1 – "Мінімальна довірча цілісність"

Методика випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.6.1.1-Б.6.1.7, має містити:

В.6.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.1.7, шляхом попереднього (перед

виконанням перевірок згідно з п. В.6.1.2-В.6.1.5) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.6.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.1.1, Б.6.1.2, шляхом виконання, з використанням відповідних засобів випробувань, запитів з метою доступу користувачів усіх типів, наведених при відповіді на п. А.7.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.7.5.1 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав модифікації об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6. Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.1.1, Б.6.1.3, Б.6.1.4, шляхом виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.7.4.2, до об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.7.5.1, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.6.1.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.1.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.1.1, Б.6.1.5, шляхом часткового повтору відповідних перевірок згідно з п. В.6.1.2 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11,

очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.1.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.1.1, Б.6.1.6, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.2 Вимоги до методики випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-2 – "Базова довірча цілісність"

Методика випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.6.2.1-Б.6.2.8, має містити:

В.6.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.2.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.6.2.2-В.6.2.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.6.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.2.1, Б.6.2.2, шляхом:

- виконання запитів з метою доступу з боку процесів усіх типів, наведених при відповіді на п. А.7.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу процесу і кожного типу захищеного об'єкта як наявність, так і відсутність у процесу прав модифікації об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.7.4.2, з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав

ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.2.1, Б.6.2.3, Б.6.2.4, Б.6.2.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу процесів усіх типів, наведених при відповіді на п. А.7.4.2, до захищених об'єктів (з метою модифікації об'єкта) всіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.7.4.2, процесів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.6.2.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.2.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.2.1, Б.6.2.6, шляхом часткового повтору відповідних перевірок згідно з п. В.6.2.2 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби

доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.2.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.2.1, Б.6.2.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.3 Вимоги до методики випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-3 – "Повна довірча цілісність"

Методика випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.6.3.1-Б.6.3.9, має містити:

В.6.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.3.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.6.3.2-В.6.3.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.6.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.3.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.6.3.3-В.6.3.6) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.6.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.3.1, Б.6.3.2, шляхом:

- виконання запитів з метою доступу з боку процесів усіх типів, наведених при відповіді на п. А.7.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у процесу прав модифікації об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.7.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.3.1, Б.6.3.3, Б.6.3.4, Б.6.3.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу процесів усіх типів, наведених при відповіді на п. А.7.4.1 (та їх груп), до захищених об'єктів (з метою модифікації об'єкта) усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.7.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2, А.7.7 таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.6.3.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.3.1, Б.6.3.6, шляхом часткового повтору

відповідних перевірок згідно з п. В.6.3.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.3.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.3.1, Б.6.3.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.4 Вимоги до методики випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-4 – "Абсолютна довірча цілісність"

Методика випробувань функціональної послуги безпеки "Довірча цілісність" рівня ЦД-4 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.6.4.1-Б.6.4.9, має містити:

В.6.4.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.4.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.6.4.2-В.6.4.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.6.4.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.4.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.6.4.3-В.6.4.6) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.6.4.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.4.1, Б.6.4.2, шляхом:

- виконання запитів з метою доступу до об'єкта з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням процесів усіх типів, наведених при відповіді на п. А.7.4.1, до захищених об'єктів усіх типів,

наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав модифікації об'єкта з використанням цього процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.7.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.4.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.4.1, Б.6.4.3, Б.6.4.4, Б.6.4.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.7.4.1 (та їх груп) і процесів усіх типів, наведених при відповіді на п. А.7.4.1 (та їх груп), до захищених об'єктів (з метою модифікації об'єкта) всіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав володіння захищеним об'єктом або процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.7.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.6.4.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.4.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.4.1, Б.6.4.6, шляхом часткового повтору відповідних перевірок згідно з п. В.6.4.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.6.4.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.6.4.1, Б.6.4.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна цілісність"

В.7.1 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-1 – "Мінімальна адміністративна цілісність"

Методика випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.7.1.1-Б.7.1.7, має містити:

В.7.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.1.7, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.1.2-В.7.1.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.7.1.2 Опис порядку перевірки вимог програми випробувань,

сформульованих з урахуванням п. Б.7.1.3, Б.7.1.4, в частині, що стосується оброблення запитів на зміну прав доступу лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.1.3-В.7.1.6) виконання для відповідних типів користувачів, наведених при відповіді на п. А.7.4.2, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.7.7, у засобах, наведених при відповіді на п. А.7.8.

В.7.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.1.1, Б.7.1.2, шляхом виконання, з використанням відповідних засобів випробувань, запитів з метою доступу користувачів усіх типів, наведених при відповіді на п. А.7.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.7.5.1 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав модифікації об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6. Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.1.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.1.1, Б.7.1.3, Б.7.1.4, шляхом виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.7.4.2, до об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.7.5.1, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.7.1.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.1.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.1.1, Б.7.1.5, шляхом часткового повтору відповідних перевірок згідно з п. В.7.1.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.1.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.1.1, Б.7.1.6, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.2 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-2 – "Базова адміністративна цілісність"

Методика випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.7.2.1-Б.7.2.8, має містити:

В.7.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.2.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.2.2-В.7.2.6) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.7.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.2.3, Б.7.2.4, в частині, що стосується оброблення запитів на зміну прав доступу лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.2.3-В.7.2.6) виконання для відповідних типів користувачів, наведених при відповіді на п. А.7.4.2, випробувань засобів реалізації функціональної

послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.7.7, у засобах, наведених при відповіді на п. А.7.8.

В.7.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.2.1, Б.7.2.2, шляхом:

- виконання запитів з метою доступу з боку процесів усіх типів, наведених при відповіді на п. А.7.4.2, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу процесу і кожного типу захищеного об'єкта як наявність, так і відсутність у процесу прав модифікації об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.7.4.2, з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.2.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.2.1, Б.7.2.3, Б.7.2.4, Б.7.2.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу процесів усіх типів, наведених при відповіді на п. А.7.4.2, до захищених об'єктів (з метою модифікації об'єкта) всіх типів, наведених при відповіді на п. А.7.4.2, для всіх можливих сполучень атрибутів доступу користувачів і захищених об'єктів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.2, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.7.4.2, процесів усіх типів, наведених при відповіді на п. А.7.4.2, для всіх

можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.7.2.3), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.2.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.2.1, Б.7.2.6, шляхом часткового повтору відповідних перевірок згідно з п. В.7.2.2 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.2. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.2.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.2.1, Б.7.2.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.2, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.3 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-3 – "Повна адміністративна цілісність"

Методика випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.7.3.1-Б.7.3.9, має містити:

В.7.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.3.2-В.7.3.7) виконання для всіх типів користувачів, наведених при відповіді на

п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.7.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.3, Б.7.3.4, в частині, що стосується оброблення запитів на зміну прав доступу лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.2.3-В.7.2.6) виконання для відповідних типів користувачів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.7.7, у засобах, наведених при відповіді на п. А.7.8.

В.7.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.3.3-В.7.3.6) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.7.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.1, Б.7.3.2, шляхом:

- виконання запитів з метою доступу з боку процесів усіх типів, наведених при відповіді на п. А.7.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у процесу прав модифікації об'єкта, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.7.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а

також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.1, Б.7.3.3, Б.7.3.4, Б.7.3.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу процесів усіх типів, наведених при відповіді на п. А.7.4.1 (та їх груп), до захищених об'єктів (з метою модифікації об'єкта) всіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.7.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.7.3.4), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.3.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.1, Б.7.3.6, шляхом часткового повтору відповідних перевірок згідно з п. В.7.3.3 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.3.7 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.3.1, Б.7.3.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій

експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.4 Вимоги до методики випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-4 – "Абсолютна адміністративна цілісність"

Методика випробувань функціональної послуги безпеки "Адміністративна цілісність" рівня ЦА-4 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.7.4.1-Б.7.4.9, має містити:

В.7.4.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.8, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.4.2-В.7.4.7) виконання для всіх типів користувачів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.7.4.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.3, Б.7.4.4, в частині, що стосується оброблення запитів на зміну прав доступу лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.4.3-В.7.4.7) виконання для відповідних типів користувачів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.7.7, у засобах, наведених при відповіді на п. А.7.8.

В.7.4.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.9, шляхом попереднього (перед виконанням перевірок згідно з п. В.7.4.3-В.7.4.7) виконання для поділюваних ресурсів, використовуваних для збереження захищених пасивних об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, випробувань засобів реалізації функціональної послуги безпеки "Повторне використання об'єктів" рівня КО-1 згідно з п. В.3.

В.7.4.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.1, Б.7.4.2, шляхом:

- виконання запитів з метою доступу до об'єкта з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням процесів усіх типів, наведених при відповіді на п. А.7.4.1, до захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача прав модифікації об'єкта з використанням цього процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6;

- виконання, з використанням відповідних засобів випробувань, запитів з метою ініціювання процесів усіх типів, наведених при відповіді на п. А.7.4.1, з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2 і таких, що визначають для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав ініціювання процесу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.7.6.

Опис порядку перевірки має містити опис, з урахуванням правил розмежування доступу, наведених при відповіді на п. А.7.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.4.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.1, Б.7.4.3, Б.7.4.4, Б.7.4.5, шляхом:

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав доступу користувачів усіх типів, наведених при відповіді на п. А.7.4.1 (та їх груп), і процесів усіх типів, наведених при відповіді на п. А.7.4.1 (та їх груп), до захищених об'єктів (з метою модифікації об'єкта) всіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів, процесів і захищених об'єктів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають для кожного типу користувачів, кожного типу процесів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ;

- виконання запитів з боку користувачів усіх типів, наведених при відповіді на п. А.7.4.1, з використанням засобів, наведених при відповіді на п. А.7.8, з метою зміни прав ініціювання користувачами всіх типів, наведених при відповіді на п. А.7.4.1 (та їх групами), процесів усіх типів, наведених при відповіді на п. А.7.4.1, для всіх можливих сполучень атрибутів доступу користувачів і процесів, наведених при відповіді на п. А.7.5.2, А.7.7 і таких, що визначають

для кожного типу користувачів і кожного типу процесів як наявність, так і відсутність у користувача прав володіння процесом, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну прав доступу до захищених об'єктів і процесів різного типу, наведених при відповіді на п. А.7.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни прав доступу, опис порядку перевірки факту зміни прав доступу (шляхом часткового повтору відповідних перевірок згідно з п. В.7.4.4), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.4.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.1, Б.7.4.6, шляхом часткового повтору відповідних перевірок згідно з п. В.7.4.4 для об'єктів усіх типів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.4.1. Опис порядку перевірки має містити опис, з урахуванням правил установлення атрибутів доступу для об'єктів, що знову створюються або ініціалізуються, наведених при відповіді на п. А.7.11, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби доступу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.7.4.7 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.7.4.1, Б.7.4.7, шляхом послідовного виконання, з використанням відповідних засобів випробувань, операцій експорту та імпорту захищених об'єктів усіх типів, наведених при відповіді на п. А.7.4.1, з подальшим контролем результатів збереження атрибутів доступу захищених об'єктів різного типу. Опис порядку перевірки має містити опис, з урахуванням правил, наведених при відповіді на п. А.7.12, А.7.13, очікуваних результатів виконання збереження атрибутів доступу об'єктів різного типу після їх експорту та імпорту, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.8 Вимоги до методики випробувань функціональної послуги безпеки "Відкат"

В.8.1 Вимоги до методики випробувань функціональної послуги безпеки "Відкат" рівня ЦО-1 – "Обмежений відкат"

Методика випробувань функціональної послуги безпеки "Відкат" рівня ЦО-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.8.1.1-Б.8.1.2, має містити:

В.8.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.8.1.2, в частині, що стосується оброблення запитів на скасування ("відкат") певного набору (множини), операцій, проведених над захищеним об'єктом певного типу за певний проміжок часу, лише авторизованим користувачем, атрибути якого автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація", шляхом попереднього (перед виконанням перевірок згідно з п. В.8.1.2)

виконання для всіх типів користувачів, наведених при відповіді на п. А.8.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.8.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.8.1.1, Б.8.1.2, шляхом виконання з боку користувачів усіх типів, наведених при відповіді на п. А.8.2, з використанням функціональних модулів ОЕ, наведених при відповіді на п. А.8.3, запитів на скасування ("відкат") різних наборів (множин) операцій, наведених при відповіді на п. А.8.4.2, проведених за певні проміжки часу над захищеними об'єктами всіх типів, наведених при відповіді на п. А.8.2, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ. Опис порядку перевірки має містити опис, з урахуванням правил функціонування механізмів виконання скасування ("відкату") різних наборів (множин) операцій, наведених при відповіді на п. А.8.3, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби виконання скасування ("відкату") різних наборів (множин) операцій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.8.2 Вимоги до методики випробувань функціональної послуги безпеки "Відкат" рівня ЦО-2 – "Повний відкат"

Методика випробувань функціональної послуги безпеки "Відкат" рівня ЦО-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.8.2.1-Б.8.2.2, має містити:

В.8.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.8.2.2, в частині, що стосується оброблення запитів на скасування ("відкат") певного набору (множини), операцій, проведених над захищеним об'єктом певного типу за певний проміжок часу, лише авторизованим користувачем, атрибути якого автентифіковані з використанням засобів реалізації послуги "Ідентифікація та автентифікація", шляхом попереднього (перед виконанням перевірок згідно з п. В.8.2.2) виконання для всіх типів користувачів, наведених при відповіді на п. А.8.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.8.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.8.2.1, Б.8.2.2, шляхом виконання з боку користувачів усіх типів, наведених при відповіді на п. А.8.2, з використанням функціональних модулів ОЕ, наведених при відповіді на п. А.8.3, запитів на скасування ("відкат") всіх операцій, наведених при відповіді на п. А.8.4.1, проведених за певні проміжки часу над захищеними об'єктами всіх типів, наведених при відповіді на п. А.8.2, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ. Опис порядку перевірки має містити опис, з урахуванням правил функціонування механізмів виконання скасування ("відкату") різних наборів (множин) операцій, наведених при відповіді на п.

А.8.3, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби виконання скасування ("відкату") різних наборів (множин) операцій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.9 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність при обміні"

В.9.1 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-1 – "Мінімальна цілісність при обміні"

Методика випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.9.1.1-Б.9.1.3, має містити:

В.9.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.1.1-Б.9.1.3, шляхом виконання спроб передачі (експорту), модифікації з використанням відповідних засобів випробувань, подальшого приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3, об'єктів усіх типів, наведених при відповіді на п. А.9.3, з подальшим аналізом результатів приймання модифікованих об'єктів з метою підтвердження можливості виявлення з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.1, А.9.4, порушень цілісності інформації, що міститься в переданих об'єктах різного типу. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби приймання (імпорту) модифікованого об'єкта кожного типу з використанням інтерфейсного процесу кожного типу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.9.2 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-2 – "Базова цілісність при обміні"

Методика випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.9.2.1-Б.9.2.6, має містити:

В.9.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.2.2, Б.9.2.6, шляхом попереднього (перед виконанням перевірок згідно з п. В.9.2.2-В.9.2.3) виконання для відповідних типів користувачів, наведених при відповіді на п. А.9.6, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.9.6, у засобах, наведених при відповіді на п. А.9.4, А.9.5.

В.9.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.2.1, Б.9.2.3-Б.9.2.5, шляхом:

- виконання спроб передачі (експорту), модифікації з використанням відповідних засобів випробувань, подальшого приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3, об'єктів усіх типів, наведених при відповіді на п. А.9.3, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.9.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, наведених при відповіді на п. А.9.7.2, атрибутів інтерфейсних процесів, що здійснюють приймання, наведених при відповіді на п. А.9.8.2, з подальшим аналізом результатів приймання модифікованих об'єктів з метою підтвердження можливості виявлення порушень цілісності інформації, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.1, А.9.4, підтвердження можливості оброблення запитів на експорт захищеного об'єкта певного типу передавальним КЗЗ (компонентом КЗЗ) на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.9.7.2, та підтвердження можливості оброблення запитів на імпорт захищеного об'єкта певного типу приймаючим КЗЗ (компонентом КЗЗ) на підставі атрибутів доступу інтерфейсного процесу відповідного типу, наведених при відповіді на п. А.9.8.2;

- виконання спроб передачі (експорту) послідовності об'єктів і подальшого приймання (імпорту) об'єктів у порядку, відмінному від порядку передачі (експорту), відмова від приймання (імпорту) деяких об'єктів з послідовності, а також багаторазового приймання (імпорту) деяких об'єктів з послідовності з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3, об'єктів усіх типів, наведених при відповіді на п. А.9.3, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.9.5 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, наведених при відповіді на п. А.9.7.2, атрибутів інтерфейсних процесів, що здійснюють приймання, наведених при відповіді на п. А.9.8.2, з подальшим аналізом результатів приймання об'єктів з метою підтвердження можливості виявлення фактів їх видалення чи дублювання, з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.2, А.9.5.

Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.9.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.2.1, Б.9.2.2, Б.9.2.6, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.9.4, А.9.5, з метою зміни рівня захищеності переданих об'єктів усіх типів, наведених при відповіді на п. А.9.3, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.9.6 і таких, що

визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну рівня захищеності переданих об'єктів різного типу, наведених при відповіді на п. А.9.6, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни рівня захищеності, опис порядку перевірки факту зміни рівня захищеності (шляхом часткового повтору відповідних перевірок згідно з п. В.9.2.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.9.3 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-3 – "Повна цілісність при обміні"

Методика випробувань функціональної послуги безпеки "Цілісність при обміні" рівня ЦВ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.9.3.1-Б.9.3.7, має містити:

В.9.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.3.2, Б.9.3.6, шляхом попереднього (перед виконанням перевірок згідно з п. В.9.3.2-В.9.3.5) виконання для відповідних типів користувачів, наведених при відповіді на п. А.9.6, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.9.6, у засобах, наведених при відповіді на п. А.9.4, А.9.5.

В.9.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.3.4, Б.9.3.5, у частині, що стосується автентифікації атрибутів джерела і приймача об'єкта, шляхом попереднього (перед виконанням перевірок згідно з п. В.9.3.3-В.9.3.5) виконання стосовно приймача об'єкта і його атрибутів, наведених при відповіді на п. А.9.7.1, та джерела об'єкта і його атрибутів, наведених при відповіді на п. А.9.8.1, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" певного рівня згідно з п. В.20.

В.9.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.3.1, Б.9.3.3-Б.9.3.5 шляхом:

- виконання спроб передачі (експорту), модифікації з використанням відповідних засобів випробувань і подальшого приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3, об'єктів усіх типів, наведених при відповіді на п. А.9.3, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.9.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, та атрибутів приймача об'єкта, наведених при відповіді на п. А.9.7.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.9.8.1, з подальшим аналізом результатів приймання модифікованих об'єктів з метою

підтвердження можливості виявлення порушень цілісності інформації, що міститься в переданих об'єктах різного типу, з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.1, А.9.4, підтвердження можливості оброблення запитів на експорт захищеного об'єкта певного типу передавальним КЗЗ (компонентом КЗЗ) на підставі атрибутів доступу інтерфейсного процесу відповідного типу і приймача об'єкта, наведених при відповіді на п. А.9.7.1, та підтвердження можливості оброблення запитів на імпорт захищеного об'єкта певного типу приймаючим КЗЗ (компонентом КЗЗ) на підставі атрибутів доступу інтерфейсного процесу відповідного типу і джерела об'єкта, наведених при відповіді на п. А.9.8.1;

- виконання спроб передачі (експорту) послідовності об'єктів і подальшого приймання (імпорту) об'єктів у порядку, відмінному від порядку передачі (експорту), відмови від приймання (імпорту) деяких об'єктів з послідовності, а також багаторазового приймання (імпорту) деяких об'єктів з послідовності з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3, об'єктів усіх типів, наведених при відповіді на п. А.9.3, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.9.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, та атрибутів приймача об'єкта, наведених при відповіді на п. А.9.7.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.9.8.1, з подальшим аналізом результатів приймання об'єктів з метою підтвердження можливості виявлення фактів їх видалення або дублювання з використанням засобів і механізмів, наведених при відповіді на п. А.9.2.2, А.9.5.

Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу і різних атрибутів одержувача або джерела об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.9.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.3.1, Б.9.3.2, Б.9.3.6, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.9.4, А.9.5, з метою зміни рівня захищеності переданих об'єктів усіх типів, наведених при відповіді на п. А.9.3, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.9.6 і таких, що визначають для кожного типу користувачів і кожного типу захищених об'єктів як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну рівня захищеності переданих об'єктів різного типу, наведених при відповіді на п. А.9.6, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни рівня захищеності, опис порядку перевірки факту зміни рівня захищеності (шляхом часткового повтору відповідних перевірок згідно з п. В.9.3.3), а також критерії

визнання результатів перевірки успішними чи неуспішними.

В.9.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.9.3.1, Б.9.3.7, шляхом виконання спроб передачі (експорту) і приймання (імпорту) з використанням існуючих інтерфейсних процесів усіх типів, наведених при відповіді на п. А.9.3, об'єктів усіх типів, наведених при відповіді на п. А.9.3, для всіх можливих сполучень атрибутів об'єктів, наведених при відповіді на п. А.9.4 і таких, що визначають рівень їх захищеності, атрибутів інтерфейсних процесів, що здійснюють передачу, та атрибутів приймача об'єкта, наведених при відповіді на п. А.9.7.1, атрибутів інтерфейсних процесів, що здійснюють приймання, та атрибутів джерела об'єкта, наведених при відповіді на п. А.9.8.1, з подальшим аналізом вмісту переданих (експортованих) і прийнятих (імпортованих) об'єктів з метою підтвердження того, що представлення захищеного об'єкта певного типу є функцією атрибутів доступу інтерфейсного процесу відповідного типу, самого об'єкта, а також його джерела і приймача, згідно з описом, наведеним при відповіді на п. А.9.9. Опис порядку перевірки має містити опис очікуваних результатів для кожної спроби передачі (експорту) і приймання (імпорту) об'єкта кожного типу з використанням інтерфейсного процесу кожного типу і різних атрибутів одержувача або джерела об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.10 Вимоги до методики випробувань функціональної послуги безпеки "Використання ресурсів"

В.10.1 Вимоги до методики випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-1 – "Квоти"

Методика випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.10.1.1-Б.10.1.4, має містити:

В.10.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.1.3, в частині, що стосується оброблення запитів на зміну встановлених обмежень лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.10.1.2-В.10.1.3) виконання для відповідних типів користувачів, наведених при відповіді на п. А.10.7, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.10.7, у засобах, наведених при відповіді на п. А.10.6.

В.10.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.1.1, Б.10.1.2, Б.10.1.4, шляхом виконання, з використанням відповідних засобів випробувань, запитів з метою

створення об'єктів усіх типів, наведених при відповіді на п. А.10.2.2, з боку окремих користувачів усіх типів, наведених при відповіді на п. А.10.4.2, для різним чином заданих обмежень, наведених при відповіді на п. А.10.3, як без перевищення, так і з перевищенням встановлених обмежень на кількість об'єктів (обсяг ресурсів) кожного типу, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.10.5. Опис порядку перевірки має містити опис, з урахуванням правил контролю за дотриманням встановлених обмежень, наведених при відповіді на п. А.10.5, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби створення об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.10.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.1.1, Б.10.1.2, Б.10.1.3, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.10.6, з метою зміни встановлених обмежень, наведених при відповіді на п. А.10.3, на кількість об'єктів (обсяг ресурсів) різного типу, наведених при відповіді на п. А.10.2.2, що виділяються користувачам усіх типів, наведених при відповіді на п. А.10.4.2, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.10.7 і таких, що визначають як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну встановлених обмежень для об'єктів різного типу, наведених при відповіді на п. А.10.7, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни встановлених обмежень, опис порядку перевірки факту зміни встановленого обмеження (шляхом часткового повтору відповідних перевірок згідно з п. В.10.1.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.10.2 Вимоги до методики випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-2 – "Припинення захоплення ресурсів"

Методика випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.10.2.1-Б.10.2.5, має містити:

В.10.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.2.3, в частині, що стосується оброблення запитів на зміну встановлених обмежень лише в тому випадку, якщо вони надходять від адміністраторів або користувачів яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.10.2.2-В.10.2.3) виконання для відповідних типів користувачів, наведених

при відповіді на п. А.10.7, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.10.7, у засобах, наведених при відповіді на п. А.10.6.

В.10.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.2.1, Б.10.2.2, Б.10.2.4, Б.10.2.5, шляхом виконання, з використанням відповідних засобів випробувань, запитів з метою створення об'єктів усіх типів, наведених при відповіді на п. А.10.2.1, з боку окремих користувачів усіх типів, наведених при відповіді на п. А.10.4.2, для різним чином заданих обмежень, наведених при відповіді на п. А.10.3, А.10.8.2, як без перевищення, так і з перевищенням встановлених обмежень на кількість об'єктів (обсяг ресурсів) кожного типу, у тому числі такого, що може призвести до недоступності послуг або ресурсів іншим користувачам, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.10.5. Опис порядку перевірки має містити опис, з урахуванням правил контролю за дотриманням встановлених обмежень, наведених при відповіді на п. А.10.5, А.10.9, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби створення об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.10.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.2.1, Б.10.2.2, Б.10.2.3, Б.10.2.4, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.10.6, з метою зміни встановлених обмежень, наведених при відповіді на п. А.10.3, на кількість об'єктів (обсяг ресурсів) різного типу, наведених при відповіді на п. А.10.2.1, що виділяються користувачам усіх типів, наведених при відповіді на п. А.10.4.2, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.10.7 і таких, що визначать як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну встановлених обмежень для об'єктів різного типу, наведених при відповіді на п. А.10.7, а також правил установлення обмежень, наведених при відповіді на п. А.10.9, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни встановлених обмежень, опис порядку перевірки факту зміни встановленого обмеження (шляхом часткового повтору відповідних перевірок згідно з п. В.10.2.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.10.3 Вимоги до методики випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-3 – "Пріоритетність використання ресурсів"

Методика випробувань функціональної послуги безпеки "Використання ресурсів" рівня ДР-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.10.3.1-Б.10.3.5, має містити:

В.10.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.3.3, в частині, що стосується оброблення запитів на зміну встановлених обмежень лише в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.10.3.2-В.10.3.3) виконання для відповідних типів користувачів, наведених при відповіді на п. А.10.7, випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.10.7, у засобах, наведених при відповіді на п. А.10.6.

В.10.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.3.1, Б.10.3.2, Б.10.3.4, Б.10.3.5, шляхом виконання, з використанням відповідних засобів випробувань, запитів з метою створення об'єктів усіх типів, наведених при відповіді на п. А.10.2.1, з боку окремих користувачів (та їх груп) усіх типів, наведених при відповіді на п. А.10.4.1, для різним чином заданих обмежень, наведених при відповіді на п. А.10.3, А.10.8.1, як без перевищення, так і з перевищенням встановлених обмежень на кількість об'єктів (обсяг ресурсів) кожного типу, у тому числі такого, яке може призвести до недоступності послуг або ресурсів іншим користувачам, з подальшим контролем результатів оброблення цих запитів засобами КЗЗ, наведеними при відповіді на п. А.10.5. Опис порядку перевірки має містити опис, з урахуванням правил контролю за дотриманням встановлених обмежень, наведених при відповіді на п. А.10.5, А.10.9, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби створення об'єкта, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.10.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.10.3.1, Б.10.3.2, Б.10.3.3, Б.10.3.4, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.10.6, з метою зміни встановлених обмежень, наведених при відповіді на п. А.10.3, на кількість об'єктів (обсяг ресурсів) різного типу, наведених при відповіді на п. А.10.2.1, що виділяються користувачам (та їх групам) усіх типів, наведених при відповіді на п. А.10.4.1, для різних наборів атрибутів доступу користувачів, наведених при відповіді на п. А.10.7 і таких, що визначають як наявність, так і відсутність у користувача адміністративних повноважень. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на зміну встановлених обмежень для об'єктів різного типу, наведених при відповіді на п. А.10.7, а також правил установлення обмежень, наведених при відповіді на п. А.10.9, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби зміни встановлених обмежень, опис порядку перевірки факту зміни встановленого обмеження (шляхом часткового повтору відповідних перевірок

згідно з п. В.10.3.2), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.11 Вимоги до методики випробувань функціональної послуги безпеки "Стійкість до відмов"

В.11.1 Вимоги до методики випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-1 – "Стійкість при обмежених відмовах"

Методика випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.11.1.1-Б.11.1.5, має містити:

В.11.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.1.1-Б.11.1.3, шляхом виконання перевірки результатів аналізу відмов та їх наслідків, наведених при відповіді на п. А.11.2, А.11.3.2, А.11.4.2. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.11.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.1.5, у частині, що стосується оповіщення про відмову будь-якого захищеного компонента адміністраторів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.11.1.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.11.5.

В.11.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.1.4, Б.11.1.5, шляхом почергової імітації, з використанням відповідних засобів випробувань, кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.11.2, А.11.3.2, з метою:

- підтвердження можливості, при відмові одного компонента, продовження функціонування інших компонентів ОЕ зі зниженням характеристик, наведених при відповіді на п. А.11.4.2;

- підтвердження можливості, з використанням засобів і механізмів, наведених при відповіді на п. А.11.5, оповіщення адміністратора про відмову будь-якого компонента.

Опис порядку перевірки має містити опис очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.11.2 Вимоги до методики випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-2 – "Стійкість з погіршенням характеристик обслуговування"

Методика випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.11.2.1-Б.11.2.5, має містити:

В.11.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.2.1-Б.11.2.3, шляхом виконання перевірки результатів аналізу відмов та їх наслідків, наведених при відповіді на п. А.11.2, А.11.3.1, А.11.4.2. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.11.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.2.5, у частині, що стосується оповіщення про відмову будь-якого захищеного компонента адміністраторів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.11.2.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.11.5.

В.11.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.2.4, Б.11.2.5, шляхом почергової імітації, з використанням відповідних засобів випробувань, кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.11.2, А.11.3.1, з метою:

- підтвердження можливості, при відмові одного компонента, продовження функціонування інших компонентів ОЕ зі зниженням характеристик, наведених при відповіді на п. А.11.4.2;

- підтвердження можливості, з використанням засобів і механізмів, наведених при відповіді на п. А.11.5, оповіщення адміністратора про відмову будь-якого компонента.

Опис порядку перевірки має містити опис очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.11.3 Вимоги до методики випробувань функціональної послуги

безпеки "Стійкість до відмов" рівня ДС-3 – "Стійкість без погіршення характеристик обслуговування"

Методика випробувань функціональної послуги безпеки "Стійкість до відмов" рівня ДС-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.11.3.1-Б.11.3.5, має містити:

В.11.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.3.1-Б.11.3.3, шляхом виконання перевірки результатів аналізу відмов та їх наслідків, наведених при відповіді на п. А.11.2, А.11.3.1, А.11.4.1. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.11.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.3.5, у частині, що стосується оповіщення про відмову будь-якого захищеного компонента адміністраторів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.11.3.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.11.5.

В.11.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.11.3.4, Б.11.3.3, шляхом почергової імітації, з використанням відповідних засобів випробувань, кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.11.2, А.11.3.1, з метою:

- підтвердження можливості, при відмові одного компонента, продовження функціонування інших компонентів ОЕ без зниження характеристик обслуговування;

- підтвердження можливості, з використанням засобів і механізмів, наведених при відповіді на п. А.11.5, оповіщення адміністратора про відмову будь-якого компонента.

Опис порядку перевірки має містити опис очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.12 Вимоги до методики випробувань функціональної послуги безпеки "Гаряча заміна"

В.12.1 Вимоги до методики випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-1 – "Модернізація"

Методика випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-1 з метою забезпечення можливості перевірки вимог програми

випробувань, розробленої з урахуванням вимог п. Б.12.1.1-Б.12.1.2, має містити:

В.12.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.1.2, в частині, що стосується виконання модернізації (upgrade) компонентів ОЕ, що входять до складу КЗЗ, адміністраторами або користувачами з відповідними повноваженнями, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.12.1.2) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.12.5, у засобах, наведених при відповіді на п. А.12.3.

В.12.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.1.1, Б.12.1.2, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.12.3, з метою виконання модернізації (upgrade) кожного з компонентів ОЕ, наведених при відповіді на п. А.12.2.2, для різних атрибутів користувачів, наведених при відповіді на п. А.12.5, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим перезапуском заміненого компонента ОЕ та виконанням перевірки його працездатності з погляду безперервності реалізації функцій захисту. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на виконання модернізації (upgrade) компонентів ОЕ, наведених при відповіді на п. А.12.3, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби виконання модернізації (upgrade), опис порядку перевірки факту збереження працездатності компонента ОЕ та безперервності реалізації функцій захисту (шляхом часткового повтору відповідних перевірок функціональних послуг безпеки, у реалізації яких задіяний цей компонент), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.12.2 Вимоги до методики випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-2 – "Обмежена гаряча заміна"

Методика випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.12.2.1-12.2.3, має містити:

В.12.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.2.3, в частині, що стосується виконання модернізації (upgrade) або заміни компонентів ОЕ, що входять до складу КЗЗ, адміністраторами або користувачами з відповідними повноваженнями, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з

п. В.12.2.2-В.12.2.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.12.5, у засобах, наведених при відповіді на п. А.12.3.

В.12.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.2.2, шляхом попереднього (перед виконанням перевірок згідно з п. В.12.2.3) виконання для компонентів ОЕ, наведених при відповіді на п. А.12.4.2, випробувань засобів реалізації функціональної послуги безпеки "Стійкість до відмов" певного рівня згідно з п. В.11.

В.12.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.2.1, Б.12.2.3, шляхом:

- виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.12.3, з метою виконання модернізації (upgrade) кожного з компонентів ОЕ, наведених при відповіді на п. А.12.2.1, для різних атрибутів користувачів, наведених при відповіді на п. А.12.5, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим перезапуском заміненого компонента ОЕ та виконанням перевірки його працездатності з погляду безперервності реалізації функцій захисту;

- виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.12.3, з метою виконання заміни без переривання обслуговування (зупинення) кожного з компонентів ОЕ, наведених при відповіді на п. А.12.4.2, для різних атрибутів користувачів, наведених при відповіді на п. А.12.5, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим виконанням перевірки його працездатності з погляду безперервності реалізації функцій захисту.

Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на виконання модернізації (upgrade) або заміни компонентів ОЕ, наведених при відповіді на п. А.12.3, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби виконання модернізації (upgrade) або заміни компонента, опис порядку перевірки факту збереження працездатності компонента ОЕ та безперервності реалізації функцій захисту (шляхом часткового повтору відповідних перевірок функціональних послуг безпеки, у реалізації яких задіяний цей компонент), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.12.3 Вимоги до методики випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-3 – "Гаряча заміна будь-якого компонента"

Методика випробувань функціональної послуги безпеки "Гаряча заміна" рівня ДЗ-3 з метою забезпечення можливості перевірки вимог програми

випробувань, розробленої з урахуванням вимог п. Б.12.3.1-Б.12.3.3, має містити:

В.12.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.3.3, в частині, що стосується виконання заміни компонентів ОЕ, що входять до складу КЗЗ, адміністраторами або користувачами з відповідними повноваженнями, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.12.3.2-В.12.3.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.12.5, у засобах, наведених при відповіді на п. А.12.3.

В.12.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.3.2, шляхом попереднього (перед виконанням перевірок згідно з п. В.12.3.3) виконання для всіх компонентів ОЕ, наведених при відповіді на п. А.12.4.1, випробувань засобів реалізації функціональної послуги безпеки "Стійкість до відмов" певного рівня згідно з п. В.11.

В.12.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.12.2.1, Б.12.2.3, шляхом виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.12.3, з метою виконання заміни без переривання обслуговування (зупинення) кожного з компонентів ОЕ, наведених при відповіді на п. А.12.4.1, для різних атрибутів користувачів, наведених при відповіді на п. А.12.5, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим виконанням перевірки його працездатності з погляду безперервності реалізації функцій захисту. Опис порядку перевірки має містити опис, з урахуванням правил оброблення запитів користувачів різного типу на виконання заміни компонентів ОЕ, наведених при відповіді на п. А.12.3, очікуваних результатів оброблення запитів засобами КЗЗ для кожної спроби виконання або заміни компонента, опис порядку перевірки факту збереження працездатності компонента ОЕ та безперервності реалізації функцій захисту (шляхом часткового повтору відповідних перевірок функціональних послуг безпеки, у реалізації яких задіяний цей компонент), а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13 Вимоги до методики випробувань функціональної послуги безпеки "Відновлення після збоїв"

В.13.1 Вимоги до методики випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-1 – "Ручне відновлення"

Методика випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-1 з метою забезпечення можливості перевірки вимог

програми випробувань, розробленої з урахуванням вимог п. Б.13.1.1-Б.13.1.3, має містити:

В.13.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.1.1, шляхом виконання перевірки результатів аналізу відмов функціональних модулів ОЕ та їх наслідків, наведених при відповіді на п. А.13.2. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.1.2, в частині, що стосується можливості повернення ОЕ до нормального функціонування після відмови лише адміністраторами або користувачами, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.13.1.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.13.10, у засобах, наведених при відповіді на п. А.13.8.

В.13.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.1.2, Б.13.1.3, шляхом:

- почергової імітації, з використанням відповідних засобів випробувань, кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, з метою підтвердження можливості за правилами, наведеними при відповіді на п. А.13.3, переведення ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувач, якому надані відповідні повноваження;

- виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.13.8, з метою повернення ОЕ зі стану з припиненням обслуговування до нормального функціонування після імітації відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.3, для різних атрибутів користувачів, наведених при відповіді на п. А.13.10, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим виконанням перевірки працездатності ОЕ (шляхом часткового повтору відповідних перевірок функціональних послуг безпеки).

Опис порядку перевірки має містити опис очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.2 Вимоги до методики випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-2 – "Автоматизоване відновлення"

Методика випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.13.2.1-Б.13.2.4, має містити:

В.13.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.2.1, шляхом виконання перевірки результатів аналізу відмов функціональних модулів ОЕ та їх наслідків, наведених при відповіді на п. А.13.2. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.2.3, в частині, що стосується можливості повернення ОЕ до нормального функціонування після відмови лише адміністраторами або користувачами, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.13.2.3-В.13.2.4) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.13.10, у засобах, наведених при відповіді на п. А.13.8.

В.13.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.2.1, Б.13.2.2, шляхом почергової імітації кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.4, з метою підтвердження можливості в засобах, наведених при відповіді на п. А.13.4, визначення можливості використання автоматизованих процедур для повернення ОЕ до нормального функціонування безпечним чином і виконання цих процедур у засобах, наведених при відповіді на п. А.13.6. Опис порядку перевірки має містити опис, з урахуванням правил прийняття рішення про можливість використання автоматизованих процедур, наведених при відповіді на п. А.13.4, і порядку повернення ОЕ до режиму нормального функціонування, наведеного при відповіді на п. А.13.6, очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.2.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.2.3, Б.13.2.4, шляхом:

- почергової імітації, з використанням відповідних засобів випробувань, кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.3 та не наведених при відповіді на п. А.13.4, з метою підтвердження можливості за правилами, наведеними при відповіді на п. А.13.7, переведення ОЕ до стану, з якого повернути його до нормального функціонування може лише адміністратор або користувач, якому надані

відповідні повноваження;

- виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.13.8, з метою повернення ОЕ зі стану з припиненням обслуговування до нормального функціонування після імітації відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.3 та не наведених при відповіді на п. А.13.4, для різних атрибутів користувачів, наведених при відповіді на п. А.13.10, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим виконанням перевірки працездатності ОЕ (шляхом часткового повтору відповідних перевірок функціональних послуг безпеки).

Опис порядку перевірки має містити опис очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.3 Вимоги до методики випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-3 – "Вибіркове відновлення"

Методика випробувань функціональної послуги безпеки "Відновлення після збоїв" рівня ДВ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.13.3.1-Б.13.3.4, має містити:

В.13.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.3.1, шляхом виконання перевірки результатів аналізу відмов функціональних модулів ОЕ та їх наслідків, наведених при відповіді на п. А.13.2. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.3.2, Б.13.3.3, в частині, що стосується можливості повернення ОЕ до нормального функціонування після відмови лише адміністраторами або користувачами, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.13.3.3-В.13.3.4) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.13.10, А.13.11, у засобах, наведених при відповіді на п. А.13.8, А.13.9.

В.13.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.2.1, Б.13.2.2, шляхом почергової імітації кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.4, А.13.5, з метою підтвердження можливості в засобах, наведених при відповіді на п. А.13.4, А.13.5, визначення можливості використання

автоматизованих процедур для повернення ОЕ до нормального функціонування або функціонування з погіршеними характеристиками обслуговування безпечним чином і виконання цих процедур у засобах, наведених при відповіді на п. А.13.6. Опис порядку перевірки має містити опис, з урахуванням правил прийняття рішення про можливість використання автоматизованих процедур, наведених при відповіді на п. А.13.4, А.13.5, та порядку повернення ОЕ до режиму нормального функціонування або функціонування з погіршеними характеристиками обслуговування, наведеного при відповіді на п. А.13.6, очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.13.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.13.3.3, Б.13.3.4, шляхом:

- почергової імітації, з використанням відповідних засобів випробувань, кожної з відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.3 та не наведених при відповіді на п. А.13.4, з метою підтвердження можливості за правилами, наведеними при відповіді на п. А.13.3, А.13.5, А.13.6, А.13.7, переведення ОЕ до стану, з якого повернути його до нормального функціонування може лише адміністратор або користувач, якому надані відповідні повноваження;

- виконання запитів з боку користувачів різного типу, з використанням засобів, наведених при відповіді на п. А.13.8, А.13.9, з метою повернення ОЕ зі стану з припиненням обслуговування до нормального функціонування після імітації відмов кожного з компонентів ОЕ, наведених при відповіді на п. А.13.2, А.13.3 та не наведених при відповіді на п. А.13.4, для різних атрибутів користувачів, наведених при відповіді на п. А.13.10, А.13.11, що визначають як наявність, так і відсутність у користувача адміністративних повноважень, з подальшим виконанням перевірки працездатності ОЕ (шляхом часткового повтору відповідних перевірок функціональних послуг безпеки).

Опис порядку перевірки має містити опис очікуваних результатів для кожної з відмов кожного з компонентів ОЕ, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14. Вимоги до методики випробувань функціональної послуги безпеки "Реєстрація"

В.14.1 Вимоги до методики випробувань функціональної послуги безпеки "Реєстрація" рівня НР-1 – "Зовнішній аналіз"

Методика випробувань функціональної послуги безпеки "Реєстрація" рівня НР-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.14.1.1-Б.14.1.6, має містити:

В.14.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.1.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.1.2-В.14.1.4) виконання для всіх типів користувачів, атрибути яких (наведені при відповіді на п. А.14.6) зберігаються в журналі реєстрації,

випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.14.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.1.1, Б.14.1.2, Б.14.1.6, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.3, з подальшим виконанням передачі журналу реєстрації в інші системи з використанням засобів, наведених при відповіді на п. А.14.8, та аналізу переданого журналу реєстрації в інших системах на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис очікуваних результатів для кожної з реєстраційних подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.1.6, шляхом виконання спроб модифікації або руйнування переданого в інші системи з використанням засобів, наведених при відповіді на п. А.14.8, журналу, що містить події, зареєстровані при виконанні перевірок згідно з п. В.14.1.2, з подальшим аналізом його в цих системах з використанням відповідних засобів на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту переданого журналу, наведеного при відповіді на п. А.14.8, очікуваних результатів для кожної спроби модифікації або руйнування журналу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.1.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.1.1, Б.14.1.3, Б.14.1.4, шляхом:

- аналізу, з використанням відповідних засобів, журналу, переданого при виконанні перевірок згідно з п. В.14.1.2 в інші системи, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події;

- аналізу, з використанням відповідних засобів, журналу, переданого при виконанні перевірок згідно з п. В.14.1.2 в інші системи, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації, достатньої для установлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Опис порядку перевірки має містити опис очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.2 Вимоги до методики випробувань функціональної послуги безпеки "Реєстрація" рівня НР-2 – "Захищений журнал"

Методика випробувань функціональної послуги безпеки "Реєстрація" рівня

НР-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.14.2.1-Б.14.2.7, має містити:

В.14.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.2.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.2.2-В.14.2.5) виконання для всіх типів користувачів, атрибути яких (наведені при відповіді на п. А.14.6) зберігаються в журналі реєстрації, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.14.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.14.2.7, у частині, що стосується наявності засобів перегляду та аналізу журналу реєстрації лише в адміністраторів і користувачів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.2.3-В.14.2.5) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.14.12.

В.14.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.2.1, Б.14.2.2, Б.14.2.7, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.3, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис очікуваних результатів для кожної з реєстраційних подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.2.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.2.6, шляхом виконання, з використанням відповідних засобів випробувань, спроб модифікації або руйнування журналу реєстрації, що містить події, зареєстровані при виконанні перевірок згідно з п. В.14.2.3, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту журналу реєстрації, наведеного при відповіді на п. А.14.10, очікуваних результатів для кожної спроби модифікації або руйнування журналу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.2.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.2.1, Б.14.2.3, Б.14.2.4, шляхом:

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12,

журналу, створеного при виконанні перевірок згідно з п. В.14.2.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події;

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.2.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації, достатньої для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Опис порядку перевірки має містити опис очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.3 Вимоги до методики випробувань функціональної послуги безпеки "Реєстрація" рівня НР-3 – "Сигналізація про небезпеку"

Методика випробувань функціональної послуги безпеки "Реєстрація" рівня НР-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.14.3.1-Б.14.3.9, має містити:

В.14.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.3.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.3.2-В.14.3.6) виконання для всіх типів користувачів, атрибути яких (наведені при відповіді на п. А.14.6) зберігаються в журналі реєстрації, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.14.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.14.3.7, у частині, що стосується наявності засобів перегляду та аналізу журналу реєстрації лише в адміністраторів і користувачів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього, (перед виконанням перевірок згідно з п. В.14.3.3-В.14.3.6) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.14.12, А.14.16.

В.14.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.3.1, Б.14.3.2, Б.14.3.7, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.3, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має

містити опис очікуваних результатів для кожної з реєстраційних подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.3.6, шляхом виконання, з використанням відповідних засобів випробувань, спроб модифікації або руйнування журналу реєстрації, що містить події, зареєстровані при виконанні перевірок згідно з п. В.14.3.3, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту журналу реєстрації, наведеного при відповіді на п. А.14.10, очікуваних результатів для кожної спроби модифікації або руйнування журналу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.3.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.3.1, Б.14.3.3, Б.14.3.4, шляхом:

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.3.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події;

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.3.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації, достатньої для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Опис порядку перевірки має містити опис очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.3.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.3.8, Б.14.3.9, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.14, з подальшим виконанням після кожного запиту або іншої дії:

- аналізу здатності КЗЗ, з використанням засобів, наведених при відповіді на
п. А.14.14, виконувати контроль одиничних або повторюваних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ;

- аналізу здатності КЗЗ, з використанням засобів, наведених при відповіді на
п. А.14.16, негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснювати неруйнівні дії з припинення повторення цих подій.

Опис порядку перевірки має містити опис, з урахуванням порядку функціонування відповідних засобів, наведеного при відповіді на п. А.14.14, А.14.16, очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.4 Вимоги до методики випробувань функціональної послуги безпеки "Реєстрація" рівня НР-4 – "Детальна реєстрація"

Методика випробувань функціональної послуги безпеки "Реєстрація" рівня НР-4 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.14.4.1-Б.14.4.10, має містити:

В.14.4.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.4.6, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.4.2-В.14.4.6) виконання для всіх типів користувачів, атрибути яких (наведені при відповіді на п. А.14.6) зберігаються в журналі реєстрації, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.14.4.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.14.4.8, у частині, що стосується наявності засобів перегляду та аналізу журналу реєстрації лише в адміністраторів і користувачів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.4.3-В.14.4.6) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.14.12, А.14.16.

В.14.4.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.4.1, Б.14.4.2, Б.14.4.3, Б.14.4.8, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.3, А.14.4, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис очікуваних результатів для кожної з реєстраційних подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.4.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.4.7, шляхом виконання, з використанням відповідних засобів випробувань, спроб модифікації або руйнування журналу реєстрації, що містить події, зареєстровані при виконанні перевірок згідно з п. В.14.4.3, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки

має містити опис, з урахуванням порядку функціонування механізмів захисту журналу реєстрації, наведеного при відповіді на п. А.14.10, очікуваних результатів для кожної спроби модифікації або руйнування журналу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.4.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.4.1, Б.14.4.4, Б.14.4.5, шляхом:

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.4.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події;

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.4.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації, достатньої для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Опис порядку перевірки має містити опис очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.4.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.4.9, Б.14.4.10, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.14, з подальшим виконанням після кожного запиту або іншої дії:

- аналізу здатності КЗЗ, з використанням засобів, наведених при відповіді на
п. А.14.14, виконувати контроль одиничних чи повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ;

- аналізу здатності КЗЗ, з використанням засобів, наведених при відповіді на
п. А.14.16, негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснювати неруйнівні дії з припинення повторення цих подій.

Опис порядку перевірки має містити опис, з урахуванням порядку функціонування відповідних засобів, наведеного при відповіді на п. А.14.14, А.14.16, очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.5 Вимоги до методики випробувань функціональної послуги безпеки "Реєстрація" рівня НР-5 – "Аналіз у реальному часі"

Методика випробувань функціональної послуги безпеки "Реєстрація" рівня НР-5 з метою забезпечення можливості перевірки вимог програми випробувань,

розробленої з урахуванням вимог п. Б.14.5.1-Б.14.5.11, має містити:

В.14.5.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.5.6, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.5.2-В.14.5.6) виконання для всіх типів користувачів, атрибути яких (наведені при відповіді на п. А.14.6) зберігаються в журналі реєстрації, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.14.5.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.14.5.8, у частині, що стосується наявності засобів перегляду та аналізу журналу реєстрації лише в адміністраторів і користувачів, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.14.5.3-В.14.5.6) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, у засобах, наведених при відповіді на п. А.14.12, А.14.14.

В.14.5.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.5.1, Б.14.5.2, Б.14.5.3, Б.14.5.8, шляхом виконання, з використанням відповідних засобів випробувань, запитів та інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.2, А.14.3, А.14.4, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис очікуваних результатів для кожної з реєстраційних подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.5.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.5.7, шляхом виконання спроб модифікації або руйнування журналу реєстрації, що містить події, зареєстровані при виконанні перевірок згідно з п. В.14.5.3, з подальшим виконанням аналізу журналу реєстрації з використанням засобів, наведених при відповіді на п. А.14.12, на предмет наявності записів про всі зареєстровані події. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту журналу реєстрації, наведеного при відповіді на п. А.14.10, очікуваних результатів для кожної спроби модифікації або руйнування журналу, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.5.5 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.5.1, Б.14.5.4, Б.14.5.5, шляхом:

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.5.3, на предмет

наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації про дату, час, місце, тип і успішність або неуспішність кожної зареєстрованої події;

- аналізу, з використанням засобів, наведених при відповіді на п. А.14.12, журналу, створеного при виконанні перевірок згідно з п. В.14.5.3, на предмет наявності в записах журналу, згідно з описом їх структури, наведеним при відповіді на п. А.14.6, інформації, достатньої для встановлення користувача, процесу та/або об'єкта, що мали відношення до кожної зареєстрованої події.

Опис порядку перевірки має містити опис очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.14.5.6 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.14.5.9, Б.14.5.10, шляхом виконання, з використанням відповідних засобів випробувань, запитів і інших дій (у тому числі шляхом часткового повтору відповідних перевірок інших функціональних послуг безпеки), результатами яких є факти реєстрації засобами, наведеними при відповіді на п. А.14.5, кожної з подій, наведених при відповіді на п. А.14.14, з подальшим виконанням після кожного запиту або іншої дії:

- аналізу здатності КЗЗ, з використанням засобів, наведених при відповіді на

п. А.14.14, виконувати в реальному часі контроль одиничних чи повторюваних реєстраційних подій, що можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ;

- аналізу здатності КЗЗ, з використанням засобів, наведених при відповіді на

п. А.14.16, негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснювати неруйнівні дії з припинення повторення цих подій.

Опис порядку перевірки має містити опис, з урахуванням порядку функціонування відповідних засобів, наведеного при відповіді на п. А.14.14, А.14.16, очікуваних результатів для кожної із зареєстрованих подій, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.15 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація"

В.15.1 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-1 – "Зовнішня ідентифікація та автентифікація"

Методика випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.15.1.1-Б.15.1.3, має містити:

В.15.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.1.1-Б.15.1.3, шляхом одержання, для

всіх типів користувачів, наведених при відповіді на п. А.15.1, з використанням засобів, наведених при відповіді на п. А.15.4, від зовнішнього джерела, наведеного при відповіді на п. А.15.4, автентифікованого ідентифікатора користувача, з подальшим частковим повтором перевірок тих функціональних послуг безпеки, наведених при відповіді на п. А.15.2, для виконання яких потрібні атрибути користувачів, однозначно пов'язані з їх ідентифікаторами та наведені при відповіді на п. А.15.1. При цьому повинна передбачатися, з урахуванням порядку функціонування механізмів захисту переданих ідентифікаторів, наведеного при відповіді на п. А.15.4, можливість виконання, з використанням відповідних засобів випробувань, спроб несанкціонованої модифікації (підміни) переданих ідентифікаторів. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту переданих ідентифікаторів, наведеного при відповіді на п. А.15.4, а також виконуваних перевірок різних функціональних послуг безпеки, наведених при відповіді на п. А.15.2, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.15.2 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-2 – "Одиночна ідентифікація та автентифікація"

Методика випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.15.2.1-Б.15.2.5, має містити:

В.15.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.2.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.15.2.2-В.15.2.3) виконання для всіх типів користувачів, наведених при відповіді на п. А.15.1, випробувань засобів реалізації функціональної послуги безпеки "Достовірний канал" певного рівня згідно з п. В.16, у частині, що стосується використання достовірного каналу для початкової ідентифікації та автентифікації користувача.

В.15.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.2.1-Б.15.2.3, шляхом виконання, для всіх типів користувачів, наведених при відповіді на п. А.15.1, з використанням засобів, наведених при відповіді на п. А.15.7 і таких, що реалізують механізм автентифікації, зазначений при відповіді на п. А.15.6.2, спроб ідентифікації та автентифікації користувача з подальшим частковим повтором перевірок тих функціональних послуг безпеки, наведених при відповіді на п. А.15.2, для виконання яких потрібні атрибути користувачів, однозначно пов'язані з їх ідентифікаторами та наведені при відповіді на п. А.15.1. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу автентифікації, наведеного при відповіді на п. А.15.7, можливість виконання

спроб несанкціонованого входу з порушенням установленого протоколу або пред'явленням хибних даних автентифікації. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу автентифікації, наведеного при відповіді на п. А.15.7, а також виконуваних перевірок різних функціональних послуг безпеки, наведених при відповіді на п. А.15.2, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.15.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.2.4, шляхом виконання, з використанням відповідних засобів випробувань, спроб несанкціонованого доступу з метою перегляду, модифікації або руйнування даних автентифікації, з подальшим виконанням аналізу реакції засобів КЗЗ, наведених при відповіді на п. А.15.9, на такі спроби. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту даних автентифікації, наведених при відповіді на п. А.15.9, очікуваних результатів для кожної спроби несанкціонованого доступу до даних автентифікації, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.15.3 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-3 – "Множинна ідентифікація та автентифікація"

Методика випробувань функціональної послуги безпеки "Ідентифікація та автентифікація" рівня НИ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.15.3.1-Б.15.3.5, має містити:

В.15.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.3.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.15.3.2-В.15.3.3) виконання для всіх типів користувачів, наведених при відповіді на п. А.15.1, і для всіх типів механізмів автентифікації, наведених при відповіді на п. А.15.6.1, випробувань засобів реалізації функціональної послуги безпеки "Достовірний канал" певного рівня згідно з п. В.16, у частині, що стосується використання достовірного каналу для початкової ідентифікації та автентифікації користувача.

В.15.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.3.1-Б.15.3.3, шляхом виконання, для всіх типів користувачів, наведених при відповіді на п. А.15.1, з використанням засобів, наведених при відповіді на п. А.15.7 і таких, що реалізують різні механізми автентифікації, наведені при відповіді на п. А.15.6.1, спроб ідентифікації та автентифікації користувача з подальшим частковим повтором перевірок тих функціональних послуг безпеки, наведених при відповіді на п. А.15.2, для виконання яких потрібні атрибути користувачів, однозначно пов'язані з їх ідентифікаторами та наведені при відповіді на п. А.15.1. При цьому повинна передбачатися, з урахуванням особливостей використовуваних

протоколів автентифікації, наведених при відповіді на п. А.15.7, можливість виконання спроб несанкціонованого входу з порушенням установлених протоколів або пред'явленням хибних даних автентифікації для кожного з механізмів. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколів автентифікації, наведених при відповіді на п. А.15.7, а також виконуваних перевірок різних функціональних послуг безпеки, наведених при відповіді на п. А.15.2, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.15.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.15.3.4, шляхом виконання, з використанням відповідних засобів випробувань, спроб несанкціонованого доступу з метою перегляду, модифікації або руйнування даних автентифікації, що використовуються кожним механізмом, з подальшим виконанням аналізу реакції засобів КЗЗ, наведених при відповіді на п. А.15.9, на такі спроби. Опис порядку перевірки має містити опис, з урахуванням порядку функціонування механізмів захисту даних автентифікації, наведених при відповіді на п. А.15.9, очікуваних результатів для кожної спроби несанкціонованого доступу до даних автентифікації, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.16 Вимоги до методики випробувань функціональної послуги безпеки "Достовірний канал"

В.16.1 Вимоги до методики випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-1 – "Однонаправлений достовірний канал"

Методика випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.16.1.1-Б.16.1.2, має містити:

В.16.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.16.1.1, Б.16.1.2, шляхом виконання, для всіх типів користувачів, наведених при відповіді на п. А.16.2.1, з використанням засобів, наведених при відповіді на п. А.16.4, спроб ініціювання достовірного каналу між користувачем і КЗЗ, використовуваного для початкової ідентифікації та автентифікації. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення достовірного каналу і механізмів його реалізації, наведених при відповіді на п. А.16.4, можливість виконання спроби підміни компонента КЗЗ, з яким ініціюється взаємодія, або доводитися неможливість виконання такої підміни. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення достовірного каналу і механізмів його реалізації, наведених при відповіді на п. А.16.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.16.2 Вимоги до методики випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-2 – "Двонаправлений достовірний канал"

Методика випробувань функціональної послуги безпеки "Достовірний канал" рівня НК-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.16.2.1-Б.16.2.3, має містити:

В.16.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.16.2.1, Б.16.2.2, у частині організації каналу користувач/ КЗЗ, шляхом виконання, для всіх типів користувачів, наведених при відповіді на п. А.16.2.1, з використанням засобів, наведених при відповіді на п. А.16.4, спроб ініціювання достовірного каналу між користувачем і КЗЗ, використовуваного для початкової ідентифікації та автентифікації. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення достовірного каналу і механізмів його реалізації, наведених при відповіді на п. А.16.4, можливість виконання, з використанням відповідних засобів випробувань, спроби підміни компонента КЗЗ, з яким ініціюється взаємодія, або доводитися неможливість виконання такої підміни. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення достовірного каналу і механізмів його реалізації, наведених при відповіді на п. А.16.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.16.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.16.2.1, Б.16.2.2, Б.16.2.3, у частині організації каналу КЗЗ/ користувач, шляхом виконання, для всіх типів користувачів, наведених при відповіді на п. А.16.2.2, з використанням засобів, наведених при відповіді на п. А.16.5, спроб ініціювання достовірного каналу між КЗЗ і користувачем, що використовується з метою, відмінною від початкової ідентифікації та автентифікації. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення достовірного каналу і механізмів його реалізації, наведених при відповіді на п. А.16.5, можливість виконання спроби ініціювання обміну з використанням достовірного каналу без позитивного підтвердження готовності до обміну з боку користувача згідно з правилами, наведеними при відповіді на п. А.16.6. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення достовірного каналу і механізмів його реалізації, наведених при відповіді на п. А.16.5, А.16.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.17 Вимоги до методики випробувань функціональної послуги безпеки "Розмежування обов'язків"

В.17.1 Вимоги до методики випробувань функціональної послуги

безпеки "Розмежування обов'язків" рівня НО-1 – "Виділення адміністратора"

Методика випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.17.1.1-Б.17.1.4, має містити:

В.17.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.17.1.4, шляхом попереднього (перед виконанням перевірок згідно з п. В.17.1.2-В.17.1.3) виконання для користувачів, які відносяться до всіх типів ролей, наведених при відповіді на п. А.17.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.17.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.17.1.1, шляхом виконання аналізу описів ролей і функцій, притаманних різним ролям та наведених при відповіді на п. А.17.2, А.17.3, А.17.4, з метою перевірки факту визначення ролі адміністратора та ролі звичайного користувача і притаманних їм функцій. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.17.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.17.1.2, Б.17.1.3, шляхом виконання для користувачів, які відносяться до всіх типів ролей, наведених при відповіді на п. А.17.2, початкової ідентифікації та автентифікації з використанням засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" з подальшим ініціюванням запуску кожного з функціональних модулів, наведених при відповіді на п. А.17.6, з метою:

- перевірки можливості підтримки у наведених при відповіді на п. А.17.6 модулях призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на п. А.17.5, та доступності чи недоступності їм відповідних функцій, наведених при відповіді та п. А.17.3, А.17.4;

- перевірки можливості призначення користувачів на відповідні ролі у наведених при відповіді на п. А.17.6 модулях лише у випадку виконанням користувачем дій, наведених при відповіді на п. А.17.7 і таких, що підтверджують прийняття користувачем певної ролі.

Опис порядку перевірки має містити опис, з урахуванням функцій, притаманних різним ролям та наведених при відповіді на п. А.17.3, А.17.4, а також особливостей призначення користувачів на різні ролі в різних функціональних модулях, наведених при відповіді на п. А.17.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.17.2 Вимоги до методики випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-2 – "Розмежування обов'язків адміністраторів"

Методика випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.17.2.1-Б.17.2.5, має містити:

В.17.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.17.2.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.17.2.2-В.17.2.3) виконання для користувачів, які відносяться до всіх типів ролей, наведених при відповіді на п. А.17.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.17.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.17.2.1, Б.17.2.2, шляхом виконання аналізу описів ролей і функцій, притаманних різним ролям та наведених при відповіді на п. А.17.2, А.17.3, А.17.4, з метою перевірки факту визначення мінімум двох різних адміністративних ролей, адміністратора безпеки та іншого адміністратора, з мінімізацією функцій, притаманних кожній з адміністративних ролей та наведених при відповіді на п. А.17.3, а також ролі звичайного користувача і притаманних їй функцій, наведених при відповіді на п. А.17.4. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.17.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.17.2.3, Б.17.2.4, шляхом виконання для користувачів, які відносяться до всіх типів ролей, наведених при відповіді на п. А.17.2, початкової ідентифікації та автентифікації з використанням засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація", з подальшим ініціюванням запуску кожного з функціональних модулів, наведених при відповіді на п. А.17.6, з метою:

- перевірки можливості підтримки у наведених при відповіді на п. А.17.6 модулях призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на п. А.17.5, та доступності чи недоступності їм відповідних функцій, наведених при відповіді та п. А.17.3, А.17.4;

- перевірки можливості призначення користувачів на відповідні ролі у наведених при відповіді на п. А.17.6 модулях лише у випадку виконанням користувачем дій, наведених при відповіді на п. А.17.7 і таких, що підтверджують прийняття користувачем певної ролі.

Опис порядку перевірки має містити опис, з урахуванням функцій, притаманних різним ролям, наведених при відповіді на п. А.17.3, А.17.4, а також особливостей призначення користувачів на різні ролі в різних

функціональних модулях, наведених при відповіді на п. А.17.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.17.3 Вимоги до методики випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-3 – "Розмежування обов'язків на підставі привілеїв"

Методика випробувань функціональної послуги безпеки "Розмежування обов'язків" рівня НО-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.17.3.1-Б.17.3.6, має містити:

В.17.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.17.3.6, шляхом попереднього (перед виконанням перевірок згідно з п. В.17.3.2-В.17.3.3) виконання для користувачів, які відносяться до всіх типів ролей, наведених при відповіді на п. А.17.2, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.17.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.17.3.1-Б.17.3.3, шляхом виконання аналізу описів ролей і функцій, притаманних різним ролям та наведених при відповіді на п. А.17.2, А.17.3, А.17.4, з метою перевірки факту визначення мінімум двох різних адміністративних ролей, адміністратора безпеки та іншого адміністратора, з мінімізацією функцій, притаманних кожній з адміністративних ролей та наведених при відповіді на п. А.17.3, а також декількох ролей звичайних користувачів і притаманних їм функцій, наведених при відповіді на п. А.17.4. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.17.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.17.3.3, Б.17.3.5, шляхом виконання для користувачів, які відносяться до всіх типів ролей, наведених при відповіді на п. А.17.2, початкової ідентифікації та автентифікації з використанням засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація", з подальшим ініціюванням запуску кожного з функціональних модулів, наведених при відповіді на п. А.17.6, з метою:

- перевірки можливості підтримки у наведених при відповіді на п. А.17.6 модулях призначення користувачів на відповідні ролі згідно з атрибутами, наведеними при відповіді на п. А.17.5, та доступності чи недоступності їм відповідних функцій, наведених при відповіді та п. А.17.3, А.17.4;

- перевірки можливості призначення користувачів на відповідні ролі у наведених при відповіді на п. А.17.6 модулях лише у випадку виконання

користувачем дій, наведених при відповіді на п. А.17.7 і таких, що підтверджують прийняття користувачем певної ролі.

Опис порядку перевірки має містити опис, з урахуванням функцій, притаманних різним ролям та наведених при відповіді на п. А.17.3, А.17.4, а також особливостей призначення користувачів на різні ролі в різних функціональних модулях, наведених при відповіді на п. А.17.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.18 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту"

В.18.1 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-1 – "КЗЗ з контролем цілісності"

Методика випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.18.1.1-Б.18.1.3, має містити:

В.18.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.1.2, у частині, що стосується можливості оповіщення адміністратора про порушення цілісності компонента КЗЗ і можливості повернення ОЕ до нормального функціонування після виявлення порушення цілісності будь-якого компонента лише адміністраторами або користувачами, які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.18.1.2) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.18.6, у засобах, наведених при відповіді на п. А.18.5.

В.18.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.1.1, Б.18.1.2, шляхом виконання почергової модифікації, з використанням відповідних засобів випробувань, кожного з компонентів КЗЗ, наведених при відповіді на п. А.1.2.1, А.1.2.2, перед їх запуском, з контролем фактів:

- виявлення порушення цілісності засобами і механізмами, наведеними при відповіді на п. А.18.3;
- оповіщення адміністратора про виявлені факти порушення цілісності засобами і механізмами, наведеними при відповіді на п. А.18.4;
- реєстрації відповідних подій засобами реалізації послуги "Реєстрація" певного рівня;

- автоматичного відновлення засобами, наведеними при відповіді на п. А.18.5, відповідності компонента КЗЗ еталону або переведення ними ОЕ у стан, з якого повернути його до нормального функціонування може лише адміністратор або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3.

Перевірка засобів реалізації послуги "Реєстрація" у частині, що стосується реєстрації відповідних подій, може виконуватися, шляхом випробувань згідно з п. В.14. Опис порядку перевірки має містити опис, з урахуванням особливостей реалізації механізмів і засобів виявлення порушень цілісності різних компонентів КЗЗ, наведених при відповіді на п. А.18.3, механізмів і засобів оповіщення адміністраторів про виявлені факти порушення цілісності, наведених при відповіді на п. А.18.4, засобів автоматичного відновлення відповідності зруйнованих компонентів КЗЗ еталону, наведених при відповіді на п. А.18.5, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.18.1.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.1.3, шляхом виконання аналізу наведених при відповіді на п. А.18.10 описів обмежень, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.18.2 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-2 – "КЗЗ з гарантованою цілісністю"

Методика випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.18.2.1-Б.18.2.3, має містити:

В.18.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.2.1, Б.18.2.2, шляхом виконання, з використанням відповідних засобів випробувань, з урахуванням атрибутів, наведених при відповіді на п. А.18.8, на підставі яких реалізується виділення домену КЗЗ, спроб порушення цілісності кожного з компонентів КЗЗ, наведених при відповіді на п. А.1.2.1, А.1.2.2, які знаходяться як у стані зберігання, так і в стані виконання, з подальшим контролем реакції засобів КЗЗ, наведених при відповіді на п. А.18.9, на такі спроби. Опис порядку перевірки має містити опис, з урахуванням особливостей реалізації механізмів і засобів виділення домену

КЗЗ, наведених при відповіді на п. А.18.9, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.18.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.2.3, шляхом виконання аналізу наведених при відповіді на п. А.18.10 описів обмежень, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.18.3 Вимоги до методики випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-3 – "КЗЗ з функціями диспетчера доступу"

Методика випробувань функціональної послуги безпеки "Цілісність комплексу засобів захисту" рівня НЦ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.18.3.1-Б.18.3.3, має містити:

В.18.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.3.1, Б.18.3.2, шляхом виконання, з використанням відповідних засобів випробувань, з урахуванням атрибутів, наведених при відповіді на п. А.18.8, на підставі яких реалізується виділення домену КЗЗ, спроб порушення цілісності кожного з компонентів КЗЗ, наведених при відповіді на п. А.1.2.1, А.1.2.2, які знаходяться як у стані зберігання, так і в стані виконання, з подальшим контролем реакції засобів КЗЗ, наведених при відповіді на п. А.18.9, на такі спроби. Опис порядку перевірки має містити опис, з урахуванням особливостей реалізації механізмів і засобів виділення домену КЗЗ, наведених при відповіді на п. А.18.9, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.18.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.18.3.3, шляхом виконання аналізу наведених при відповіді на п. А.18.11 обґрунтувань тверджень про те, що всі послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ. Опис порядку перевірки має містити опис очікуваних результатів перевірки за кожним з пунктів методики випробувань, сформульованих з урахуванням вимог відповідних пунктів програми випробувань, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.19 Вимоги до методики випробувань функціональної послуги безпеки "Самотестування"

В.19.1 Вимоги до методики випробувань функціональної послуги безпеки "Самотестування" рівня НТ-1 – "Самотестування за запитом"

Методика випробувань функціональної послуги безпеки "Самотестування" рівня НТ-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.19.1.1-Б.19.1.2, має містити:

В.19.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.1.2, у частині, що стосується можливості виконання набору тестів за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.19.1.2) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.19.5, у засобах, наведених при відповіді на п. А.19.5.

В.19.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.1.1, Б.19.1.2, шляхом виконання, з використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.2, з подальшим ініціюванням виконання, з використанням засобів, наведених при відповіді на п. А.19.5, наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів, наведених при відповіді на п. А.19.3, та контролю результатів виконання різних тестів. Опис порядку перевірки має містити опис, з урахуванням наведеного при відповіді на п. А.19.5 порядку оброблення запитів на виконання різних тестів, використовуваних для оцінювання правильності функціонування різних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, з використанням засобів, наведених при відповіді на п. А.19.5, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.19.2 Вимоги до методики випробувань функціональної послуги безпеки "Самотестування" рівня НТ-2 – "Самотестування при старті"

Методика випробувань функціональної послуги безпеки "Самотестування" рівня НТ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.19.2.1-Б.19.2.3, має містити:

В.19.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.2.2, у частині, що стосується можливості виконання набору тестів за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою

реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.19.2.2-В.19.2.3) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.19.5, у засобах, наведених при відповіді на п. А.19.5.

В.19.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.2.1, Б.19.2.2, шляхом виконання, з використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.2, з подальшим ініціюванням виконання, з використанням засобів, наведених при відповіді на п. А.19.5, наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів, наведених при відповіді на п. А.19.3, та контролю результатів виконання різних тестів. Опис порядку перевірки має містити опис, з урахуванням наведеного при відповіді на п. А.19.5 порядку оброблення запитів на виконання різних тестів, використовуваних для оцінювання правильності функціонування різних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, з використанням засобів, наведених при відповіді на А.19.5, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.19.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.2.1, Б.19.2.3, шляхом виконання, з використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.2, з подальшим перезапуском ОЕ з метою ініціювання виконання, з використанням засобів, наведених при відповіді на п. А.19.6, наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів, наведених при відповіді на п. А.19.3, при старті ОЕ, та контролю результатів виконання різних тестів. Опис порядку перевірки має містити опис, з урахуванням наведеного при відповіді на п. А.19.6 порядку виконання при старті ОЕ різних тестів, використовуваних для оцінювання правильності функціонування різних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, з використанням засобів, наведених при відповіді на А.19.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.19.3 Вимоги до методики випробувань функціональної послуги безпеки "Самотестування" рівня НТ-3 – "Самотестування в реальному часі"

Методика випробувань функціональної послуги безпеки "Самотестування" рівня НТ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.19.3.1-Б.19.3.4, має

містити:

В.19.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.3.2, у частині, що стосується можливості виконання набору тестів за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги "Розмежування обов'язків" рівня НО-1 або вище, наведеною при відповіді на п. А.17.2-А.17.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.19.3.2-В.19.3.4) виконання випробувань засобів реалізації функціональної послуги безпеки "Розмежування обов'язків" певного рівня згідно з п. В.17, з використанням атрибутів користувачів, наведених при відповіді на п. А.19.5, у засобах, наведених при відповіді на п. А.19.5.

В.19.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.3.1, Б.19.3.2, шляхом виконання, з використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.2, з подальшим ініціюванням виконання, з використанням засобів, наведених при відповіді на п. А.19.5, наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів, наведених при відповіді на п. А.19.3, та контролю результатів виконання різних тестів. Опис порядку перевірки має містити опис, з урахуванням наведеного при відповіді на п. А.19.5 порядку оброблення запитів на виконання різних тестів, використовуваних для оцінювання правильності функціонування різних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, з використанням засобів, наведених при відповіді на п. А.19.5, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.19.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.3.1, Б.19.3.3, шляхом виконання, з використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.2, з подальшим перезапуском ОЕ з метою ініціювання виконання, з використанням засобів, наведених при відповіді на п. А.19.6, наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів, наведених при відповіді на п. А.19.3, при старті ОЕ, та контролю результатів виконання різних тестів. Опис порядку перевірки має містити опис, з урахуванням наведеного при відповіді на п. А.19.6 порядку виконання при старті ОЕ різних тестів, використовуваних для оцінювання правильності функціонування різних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, з використанням засобів, наведених при відповіді на А.19.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.19.3.4 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.19.3.1, Б.19.3.4, шляхом виконання, з

використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.2, з подальшим перезапуском відповідного компонента з метою ініціювання виконання, з використанням засобів, наведених при відповіді на п. А.19.7, наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів, наведених при відповіді на п. А.19.3, у процесі штатного функціонування ОЕ, та контролю результатів виконання різних тестів. Опис порядку перевірки має містити опис, з урахуванням наведеного при відповіді на п. А.19.7 порядку виконання в процесі штатного функціонування ОЕ різних тестів, використовуваних для оцінювання правильності функціонування різних компонентів ОЕ, що входять до складу КЗЗ, наведених при відповіді на п. А.19.3, з використанням засобів, наведених при відповіді на А.19.7, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.20 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні"

В.20.1 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-1 – "Автентифікація вузла"

Методика випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.20.1.1-Б.20.1.3, має містити:

В.20.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.20.1.1-Б.20.1.3, шляхом виконання спроб взаємодії з іншим КЗЗ (компонентом КЗЗ) з ініціюванням виконання засобами, наведеними при відповіді на п. А.20.4, що реалізують механізми взаємної ідентифікації та автентифікації, наведені при відповіді на п. А.20.4, операцій взаємної ідентифікації та автентифікації різних КЗЗ (компонентів КЗЗ) з подальшим контролем результатів виконання взаємної ідентифікації та автентифікації. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу взаємної автентифікації, наведеного при відповіді на п. А.20.4, можливість ініціювання виконання взаємної ідентифікації та автентифікації з порушенням установленого протоколу або використанням хибних атрибутів КЗЗ, наведених при відповіді на п. А.20.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу автентифікації, наведеного при відповіді на п. А.20.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.20.2 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-2 – "Автентифікація джерела даних"

Методика випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.20.2.1-Б.20.2.4, має містити:

В.20.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.20.2.1-Б.20.2.3, шляхом виконання спроб взаємодії з іншим КЗЗ (компонентом КЗЗ) з ініціюванням виконання засобами, наведеними при відповіді на п. А.20.4, що реалізують механізми взаємної ідентифікації та автентифікації, наведені при відповіді на п. А.20.4, операцій взаємної ідентифікації та автентифікації різних КЗЗ (компонентів КЗЗ) з подальшим контролем результатів виконання взаємної ідентифікації та автентифікації. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу взаємної автентифікації, наведеного при відповіді на п. А.20.4, можливість ініціювання виконання взаємної ідентифікації та автентифікації з порушенням установленого протоколу або використанням хибних атрибутів КЗЗ, наведених при відповіді на п. А.20.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу автентифікації, наведеного при відповіді на п. А.20.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.20.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.20.2.4, шляхом виконання спроб передачі (експорту) з різних джерел, модифікації та подальшого приймання (імпорту) об'єктів усіх типів, наведених при відповіді на п. А.20.1, з використанням засобів, наведених при відповіді на п. А.20.7, з подальшим аналізом результатів приймання об'єктів різного типу від різних джерел об'єктів з метою підтвердження можливості встановлення джерела кожного експортованого та імпортованого об'єкта кожного типу. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення джерела об'єкта кожного типу, наведеного при відповіді на п. А.20.7, можливість виконання, з використанням відповідних засобів випробувань, передачі об'єктів з порушенням установленого протоколу або використанням хибних атрибутів переданих об'єктів, наведених при відповіді на п. А.20.6. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення джерела об'єкта кожного типу, наведеного при відповіді на п. А.20.7, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.20.3 Вимоги до методики випробувань функціональної послуги безпеки "Ідентифікація та автентифікація при обміні" рівня НВ-3 – "Автентифікація з підтвердженням"

Методика випробувань функціональної послуги безпеки "Ідентифікація та

автентифікація при обміні" рівня НВ-3 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.20.3.1-Б.20.3.5, має містити:

В.20.3.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.20.3.1-Б.20.3.3, шляхом виконання спроб взаємодії з іншим КЗЗ (компонентом КЗЗ) з ініціюванням виконання засобами, наведеними при відповіді на п. А.20.4, що реалізують механізми взаємної ідентифікації та автентифікації, наведені при відповіді на п. А.20.4, операцій взаємної ідентифікації та автентифікації різних КЗЗ (компонентів КЗЗ) з подальшим контролем результатів виконання взаємної ідентифікації та автентифікації. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу взаємної автентифікації, наведеного при відповіді на п. А.20.4, можливість ініціювання виконання взаємної ідентифікації та автентифікації з порушенням установленого протоколу або використанням хибних атрибутів КЗЗ, наведених при відповіді на п. А.20.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу автентифікації, наведеного при відповіді на п. А.20.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.20.3.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.20.3.4, шляхом виконання спроб передачі (експорту) з різних джерел, модифікації та подальшого приймання (імпорту) об'єктів усіх типів, наведених при відповіді на п. А.20.1, з використанням засобів, наведених при відповіді на п. А.20.7, з подальшим аналізом результатів приймання об'єктів різного типу від різних джерел об'єктів з метою підтвердження можливості встановлення джерела кожного експортованого та імпортованого об'єкта кожного типу. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення джерела об'єкта кожного типу, наведеного при відповіді на п. А.20.7, можливість виконання, з використанням відповідних засобів випробувань, передачі об'єктів з порушенням установленого протоколу або використанням хибних атрибутів переданих об'єктів, наведених при відповіді на п. А.20.6. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення джерела об'єкта кожного типу, наведеного при відповіді на п. А.20.7, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.20.3.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.20.3.5, шляхом виконання спроб підтвердження джерела всіх об'єктів усіх типів, використаних при виконанні перевірок згідно з п. В.20.3.2, незалежною третьою стороною, з використанням засобів, наведених при відповіді на п. А.20.7, з подальшим аналізом результатів для кожного об'єкта кожного типу. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу підтвердження джерела об'єкта кожного типу незалежною третьою стороною, наведеного при відповіді на п. А.20.9, можливість виконання передачі об'єктів з порушенням

установленого протоколу або використанням хибних атрибутів переданих об'єктів, наведених при відповіді на п. А.20.9. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу підтвердження джерела об'єкта кожного типу незалежною третьою стороною, наведеного при відповіді на п. А.20.9, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.21 Вимоги до методики випробувань функціональної послуги безпеки "Автентифікація відправника"

В.21.1 Вимоги до методики випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-1 – "Базова автентифікація відправника"

Методика випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.21.1.1-Б.21.1.3, має містити:

В.21.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.21.1.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.21.1.2) виконання для всіх типів користувачів-відправників, атрибути яких наведені при відповіді на п. А.21.3, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.21.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.21.1.1, Б.21.1.2, шляхом виконання спроб передачі (експорту) і подальшого приймання (імпорту) об'єктів усіх типів, наведених при відповіді на п. А.21.1, з використанням засобів, наведених при відповіді на п. А.21.4, для всіх можливих сполучень атрибутів користувачів-відправників, переданих об'єктів та інтерфейсних процесів усіх типів, наведених при відповіді на п. А.21.3, з подальшим аналізом результатів приймання об'єктів різного типу від різних відправників з метою підтвердження можливості встановлення приналежності кожного об'єкта. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення джерела об'єкта кожного типу, наведеного при відповіді на п. А.21.4, можливість виконання, з використанням відповідних засобів випробувань, передачі об'єктів з порушенням установленого протоколу або використанням хибних атрибутів відправників, інтерфейсних процесів та переданих об'єктів, наведених при відповіді на п. А.21.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення приналежності об'єкта кожного типу, наведеного при відповіді на п. А.21.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.21.2 Вимоги до методики випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-2 – "Автентифікація

відправника з підтвердженням"

Методика випробувань функціональної послуги безпеки "Автентифікація відправника" рівня НА-2 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.21.2.1-Б.21.2.5, має містити:

В.21.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.21.2.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.21.2.2-В.21.2.3) виконання для всіх типів користувачів-відправників, атрибути яких наведені при відповіді на п. А.21.3, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.21.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.21.2.1, Б.21.2.2, шляхом виконання спроб передачі (експорту) і подальшого приймання (імпорту) об'єктів усіх типів, наведених при відповіді на п. А.21.1, з використанням засобів, наведених при відповіді на п. А.21.4, для всіх можливих сполучень атрибутів користувачів-відправників, переданих об'єктів та інтерфейсних процесів усіх типів, наведених при відповіді на п. А.21.3, з подальшим аналізом результатів приймання об'єктів різного типу від різних відправників з метою підтвердження можливості встановлення приналежності кожного об'єкта. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення джерела об'єкта кожного типу, наведеного при відповіді на п. А.21.4, можливість виконання, з використанням відповідних засобів випробувань, передачі об'єктів з порушенням установленого протоколу або використанням хибних атрибутів відправників, інтерфейсних процесів та переданих об'єктів, наведених при відповіді на п. А.21.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення приналежності об'єкта кожного типу, наведеного при відповіді на п. А.21.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.21.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.21.2.3, Б.21.2.4, шляхом виконання спроб підтвердження приналежності всіх об'єктів усіх типів, використаних при виконанні перевірок згідно з п. В.21.2.2, незалежною третьою стороною, з використанням засобів, наведених при відповіді на п. А.21.4, з подальшим аналізом результатів для кожного об'єкта кожного типу. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу підтвердження приналежності об'єкта кожного типу незалежною третьою стороною, наведеного при відповіді на п. А.21.6, можливість виконання, з використанням відповідних засобів випробувань, передачі об'єктів з порушенням установленого протоколу або використанням хибних атрибутів переданих об'єктів, наведених при відповіді на п. А.21.6. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу підтвердження приналежності об'єкта кожного типу незалежною третьою

стороною, наведеного при відповіді на п. А.21.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.22 Вимоги до методики випробувань функціональної послуги безпеки "Автентифікація одержувача"

В.22.1 Вимоги до методики випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-1 – "Базова автентифікація одержувача"

Методика випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-1 з метою забезпечення можливості перевірки вимог програми випробувань, розробленої з урахуванням вимог п. Б.22.1.1-Б.22.1.3, має містити:

В.22.1.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.22.1.3, шляхом попереднього (перед виконанням перевірок згідно з п. В.22.1.2) виконання для всіх типів користувачів-одержувачів, атрибути яких наведені при відповіді на п. А.22.3, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.22.1.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.22.1.1, Б.22.1.2, шляхом виконання спроб передачі (експорту) і подальшого приймання (імпорту) об'єктів усіх типів, наведених при відповіді на п. А.22.1, з використанням засобів, наведених при відповіді на п. А.22.4, для всіх можливих сполучень атрибутів користувачів-одержувачів, переданих об'єктів та інтерфейсних процесів усіх типів, наведених при відповіді на п. А.22.3, з подальшим аналізом результатів підтвердження одержання об'єктів різного типу різними одержувачами з метою підтвердження можливості встановлення одержувача кожного об'єкта. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення одержувача об'єкта кожного типу, наведеного при відповіді на п. А.22.4, можливість виконання, з використанням відповідних засобів випробувань, приймання об'єктів з порушенням установленого протоколу або використанням хибних атрибутів одержувачів, інтерфейсних процесів та переданих об'єктів, наведених при відповіді на п. А.22.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення одержувача об'єкта кожного типу, наведеного при відповіді на п. А.22.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.22.2 Вимоги до методики випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-2 – "Автентифікація одержувача з підтвердженням"

Методика випробувань функціональної послуги безпеки "Автентифікація одержувача" рівня НП-2 з метою забезпечення можливості перевірки вимог

програми випробувань, розробленої з урахуванням вимог п. Б.22.2.1-Б.22.2.5, має містити:

В.22.2.1 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.22.2.5, шляхом попереднього (перед виконанням перевірок згідно з п. В.22.2.2-В.22.2.3) виконання для всіх типів користувачів-одержувачів, атрибути яких наведені при відповіді на п. А.22.3, випробувань засобів реалізації функціональної послуги безпеки "Ідентифікація та автентифікація" певного рівня згідно з п. В.15.

В.22.2.2 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням п. Б.22.2.1, Б.22.2.2, шляхом виконання спроб передачі (експорту) і подальшого приймання (імпорту) об'єктів усіх типів, наведених при відповіді на п. А.22.1, з використанням засобів, наведених при відповіді на п. А.22.4, для всіх можливих сполучень атрибутів користувачів-одержувачів, переданих об'єктів та інтерфейсних процесів усіх типів, наведених при відповіді на п. А.22.3, з подальшим аналізом результатів підтвердження одержання об'єктів різного типу різними одержувачами з метою підтвердження можливості встановлення одержувача кожного об'єкта. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу встановлення одержувача об'єкта кожного типу, наведеного при відповіді на п. А.22.4, можливість виконання, з використанням відповідних засобів випробувань, приймання об'єктів з порушенням установленого протоколу або використанням хибних атрибутів одержувачів, інтерфейсних процесів та переданих об'єктів, наведених при відповіді на п. А.22.3. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу встановлення одержувача об'єкта кожного типу, наведеного при відповіді на п. А.22.4, очікуваних результатів для кожної перевірки, а також критерії визнання результатів перевірки успішними чи неуспішними.

В.22.2.3 Опис порядку перевірки вимог програми випробувань, сформульованих з урахуванням Б.22.2.3, Б.22.2.4, шляхом виконання спроб підтвердження факту одержання всіх об'єктів усіх типів, використаних при виконанні перевірок згідно з п. В.22.2.2, незалежною третьою стороною, з використанням засобів, наведених при відповіді на п. А.22.4, з подальшим аналізом результатів для кожного об'єкта кожного типу. При цьому повинна передбачатися, з урахуванням особливостей використовуваного протоколу підтвердження факту одержання об'єкта кожного типу незалежною третьою стороною, наведеного при відповіді на п. А.22.6, можливість виконання, з використанням відповідних засобів випробувань, приймання об'єктів з порушенням установленого протоколу або використанням хибних атрибутів переданих об'єктів, наведених при відповіді на п. А.22.6. Опис порядку перевірки має містити опис, з урахуванням особливостей протоколу підтвердження факту одержання об'єкта кожного типу незалежною третьою стороною, наведеного при відповіді на п. А.22.6, очікуваних результатів для кожної перевірки, а також критерії визнання результатів